نام و نام خانوادگی	شماره دانشجویی	نام درس	تاریخ	شماره برگه
		امنیت سیستم‌های کامپیوتری	۱۴۰۳/۰۲/۱۱	۱

۱. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۲. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن آشکار - متن رمز شده

ب) گمراه کنندگی - متن آشکار - متن رمز شده

ج) انتشار - متن رمز شده - متن آشکار

د) گمراه کنندگی - متن رمز شده - متن آشکار

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۳. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۴. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 6

ب) 27

ج) 2

د) 25

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۵. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) انتشار - رمز - کلید

ب) انتشار - آشکار - متن رمز

ج) گمراه کنندگی - آشکار - متن رمز

د) گمراه کنندگی - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۶. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) F

ب) E

ج) S

د) P

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۷. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۸. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۹. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 5 ب) 4 ج) 3 د) 6

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۱۰. رقم آخر عدد 3^{90} چند است؟

الف) 9 ب) 6 ج) 8 د) 7

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۱۱. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله از نوع اثبات دانایی صفر است.

ب) یک مساله از نوع روش‌های غیرتعاملی است.

ج) همه گزینه‌ها صحیح است.

د) یک مساله تسهیم راز است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۱۲. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.
ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$
د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۱۳. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 8 ب) 6 ج) 2 د) 4

پاسخ: این عدد ریشه اولیه ندارد.

۱۴. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice ب) کلید محرمانه Alice ج) کلید محرمانه Bob د) کلید عمومی Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۱۵. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۱۶. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۷. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob ب) کلید محرمانه Alice ج) کلید عمومی Alice د) کلید عمومی Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۱۸. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول ب) هیچ‌کدام ج) حمله نوع سوم د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۹. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۰. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به $\phi(n)$ اول باشد.
ب) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
ج) متن اصلی باید نسبت به n اول باشد.
د) کلید عمومی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲۱. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم
ب) حمله نوع سوم
ج) هیچ‌کدام
د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۲. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.
ب) کلید باید به صورت کاملا تصادفی تولید شود.
ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.
د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۲۳. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۲۴. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه کاربرد
ب) لایه پیوند داده
ج) لایه شبکه
د) لایه انتقال

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۲۵. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 7 ب) 34 ج) 17 د) 10

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۲۶. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۷. طول واقعی کلید DES برابر است با .....

الف) ۶۴ ب) ۳۲ ج) ۵۶ د) ۴۸

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۲۸. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۲۹. در SSH چگونه از حمله تغییر قابلیت‌های مشترک نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۳۰. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۱. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 17 ب) 34 ج) 10 د) 7

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۳. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۴. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول ب) حمله نوع دوم ج) هیچ‌کدام د) حمله نوع سوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۵. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۶. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - رمز - کلید ب) انتشار - رمز - کلید

ج) انتشار - آشکار - متن رمز د) گمراه کنندگی - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۷. در SSH چگونه از حمله تغییر قابلیت‌های مشترک نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH

- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۸. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 4 ب) 6 ج) 2 د) 8

پاسخ: این عدد ریشه اولیه ندارد.

۹. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه شبکه ب) لایه انتقال ج) لایه کاربرد د) لایه پیوند داده

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۱۰. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۱۱. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۲. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم ب) هیچ‌کدام ج) حمله نوع سوم د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۳. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۱۴. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) F ب) E ج) P د) S

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۱۵. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۱۶. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۱۷. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob ب) کلید عمومی Bob ج) کلید محرمانه Alice د) کلید عمومی Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۱۸. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به n اول باشد.

ب) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.

ج) متن اصلی باید نسبت به $\phi(n)$ اول باشد.

د) کلید عمومی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۱۹. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۲۰. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۲۱. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 25 ب) 2 ج) 27 د) 6

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۲۲. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله تسهیم راز است.
ب) یک مساله از نوع روش‌های غیرتعاملی است.
ج) همه گزینه‌ها صحیح است.
د) یک مساله از نوع اثبات دانایی صفر است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۲۳. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.
ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$
د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۲۴. طول واقعی کلید DES برابر است با .....

الف) ۶۴ ب) ۳۲ ج) ۵۶ د) ۴۸

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۲۵. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۲۶. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 4 ب) 5 ج) 6 د) 3

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۲۷. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۸. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن آشکار - متن رمز شده
ب) گمراه کنندگی - متن رمز شده - متن آشکار
ج) انتشار - متن آشکار - متن رمز شده
د) انتشار - متن رمز شده - متن آشکار

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۲۹. رقم آخر عدد 3^{90} چند است؟

الف) 9
ب) 6
ج) 8
د) 7

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۳۰. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice
ب) کلید محرمانه Bob
ج) کلید عمومی Alice
د) کلید عمومی Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۱. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه انتقال　　ب) لایه شبکه　　ج) لایه کاربرد　　د) لایه پیوند داده

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۲. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۳. رقم آخر عدد 3^{90} چند است؟

الف) 8　　ب) 9　　ج) 6　　د) 7

پاسخ: ✍ دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

✍ آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۴. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 6　　ب) 8　　ج) 2　　د) 4

پاسخ: این عدد ریشه اولیه ندارد.

۵. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۶. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) همه گزینه‌ها صحیح است.　　ب) یک مساله از نوع روش‌های غیرتعاملی است.

ج) یک مساله تسهیم راز است.　　د) یک مساله از نوع اثبات دانایی صفر است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۷. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init

- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۸. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۹. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Bob　　ب) کلید عمومی Alice　　ج) کلید محرمانه Bob　　د) کلید محرمانه Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۱۰. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۱. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۱۲. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 27　　ب) 25　　ج) 2　　د) 6

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۱۳. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 34　　ب) 17　　ج) 10　　د) 7

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۱۴. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۱۵. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) S　　ب) P　　ج) E　　د) F

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۱۶. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۱۷. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم　　ب) حمله نوع دوم　　ج) حمله نوع اول　　د) هیچ‌کدام

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۸. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice　　ب) کلید عمومی Bob　　ج) کلید محرمانه Alice　　د) کلید محرمانه Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۱۹. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 3　　ب) 5　　ج) 6　　د) 4

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۲۰. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۲۱. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۲۲. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم　　ب) حمله نوع دوم　　ج) هیچ‌کدام　　د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۳. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۴. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن رمز شده - متن آشکار　　ب) گمراه کنندگی - متن آشکار - متن رمز شده
ج) انتشار - متن آشکار - متن رمز شده　　د) انتشار - متن رمز شده - متن آشکار

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۲۵. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۲۶. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - رمز - کلید　　ب) انتشار - رمز - کلید
ج) گمراه کنندگی - آشکار - متن رمز　　د) انتشار - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۲۷. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به $\phi(n)$ اول باشد.
ب) کلید عمومی باید نسبت به n اول باشد.
ج) متن اصلی باید نسبت به n اول باشد.
د) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲۸. طول واقعی کلید DES برابر است با .....

الف) ۴۸
ب) ۳۲
ج) ۵۶
د) ۶۴

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۲۹. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۳۰. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.
ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.
ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.
د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۱. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۳. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول ب) حمله نوع سوم ج) هیچ‌کدام د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۴. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۵. رقم آخر عدد 3^{90} چند است؟

الف) 8 ب) 9 ج) 7 د) 6

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۶. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۷. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۸. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۹. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۱۰. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۱. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۱۲. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۱۳. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه انتقال ب) لایه کاربرد ج) لایه شبکه د) لایه پیوند داده

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۱۴. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.

ب) متن اصلی باید نسبت به $\phi(n)$ اول باشد.

ج) کلید عمومی باید نسبت به n اول باشد.

د) متن اصلی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۱۵. طول واقعی کلید DES برابر است با .....

الف) ۶۴ ب) ۵۶ ج) ۴۸ د) ۳۲

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۱۶. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Bob ب) کلید عمومی Alice ج) کلید محرمانه Bob د) کلید محرمانه Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۱۷. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) انتشار - رمز - کلید
ب) گمراه کنندگی - رمز - کلید
ج) انتشار - آشکار - متن رمز
د) گمراه کنندگی - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۱۸. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 4
ب) 5
ج) 6
د) 3

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۱۹. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۲۰. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۲۱. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 10
ب) 17
ج) 7
د) 34

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۲۲. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله تسهیم راز است.
ب) یک مساله از نوع روش‌های غیرتعاملی است.
ج) همه گزینه‌ها صحیح است.
د) یک مساله از نوع اثبات دانایی صفر است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۲۳. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۴. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 4 ب) 8 ج) 2 د) 6

پاسخ: این عدد ریشه اولیه ندارد.

۲۵. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن رمز شده - متن آشکار
ب) انتشار - متن آشکار - متن رمز شده
ج) گمراه کنندگی - متن آشکار - متن رمز شده
د) انتشار - متن رمز شده - متن آشکار

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۲۶. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 2 ب) 27 ج) 6 د) 25

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۲۷. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) S ب) F ج) E د) P

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۲۸. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام ب) حمله نوع اول ج) حمله نوع دوم د) حمله نوع سوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۹. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۳۰. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob ب) کلید عمومی Bob ج) کلید عمومی Alice د) کلید محرمانه Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

نام و نام خانوادگی	شماره دانشجویی	نام درس	تاریخ	شماره برگه
		امنیت سیستم‌های کامپیوتری	۱۴۰۳/۰۲/۱۱	۵

۱. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) S　　ب) F　　ج) E　　د) P

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۲. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 8　　ب) 6　　ج) 4　　د) 2

پاسخ: این عدد ریشه اولیه ندارد.

۳. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۴. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۵. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 2　　ب) 6　　ج) 25　　د) 27

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۶. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۷. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob　　ب) کلید عمومی Bob　　ج) کلید عمومی Alice　　د) کلید محرمانه Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۸. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۹. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۰. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۱۱. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۱۲. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول ب) حمله نوع دوم ج) هیچ‌کدام د) حمله نوع سوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۳. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۱۴. طول واقعی کلید DES برابر است با .....

الف) ۴۸ ب) ۶۴ ج) ۵۶ د) ۳۲

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۱۵. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۱۶. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۱۷. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - رمز - کلید
ب) گمراه کنندگی - آشکار - متن رمز
ج) انتشار - رمز - کلید
د) انتشار - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۱۸. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به n اول باشد.
ب) متن اصلی باید نسبت به $\phi(n)$ اول باشد.
ج) کلید عمومی باید نسبت به n اول باشد.
د) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۱۹. رقم آخر عدد 3^{90} چند است؟

الف) 6
ب) 9
ج) 7
د) 8

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲۰. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۱. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) همه گزینه‌ها صحیح است.
ب) یک مساله از نوع روش‌های غیرتعاملی است.
ج) یک مساله تسهیم راز است.
د) یک مساله از نوع اثبات دانایی صفر است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۲۲. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام
ب) حمله نوع دوم
ج) حمله نوع اول
د) حمله نوع سوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۳. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.
ب) کلید باید به صورت کاملا تصادفی تولید شود.
ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.
د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۲۴. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.
ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.
ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.
د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۲۵. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 10
ب) 34
ج) 17
د) 7

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۲۶. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice
ب) کلید عمومی Bob
ج) کلید محرمانه Bob
د) کلید عمومی Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۲۷. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.
ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$
د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۲۸. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه کاربرد　　ب) لایه شبکه　　ج) لایه انتقال　　د) لایه پیوند داده

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۲۹. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 3　　ب) 5　　ج) 4　　د) 6

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۳۰. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن رمز شده - متن آشکار　　ب) گمراه کنندگی - متن آشکار - متن رمز شده
ج) گمراه کنندگی - متن رمز شده - متن آشکار　　د) انتشار - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۱. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۲. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۳. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام ب) حمله نوع سوم ج) حمله نوع دوم د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۴. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۵. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم ب) حمله نوع اول ج) حمله نوع دوم د) هیچ‌کدام

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۶. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۷. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۸. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله تسهیم راز است.

ب) یک مساله از نوع اثبات دانایی صفر است.

ج) یک مساله از نوع روش‌های غیرتعاملی است.

د) همه گزینه‌ها صحیح است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۹. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 10

ب) 34

ج) 17

د) 7

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۱۰. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۱۱. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه شبکه

ب) لایه انتقال

ج) لایه پیوند داده

د) لایه کاربرد

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۱۲. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) P

ب) E

ج) S

د) F

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۱۳. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 5 ب) 4 ج) 6 د) 3

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۱۴. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod{n}$$

۱۵. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۱۶. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice ب) کلید عمومی Bob ج) کلید محرمانه Bob د) کلید عمومی Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۱۷. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۸. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۹. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به n اول باشد. ب) متن اصلی باید نسبت به n اول باشد.

ج) کلید عمومی باید نسبت به $\phi(n)$ اول باشد. د) متن اصلی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲۰. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۲۱. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۲. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice　　ب) کلید محرمانه Alice　　ج) کلید محرمانه Bob　　د) کلید عمومی Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲۳. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن آشکار - متن رمز شده　　ب) گمراه کنندگی - متن رمز شده - متن آشکار
ج) انتشار - متن رمز شده - متن آشکار　　د) گمراه کنندگی - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۲۴. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - آشکار - متن رمز　　ب) گمراه کنندگی - رمز - کلید
ج) انتشار - رمز - کلید　　د) انتشار - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۲۵. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 8　　ب) 6　　ج) 4　　د) 2

پاسخ: این عدد ریشه اولیه ندارد.

۲۶. رقم آخر عدد 3^{90} چند است؟

الف) 9　　ب) 8　　ج) 6　　د) 7

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.

- عدد سه و ده نسبت به هم اول هستند، یعنی $(3,10)=1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

✍ آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲۷. طول واقعی کلید DES برابر است با .....

الف) ۵۶ ب) ۳۲ ج) ۶۴ د) ۴۸

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۲۸. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۹. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۳۰. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 6 ب) 2 ج) 25 د) 27

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2\times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۱. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) F ب) P ج) E د) S

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۳. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۴. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice ب) کلید عمومی Bob ج) کلید محرمانه Bob د) کلید عمومی Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۵. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۶. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) انتشار - آشکار - متن رمز ب) گمراه کنندگی - آشکار - متن رمز

ج) گمراه کنندگی - رمز - کلید د) انتشار - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۷. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۸. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله تسهیم راز است.
ب) همه گزینه‌ها صحیح است.
ج) یک مساله از نوع روش‌های غیرتعاملی است.
د) یک مساله از نوع اثبات دانایی صفر است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۹. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 2
ب) 8
ج) 4
د) 6

پاسخ: این عدد ریشه اولیه ندارد.

۱۰. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم
ب) حمله نوع اول
ج) هیچ‌کدام
د) حمله نوع سوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۱. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۱۲. رقم آخر عدد 3^{90} چند است؟

الف) 6
ب) 9
ج) 7
د) 8

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۱۳. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۱۴. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۱۵. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه انتقال　　ب) لایه کاربرد　　ج) لایه پیوند داده　　د) لایه شبکه

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۱۶. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۱۷. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۱۸. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم　　ب) حمله نوع سوم　　ج) هیچ‌کدام　　د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۹. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۰. طول واقعی کلید DES برابر است با .....

الف) ۵۶　　ب) ۶۴　　ج) ۳۲　　د) ۴۸

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۲۱. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 25 ب) 27 ج) 2 د) 6

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۲۲. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن آشکار - متن رمز شده
ب) انتشار - متن رمز شده - متن آشکار
ج) انتشار - متن آشکار - متن رمز شده
د) گمراه کنندگی - متن رمز شده - متن آشکار

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۲۳. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 5 ب) 3 ج) 6 د) 4

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۲۴. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۵. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۲۶. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob ب) کلید عمومی Alice ج) کلید محرمانه Alice د) کلید عمومی Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۲۷. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۲۸. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۲۹. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به $\phi(n)$ اول باشد.
ب) کلید عمومی باید نسبت به n اول باشد.
ج) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
د) متن اصلی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۳۰. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 34
ب) 10
ج) 17
د) 7

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۱. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۲. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 6 ب) 2 ج) 4 د) 8

پاسخ: این عدد ریشه اولیه ندارد.

۳. رقم آخر عدد 3^{90} چند است؟

الف) 9 ب) 8 ج) 7 د) 6

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۴. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۵. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم ب) هیچ‌کدام ج) حمله نوع اول د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۶. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۷. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 2 ب) 25 ج) 6 د) 27

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۸. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) S ب) E ج) F د) P

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۹. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۱۰. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 17 ب) 7 ج) 34 د) 10

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۱۱. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۲. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۳. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به n اول باشد.

ب) متن اصلی باید نسبت به $\phi(n)$ اول باشد.

ج) متن اصلی باید نسبت به n اول باشد.

د) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۱۴. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 4 ب) 6 ج) 3 د) 5

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۱۵. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۱۶. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۷. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۱۸. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم ب) هیچ‌کدام ج) حمله نوع دوم د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۹. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) انتشار - رمز - کلید
ب) گمراه کنندگی - رمز - کلید
ج) گمراه کنندگی - آشکار - متن رمز
د) انتشار - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۲۰. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice
ب) کلید محرمانه Alice
ج) کلید عمومی Bob
د) کلید محرمانه Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۲۱. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۲۲. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله از نوع روش‌های غیرتعاملی است.
ب) همه گزینه‌ها صحیح است.
ج) یک مساله از نوع اثبات دانایی صفر است.
د) یک مساله تسهیم راز است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۲۳. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا
ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا
ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن
د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۲۴. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH

- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۲۵. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن رمز شده - متن آشکار
ب) انتشار - متن آشکار - متن رمز شده
ج) انتشار - متن رمز شده - متن آشکار
د) گمراه کنندگی - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۲۶. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۷. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۸. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob
ب) کلید محرمانه Alice
ج) کلید عمومی Bob
د) کلید عمومی Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲۹. طول واقعی کلید DES برابر است با .....

الف) ۳۲
ب) ۶۴
ج) ۴۸
د) ۵۶

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۳۰. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه کاربرد
ب) لایه پیوند داده
ج) لایه انتقال
د) لایه شبکه

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۱. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۳. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) S　　ب) F　　ج) E　　د) P

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۴. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۵. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۶. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Bob　　ب) کلید محرمانه Bob　　ج) کلید عمومی Alice　　د) کلید محرمانه Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۷. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob　　ب) کلید عمومی Bob　　ج) کلید محرمانه Alice　　د) کلید عمومی Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۸. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۹. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 4 ب) 2 ج) 8 د) 6

پاسخ: این عدد ریشه اولیه ندارد.

۱۰. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۱. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) انتشار - آشکار - متن رمز ب) انتشار - رمز - کلید
ج) گمراه کنندگی - رمز - کلید د) گمراه کنندگی - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۱۲. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول ب) حمله نوع سوم ج) هیچ‌کدام د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۳. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۱۴. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۱۵. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم　　ب) حمله نوع اول　　ج) حمله نوع دوم　　د) هیچ‌کدام

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۶. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۱۷. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن آشکار - متن رمز شده　　ب) گمراه کنندگی - متن رمز شده - متن آشکار

ج) انتشار - متن رمز شده - متن آشکار　　د) گمراه کنندگی - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۱۸. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۹. در SSH چگونه از حمله تغییر قابلیت‌های مشترک نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۲۰. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه شبکه　　ب) لایه پیوند داده　　ج) لایه انتقال　　د) لایه کاربرد

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۲۱. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 5　　ب) 6　　ج) 4　　د) 3

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۲۲. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۳. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod{n}$$

۲۴. رقم آخر عدد 3^{90} چند است؟

الف) 7 ب) 6 ج) 9 د) 8

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲۵. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
ب) متن اصلی باید نسبت به n اول باشد.
ج) کلید عمومی باید نسبت به n اول باشد.
د) متن اصلی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲۶. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله از نوع روش‌های غیرتعاملی است.
ب) یک مساله از نوع اثبات دانایی صفر است.
ج) یک مساله تسهیم راز است.
د) همه گزینه‌ها صحیح است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۲۷. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 2
ب) 6
ج) 25
د) 27

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۲۸. طول واقعی کلید DES برابر است با .....

الف) ۴۸
ب) ۳۲
ج) ۶۴
د) ۵۶

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۲۹. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.
ب) کلید باید به صورت کاملا تصادفی تولید شود.
ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.
د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۳۰. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 17
ب) 7
ج) 34
د) 10

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

نام و نام خانوادگی	شماره دانشجویی	نام درس	تاریخ	شماره برگه
		امنیت سیستم‌های کامپیوتری	۱۴۰۳/۰۲/۱۱	۱۰

۱. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله از نوع اثبات دانایی صفر است.
ب) یک مساله از نوع روش‌های غیرتعاملی است.
ج) یک مساله تسهیم راز است.
د) همه گزینه‌ها صحیح است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۲. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه انتقال
ب) لایه پیوند داده
ج) لایه شبکه
د) لایه کاربرد

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۳. طول واقعی کلید DES برابر است با .....

الف) ۵۶
ب) ۶۴
ج) ۳۲
د) ۴۸

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۴. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob
ب) کلید عمومی Alice
ج) کلید عمومی Bob
د) کلید محرمانه Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۵. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن رمز شده - متن آشکار
ب) گمراه کنندگی - متن آشکار - متن رمز شده
ج) انتشار - متن آشکار - متن رمز شده
د) انتشار - متن رمز شده - متن آشکار

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۶. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۷. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۸. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) E　　ب) P　　ج) S　　د) F

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۹. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۰. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - رمز - کلید　　ب) انتشار - رمز - کلید

ج) انتشار - آشکار - متن رمز　　د) گمراه کنندگی - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۱۱. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 10　　ب) 7　　ج) 34　　د) 17

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۱۲. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۱۳. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۴. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۱۵. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۶. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۷. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۱۸. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۹. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به n اول باشد.

ب) کلید عمومی باید نسبت به n اول باشد.

ج) متن اصلی باید نسبت به $\phi(n)$ اول باشد.

د) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲۰. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 2

ب) 27

ج) 6

د) 25

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۲۱. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 6

ب) 5

ج) 3

د) 4

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۲۲. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۲۳. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۲۴. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۲۵. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام　　ب) حمله نوع سوم　　ج) حمله نوع اول　　د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۶. در SSH چگونه از حمله تغییر قابلیت‌های مشترک نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH

- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۲۷. رقم آخر عدد 3^{90} چند است؟

الف) 8 ب) 9 ج) 6 د) 7

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲۸. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 4 ب) 2 ج) 6 د) 8

پاسخ: این عدد ریشه اولیه ندارد.

۲۹. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice ب) کلید عمومی Bob ج) کلید محرمانه Bob د) کلید محرمانه Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۳۰. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول ب) هیچ‌کدام ج) حمله نوع سوم د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به n اول باشد.
ب) متن اصلی باید نسبت به $\phi(n)$ اول باشد.
ج) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
د) کلید عمومی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۳. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۴. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۵. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - رمز - کلید
ب) انتشار - آشکار - متن رمز
ج) گمراه کنندگی - آشکار - متن رمز
د) انتشار - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۶. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۷. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۸. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۹. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Bob ب) کلید محرمانه Bob ج) کلید عمومی Alice د) کلید محرمانه Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۱۰. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۱. طول واقعی کلید DES برابر است با .....

الف) ۴۸ ب) ۵۶ ج) ۳۲ د) ۶۴

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۱۲. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۳. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۴. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 5 ب) 3 ج) 4 د) 6

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۱۵. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۱۶. رقم آخر عدد 3^{90} چند است؟

الف) 6 ب) 9 ج) 8 د) 7

پاسخ: ✍ دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

✍ آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۱۷. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 2 ب) 6 ج) 25 د) 27

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۱۸. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن رمز شده - متن آشکار
ب) گمراه کنندگی - متن آشکار - متن رمز شده
ج) انتشار - متن آشکار - متن رمز شده
د) انتشار - متن رمز شده - متن آشکار

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۱۹. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice ب) کلید محرمانه Alice ج) کلید محرمانه Bob د) کلید عمومی Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲۰. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۲۱. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم ب) هیچ‌کدام ج) حمله نوع سوم د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۲. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه شبکه ب) لایه انتقال ج) لایه کاربرد د) لایه پیوند داده

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۲۳. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) همه گزینه‌ها صحیح است. ب) یک مساله از نوع اثبات دانایی صفر است.
ج) یک مساله از نوع روش‌های غیرتعاملی است. د) یک مساله تسهیم راز است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۲۴. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.
ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.
ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.
د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۲۵. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 2 ب) 8 ج) 6 د) 4

پاسخ: این عدد ریشه اولیه ندارد.

۲۶. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا
ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا
ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن
د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۲۷. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۲۸. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) F ب) S ج) P د) E

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۲۹. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 34 ب) 17 ج) 7 د) 10

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۳۰. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول ب) هیچ‌کدام ج) حمله نوع دوم د) حمله نوع سوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 6 ب) 5 ج) 3 د) 4

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۲. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۳. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه پیوند داده ب) لایه شبکه ج) لایه کاربرد د) لایه انتقال

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۴. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) همه گزینه‌ها صحیح است. ب) یک مساله تسهیم راز است.
ج) یک مساله از نوع اثبات دانایی صفر است. د) یک مساله از نوع روش‌های غیرتعاملی است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۵. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم　　ب) حمله نوع دوم　　ج) هیچ‌کدام　　د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۶. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۷. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به $\phi(n)$ اول باشد.　　ب) کلید عمومی باید نسبت به n اول باشد.

ج) متن اصلی باید نسبت به n اول باشد.　　د) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۸. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob　　ب) کلید عمومی Alice　　ج) کلید محرمانه Alice　　د) کلید عمومی Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۹. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۱۰. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۱۱. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) F　　ب) E　　ج) P　　د) S

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۱۲. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.
ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.
ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.
د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۱۳. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۱۴. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 4 ب) 8 ج) 6 د) 2

پاسخ: این عدد ریشه اولیه ندارد.

۱۵. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۱۶. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن رمز شده - متن آشکار
ب) گمراه کنندگی - متن رمز شده - متن آشکار
ج) گمراه کنندگی - متن آشکار - متن رمز شده
د) انتشار - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۱۷. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.
ب) کلید باید به صورت کاملا تصادفی تولید شود.
ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.
د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۸. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۹. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - رمز - کلید
ب) گمراه کنندگی - آشکار - متن رمز
ج) انتشار - آشکار - متن رمز
د) انتشار - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۲۰. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۱. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice
ب) کلید محرمانه Alice
ج) کلید محرمانه Bob
د) کلید عمومی Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۲۲. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 7
ب) 34
ج) 17
د) 10

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۲۳. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 2
ب) 27
ج) 6
د) 25

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۲۴. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۲۵. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم
ب) حمله نوع سوم
ج) هیچ‌کدام
د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۶. رقم آخر عدد 3^{90} چند است؟

الف) 6 ب) 8 ج) 9 د) 7

پاسخ: ✍ دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

✍ آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲۷. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۸. طول واقعی کلید DES برابر است با .....

الف) ۴۸ ب) ۵۶ ج) ۶۴ د) ۳۲

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۲۹. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۳۰. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod{n}$$

۱. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob ب) کلید عمومی Bob ج) کلید عمومی Alice د) کلید محرمانه Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۲. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) همه گزینه‌ها صحیح است. ب) یک مساله تسهیم راز است.
ج) یک مساله از نوع روش‌های غیرتعاملی است. د) یک مساله از نوع اثبات دانایی صفر است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۳. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن رمز شده - متن آشکار ب) انتشار - متن آشکار - متن رمز شده
ج) انتشار - متن رمز شده - متن آشکار د) گمراه کنندگی - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۴. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۵. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم ب) حمله نوع سوم ج) حمله نوع اول د) هیچ‌کدام

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۶. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۷. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.
ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$
د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۸. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم　　ب) حمله نوع دوم　　ج) هیچ‌کدام　　د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۹. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۱۰. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۱۱. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۱۲. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) E　　ب) F　　ج) P　　د) S

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۱۳. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۴. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice　　ب) کلید محرمانه Alice　　ج) کلید عمومی Bob　　د) کلید محرمانه Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۱۵. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۶. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۱۷. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۱۸. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 4 ب) 2 ج) 6 د) 8

پاسخ: این عدد ریشه اولیه ندارد.

۱۹. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه شبکه ب) لایه کاربرد ج) لایه انتقال د) لایه پیوند داده

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۲۰. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۲۱. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۲۲. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۳. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 34 ب) 10 ج) 17 د) 7

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۲۴. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۲۵. رقم آخر عدد 3^{90} چند است؟

الف) 6 ب) 7 ج) 8 د) 9

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲۶. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 5 ب) 3 ج) 4 د) 6

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۲۷. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به n اول باشد.
ب) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
ج) متن اصلی باید نسبت به $\phi(n)$ اول باشد.
د) متن اصلی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲۸. طول واقعی کلید DES برابر است با .....

الف) ۴۸
ب) ۵۶
ج) ۳۲
د) ۶۴

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۲۹. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 25
ب) 2
ج) 27
د) 6

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۳۰. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) انتشار - رمز - کلید
ب) انتشار - آشکار - متن رمز
ج) گمراه کنندگی - آشکار - متن رمز
د) گمراه کنندگی - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۱. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به n اول باشد.
ب) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
ج) کلید عمومی باید نسبت به n اول باشد.
د) متن اصلی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲. طول واقعی کلید DES برابر است با .....

الف) ۴۸
ب) ۶۴
ج) ۵۶
د) ۳۲

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۳. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۴. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.
ب) کلید باید به صورت کاملا تصادفی تولید شود.
ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.
د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۵. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - آشکار - متن رمز
ب) انتشار - رمز - کلید
ج) انتشار - آشکار - متن رمز
د) گمراه کنندگی - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۶. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 4
ب) 6
ج) 5
د) 3

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۷. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۸. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 27 ب) 25 ج) 2 د) 6

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۹. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 6 ب) 4 ج) 8 د) 2

پاسخ: این عدد ریشه اولیه ندارد.

۱۰. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۱۱. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod{n}$$

۱۲. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice ب) کلید عمومی Bob ج) کلید عمومی Alice د) کلید محرمانه Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۱۳. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه شبکه ب) لایه کاربرد ج) لایه انتقال د) لایه پیوند داده

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۱۴. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob ب) کلید محرمانه Alice ج) کلید عمومی Alice د) کلید عمومی Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۱۵. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) S ب) P ج) F د) E

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۱۶. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن رمز شده - متن آشکار ب) انتشار - متن آشکار - متن رمز شده
ج) انتشار - متن رمز شده - متن آشکار د) گمراه کنندگی - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۱۷. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.
ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$
د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۱۸. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۹. رقم آخر عدد 3^{90} چند است؟

الف) 8 ب) 6 ج) 7 د) 9

پاسخ: ✍ دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲۰. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۲۱. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم　　ب) هیچ‌کدام　　ج) حمله نوع سوم　　د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۲. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۳. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۲۴. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۲۵. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم　　ب) حمله نوع دوم　　ج) حمله نوع اول　　د) هیچ‌کدام

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۶. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۲۷. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله از نوع روش‌های غیرتعاملی است.　　ب) یک مساله از نوع اثبات دانایی صفر است.

ج) یک مساله تسهیم راز است.　　د) همه گزینه‌ها صحیح است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۲۸. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 10　　ب) 34　　ج) 7　　د) 17

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۲۹. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۳۰. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice　　ب) کلید عمومی Bob　　ج) کلید محرمانه Alice　　د) کلید محرمانه Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 25　　ب) 2　　ج) 6　　د) 27

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۳. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 34　　ب) 10　　ج) 7　　د) 17

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۴. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۵. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به $\phi(n)$ اول باشد.　　ب) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.

ج) کلید عمومی باید نسبت به n اول باشد.　　د) متن اصلی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۶. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice　　ب) کلید عمومی Alice　　ج) کلید عمومی Bob　　د) کلید محرمانه Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۷. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۸. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) انتشار - رمز - کلید
ب) انتشار - آشکار - متن رمز
ج) گمراه کنندگی - رمز - کلید
د) گمراه کنندگی - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۹. طول واقعی کلید DES برابر است با .....

الف) ۵۶
ب) ۶۴
ج) ۳۲
د) ۴۸

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۱۰. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۱۱. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۱۲. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۱۳. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۴. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم　　ب) هیچ‌کدام　　ج) حمله نوع دوم　　د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۵. در SSH چگونه از حمله تغییر قابلیت‌های مشترک نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۱۶. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) P　　ب) S　　ج) E　　د) F

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۱۷. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۱۸. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۹. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه شبکه　　ب) لایه کاربرد　　ج) لایه پیوند داده　　د) لایه انتقال

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۲۰. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۲۱. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۲۲. رقم آخر عدد 3^{90} چند است؟

الف) 7 ب) 8 ج) 9 د) 6

پاسخ: ✍ دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

✍ آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲۳. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم ب) هیچ‌کدام ج) حمله نوع سوم د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۴. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن آشکار - متن رمز شده ب) گمراه کنندگی - متن آشکار - متن رمز شده
ج) گمراه کنندگی - متن رمز شده - متن آشکار د) انتشار - متن رمز شده - متن آشکار

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۲۵. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 5 ب) 6 ج) 4 د) 3

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۲۶. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۲۷. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) همه گزینه‌ها صحیح است.

ب) یک مساله از نوع اثبات دانایی صفر است.

ج) یک مساله از نوع روش‌های غیرتعاملی است.

د) یک مساله تسهیم راز است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۲۸. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۲۹. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 2

ب) 4

ج) 6

د) 8

پاسخ: این عدد ریشه اولیه ندارد.

۳۰. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۲. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 17 ب) 34 ج) 10 د) 7

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۳. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice ب) کلید محرمانه Alice ج) کلید محرمانه Bob د) کلید عمومی Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۴. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۵. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۶. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۷. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۸. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۹. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن رمز شده - متن آشکار

ب) انتشار - متن آشکار - متن رمز شده

ج) گمراه کنندگی - متن آشکار - متن رمز شده

د) انتشار - متن رمز شده - متن آشکار

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۱۰. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۱۱. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 5 ب) 4 ج) 3 د) 6

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۱۲. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۳. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۱۴. طول واقعی کلید DES برابر است با .....

الف) ۳۲ ب) ۶۴ ج) ۵۶ د) ۴۸

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۱۵. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۶. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) E ب) F ج) P د) S

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۱۷. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 4 ب) 8 ج) 6 د) 2

پاسخ: این عدد ریشه اولیه ندارد.

۱۸. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - رمز - کلید

ب) گمراه کنندگی - آشکار - متن رمز

ج) انتشار - آشکار - متن رمز

د) انتشار - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۱۹. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) همه گزینه‌ها صحیح است.

ب) یک مساله از نوع اثبات دانایی صفر است.

ج) یک مساله از نوع روش‌های غیرتعاملی است.

د) یک مساله تسهیم راز است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۲۰. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه پیوند داده　　ب) لایه انتقال　　ج) لایه شبکه　　د) لایه کاربرد

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۲۱. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم　　ب) حمله نوع سوم　　ج) حمله نوع اول　　د) هیچ‌کدام

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۲. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۳. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob　　ب) کلید محرمانه Alice　　ج) کلید عمومی Alice　　د) کلید عمومی Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲۴. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم　　ب) هیچ‌کدام　　ج) حمله نوع دوم　　د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۵. رقم آخر عدد 3^{90} چند است؟

الف) 6　　ب) 8　　ج) 9　　د) 7

پاسخ: ✍ دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

✍ آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲۶. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به n اول باشد.　　ب) متن اصلی باید نسبت به $\phi(n)$ اول باشد.

ج) متن اصلی باید نسبت به n اول باشد.　　د) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲۷. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 25 ب) 2 ج) 27 د) 6

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۲۸. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۲۹. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right) \left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۳۰. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۱. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه شبکه　　ب) لایه پیوند داده　　ج) لایه انتقال　　د) لایه کاربرد

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۳. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۴. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۵. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 6　　ب) 5　　ج) 4　　د) 3

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۶. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول　　ب) حمله نوع سوم　　ج) هیچ‌کدام　　د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۷. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۸. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۹. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۱۰. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به n اول باشد.
ب) کلید عمومی باید نسبت به n اول باشد.
ج) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
د) متن اصلی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۱۱. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۱۲. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن رمز شده - متن آشکار
ب) گمراه کنندگی - متن آشکار - متن رمز شده
ج) انتشار - متن آشکار - متن رمز شده
د) انتشار - متن رمز شده - متن آشکار

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۱۳. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۱۴. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) همه گزینه‌ها صحیح است.
ب) یک مساله از نوع اثبات دانایی صفر است.
ج) یک مساله تسهیم راز است.
د) یک مساله از نوع روش‌های غیرتعاملی است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۱۵. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام
ب) حمله نوع سوم
ج) حمله نوع اول
د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۶. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا
ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا
ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن
د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۱۷. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - آشکار - متن رمز
ب) انتشار - آشکار - متن رمز
ج) انتشار - رمز - کلید
د) گمراه کنندگی - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۱۸. در SSH چگونه از حمله تغییر قابلیت‌های مشترک نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init

- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۱۹. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Bob　　ب) کلید محرمانه Bob　　ج) کلید عمومی Alice　　د) کلید محرمانه Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۲۰. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 7　　ب) 10　　ج) 34　　د) 17

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۲۱. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۲. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۳. رقم آخر عدد 3^{90} چند است؟

الف) 8　　ب) 6　　ج) 9　　د) 7

پاسخ: ✍ دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

✍ آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲۴. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۲۵. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 8 ب) 6 ج) 2 د) 4

پاسخ: این عدد ریشه اولیه ندارد.

۲۶. طول واقعی کلید DES برابر است با .....

الف) ۴۸ ب) ۵۶ ج) ۳۲ د) ۶۴

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۲۷. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) S ب) E ج) P د) F

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۲۸. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice ب) کلید محرمانه Alice ج) کلید عمومی Bob د) کلید محرمانه Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲۹. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 6 ب) 27 ج) 2 د) 25

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۳۰. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۲. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله از نوع اثبات دانایی صفر است.

ب) یک مساله از نوع روش‌های غیرتعاملی است.

ج) یک مساله تسهیم راز است.

د) همه گزینه‌ها صحیح است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۳. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۴. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) F

ب) P

ج) E

د) S

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۵. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 4

ب) 6

ج) 3

د) 5

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۶. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
ب) متن اصلی باید نسبت به n اول باشد.
ج) متن اصلی باید نسبت به $\phi(n)$ اول باشد.
د) کلید عمومی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۷. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم
ب) حمله نوع دوم
ج) هیچ‌کدام
د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۸. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - آشکار - متن رمز
ب) انتشار - آشکار - متن رمز
ج) انتشار - رمز - کلید
د) گمراه کنندگی - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۹. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۱۰. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۱. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 6
ب) 2
ج) 27
د) 25

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۱۲. رقم آخر عدد 3^{90} چند است؟

الف) 8 ب) 7 ج) 9 د) 6

پاسخ: ✍ دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

✍ آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۱۳. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۱۴. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۱۵. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۶. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه شبکه ب) لایه انتقال ج) لایه کاربرد د) لایه پیوند داده

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۱۷. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول ب) حمله نوع سوم ج) هیچ‌کدام د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۸. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۱۹. طول واقعی کلید DES برابر است با .....

الف) ۳۲ ب) ۶۴ ج) ۵۶ د) ۴۸

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۲۰. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۲۱. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۲۲. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 17 ب) 10 ج) 34 د) 7

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۲۳. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 2 ب) 8 ج) 4 د) 6

پاسخ: این عدد ریشه اولیه ندارد.

۲۴. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن رمز شده - متن آشکار
ب) انتشار - متن رمز شده - متن آشکار
ج) گمراه کنندگی - متن آشکار - متن رمز شده
د) انتشار - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۲۵. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۲۶. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۷. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۲۸. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Bob
ب) کلید محرمانه Alice
ج) کلید عمومی Alice
د) کلید محرمانه Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲۹. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob
ب) کلید محرمانه Alice
ج) کلید عمومی Bob
د) کلید عمومی Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۳۰. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم　　ب) حمله نوع دوم　　ج) هیچ‌کدام　　د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 10　　ب) 7　　ج) 34　　د) 17

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۳. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۴. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۵. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله از نوع روش‌های غیرتعاملی است.　　ب) یک مساله تسهیم راز است.

ج) یک مساله از نوع اثبات دانایی صفر است.　　د) همه گزینه‌ها صحیح است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۶. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 5　　ب) 6　　ج) 4　　د) 3

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۷. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 8 ب) 2 ج) 6 د) 4

پاسخ: این عدد ریشه اولیه ندارد.

۸. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۹. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم ب) حمله نوع اول ج) حمله نوع سوم د) هیچ‌کدام

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۰. در SSH چگونه از حمله تغییر قابلیت‌های مشترک نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۱۱. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۱۲. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - رمز - کلید ب) انتشار - رمز - کلید
ج) انتشار - آشکار - متن رمز د) گمراه کنندگی - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۱۳. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به n اول باشد.
ب) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
ج) متن اصلی باید نسبت به n اول باشد.
د) متن اصلی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۱۴. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۵. کدام گزینه در مورد PGP صحیح است؟
الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا
ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا
ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن
د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۱۶. طول واقعی کلید DES برابر است با .....

الف) ۴۸ ب) ۵۶ ج) ۳۲ د) ۶۴

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۱۷. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice ب) کلید محرمانه Bob ج) کلید عمومی Bob د) کلید عمومی Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۱۸. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) S ب) E ج) P د) F

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۱۹. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟
الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.
ب) کلید باید به صورت کاملا تصادفی تولید شود.
ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.
د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۲۰. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۲۱. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن آشکار - متن رمز شده

ب) گمراه کنندگی - متن رمز شده - متن آشکار

ج) انتشار - متن رمز شده - متن آشکار

د) گمراه کنندگی - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۲۲. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۲۳. رقم آخر عدد 3^{90} چند است؟

الف) 6 ب) 7 ج) 8 د) 9

پاسخ: ✍ دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

✍ آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲۴. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۵. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۲۶. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۷. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۲۸. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه شبکه　　ب) لایه کاربرد　　ج) لایه انتقال　　د) لایه پیوند داده

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۲۹. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob　　ب) کلید محرمانه Alice　　ج) کلید عمومی Bob　　د) کلید عمومی Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۳۰. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 2　　ب) 6　　ج) 27　　د) 25

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۱. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) انتشار - رمز - کلید
ب) گمراه کنندگی - رمز - کلید
ج) انتشار - آشکار - متن رمز
د) گمراه کنندگی - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۲. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Bob
ب) کلید محرمانه Bob
ج) کلید محرمانه Alice
د) کلید عمومی Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۳. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۴. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن آشکار - متن رمز شده
ب) گمراه کنندگی - متن آشکار - متن رمز شده
ج) انتشار - متن رمز شده - متن آشکار
د) گمراه کنندگی - متن رمز شده - متن آشکار

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۵. رقم آخر عدد 3^{90} چند است؟

الف) 8
ب) 6
ج) 7
د) 9

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۶. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۷. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۸. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 8 ب) 4 ج) 2 د) 6

پاسخ: این عدد ریشه اولیه ندارد.

۹. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به n اول باشد.
ب) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
ج) متن اصلی باید نسبت به n اول باشد.
د) متن اصلی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۱۰. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله از نوع روش‌های غیرتعاملی است.
ب) همه گزینه‌ها صحیح است.
ج) یک مساله از نوع اثبات دانایی صفر است.
د) یک مساله تسهیم راز است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۱۱. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice ب) کلید محرمانه Bob ج) کلید عمومی Alice د) کلید عمومی Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۱۲. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه انتقال ب) لایه پیوند داده ج) لایه کاربرد د) لایه شبکه

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۱۳. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۴. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 4 ب) 6 ج) 3 د) 5

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۱۵. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 2 ب) 27 ج) 6 د) 25

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۱۶. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod{n}$$

۱۷. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۸. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۱۹. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) P ب) S ج) E د) F

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۲۰. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۲۱. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم ب) هیچ‌کدام ج) حمله نوع سوم د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۲. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۲۳. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۴. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۲۵. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 34 ب) 17 ج) 7 د) 10

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۲۶. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۲۷. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم　　ب) حمله نوع اول　　ج) حمله نوع دوم　　د) هیچ‌کدام

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۸. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۲۹. طول واقعی کلید DES برابر است با .....

الف) ۳۲　　ب) ۶۴　　ج) ۴۸　　د) ۵۶

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۳۰. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۱. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
ب) متن اصلی باید نسبت به $\phi(n)$ اول باشد.
ج) کلید عمومی باید نسبت به n اول باشد.
د) متن اصلی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۳. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا
ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا
ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن
د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۴. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 8 ب) 2 ج) 4 د) 6

پاسخ: این عدد ریشه اولیه ندارد.

۵. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۶. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۷. رقم آخر عدد 3^{90} چند است؟

الف) 6 ب) 7 ج) 8 د) 9

پاسخ: ✍ دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

✍ آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۸. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۹. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۱۰. در SSH چگونه از حمله تغییر قابلیت‌های مشترک نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۱۱. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله تسهیم راز است.
ب) همه گزینه‌ها صحیح است.
ج) یک مساله از نوع روش‌های غیرتعاملی است.
د) یک مساله از نوع اثبات دانایی صفر است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۱۲. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم
ب) هیچ‌کدام
ج) حمله نوع دوم
د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۳. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.
ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.
ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.
د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۱۴. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 17
ب) 7
ج) 10
د) 34

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۱۵. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه کاربرد
ب) لایه انتقال
ج) لایه پیوند داده
د) لایه شبکه

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۱۶. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.
ب) کلید باید به صورت کاملا تصادفی تولید شود.
ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.
د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۷. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob
ب) کلید محرمانه Alice
ج) کلید عمومی Alice
د) کلید عمومی Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۱۸. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۱۹. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice　　ب) کلید عمومی Bob　　ج) کلید محرمانه Alice　　د) کلید محرمانه Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۲۰. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۲۱. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن آشکار - متن رمز شده　　ب) انتشار - متن رمز شده - متن آشکار
ج) گمراه کنندگی - متن رمز شده - متن آشکار　　د) گمراه کنندگی - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۲۲. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول　　ب) حمله نوع سوم　　ج) حمله نوع دوم　　د) هیچ‌کدام

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۳. طول واقعی کلید DES برابر است با .....

الف) ۶۴　　ب) ۵۶　　ج) ۴۸　　د) ۳۲

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۲۴. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۵. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) E　　ب) P　　ج) S　　د) F

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۲۶. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

- ه سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- و دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۲۷. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - رمز - کلید
ب) گمراه کنندگی - آشکار - متن رمز
ج) انتشار - آشکار - متن رمز
د) انتشار - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۲۸. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 25
ب) 6
ج) 2
د) 27

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۲۹. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 3
ب) 6
ج) 5
د) 4

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۳۰. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) F　　ب) S　　ج) P　　د) E

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۲. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۳. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن رمز شده - متن آشکار　　ب) انتشار - متن آشکار - متن رمز شده

ج) گمراه کنندگی - متن رمز شده - متن آشکار　　د) گمراه کنندگی - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۴. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به n اول باشد.　　ب) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.

ج) متن اصلی باید نسبت به n اول باشد.　　د) متن اصلی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۵. در SSH چگونه از حمله تغییر قابلیت‌های مشترک نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init

- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۶. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) انتشار - آشکار - متن رمز
ب) گمراه کنندگی - رمز - کلید
ج) انتشار - رمز - کلید
د) گمراه کنندگی - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۷. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۸. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله از نوع روش‌های غیرتعاملی است.
ب) یک مساله تسهیم راز است.
ج) یک مساله از نوع اثبات دانایی صفر است.
د) همه گزینه‌ها صحیح است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۹. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۰. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۱. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام
ب) حمله نوع دوم
ج) حمله نوع سوم
د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۲. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۱۳. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.
ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.
ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.
د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۱۴. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Bob
ب) کلید عمومی Alice
ج) کلید محرمانه Alice
د) کلید محرمانه Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۱۵. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 2 ب) 6 ج) 4 د) 8

پاسخ: این عدد ریشه اولیه ندارد.

۱۶. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۷. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 34 ب) 10 ج) 7 د) 17

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۱۸. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم ب) هیچ‌کدام ج) حمله نوع اول د) حمله نوع سوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۹. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۲۰. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 27 ب) 6 ج) 2 د) 25

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۲۱. طول واقعی کلید DES برابر است با .....

الف) ۳۲ ب) ۴۸ ج) ۶۴ د) ۵۶

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۲۲. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.

- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۲۳. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob　　ب) کلید عمومی Bob　　ج) کلید عمومی Alice　　د) کلید محرمانه Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۲۴. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۲۵. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۲۶. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه کاربرد　　ب) لایه پیوند داده　　ج) لایه انتقال　　د) لایه شبکه

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۲۷. رقم آخر عدد 3^{90} چند است؟

الف) 9　　ب) 6　　ج) 7　　د) 8

پاسخ: ✍ دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

✍ آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲۸. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 6 ب) 5 ج) 4 د) 3

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۲۹. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۳۰. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod{n}$$

۱. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) انتشار - آشکار - متن رمز
ب) گمراه کنندگی - رمز - کلید
ج) انتشار - رمز - کلید
د) گمراه کنندگی - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۲. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 25
ب) 2
ج) 27
د) 6

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۳. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله از نوع روش‌های غیرتعاملی است.
ب) یک مساله تسهیم راز است.
ج) یک مساله از نوع اثبات دانایی صفر است.
د) همه گزینه‌ها صحیح است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۴. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۵. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.
ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.
ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.
د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۶. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه پیوند داده　　ب) لایه انتقال　　ج) لایه شبکه　　د) لایه کاربرد

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۷. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن آشکار - متن رمز شده　　ب) گمراه کنندگی - متن رمز شده - متن آشکار
ج) انتشار - متن آشکار - متن رمز شده　　د) انتشار - متن رمز شده - متن آشکار

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۸. طول واقعی کلید DES برابر است با .....

الف) ۴۸　　ب) ۵۶　　ج) ۳۲　　د) ۶۴

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۹. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۱۰. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) S　　ب) F　　ج) E　　د) P

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۱۱. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به n اول باشد.　　ب) کلید عمومی باید نسبت به n اول باشد.
ج) متن اصلی باید نسبت به $\phi(n)$ اول باشد.　　د) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۱۲. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۱۳. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 6 ب) 8 ج) 2 د) 4

پاسخ: این عدد ریشه اولیه ندارد.

۱۴. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۱۵. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۱۶. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۷. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice ب) کلید عمومی Bob ج) کلید محرمانه Alice د) کلید محرمانه Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۱۸. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Bob ب) کلید محرمانه Alice ج) کلید محرمانه Bob د) کلید عمومی Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۱۹. رقم آخر عدد 3^{90} چند است؟

الف) 7 ب) 9 ج) 8 د) 6

پاسخ: ✍ دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

✍ آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲۰. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۱. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام　　ب) حمله نوع سوم　　ج) حمله نوع دوم　　د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۲. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 6　　ب) 5　　ج) 4　　د) 3

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۲۳. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۲۴. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول　　ب) حمله نوع دوم　　ج) هیچ‌کدام　　د) حمله نوع سوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۵. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.
ب) کلید باید به صورت کاملا تصادفی تولید شود.
ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.
د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود،

نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۲۶. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 17 ب) 34 ج) 7 د) 10

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۲۷. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۲۸. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۹. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۳۰. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۱. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 34 ب) 7 ج) 10 د) 17

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۲. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۳. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) انتشار - رمز - کلید ب) انتشار - آشکار - متن رمز

ج) گمراه کنندگی - رمز - کلید د) گمراه کنندگی - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۴. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۵. طول واقعی کلید DES برابر است با .....

الف) ۵۶ ب) ۴۸ ج) ۶۴ د) ۳۲

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۶. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۷. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم　　ب) حمله نوع اول　　ج) حمله نوع دوم　　د) هیچ‌کدام

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۸. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه کاربرد　　ب) لایه پیوند داده　　ج) لایه شبکه　　د) لایه انتقال

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۹. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۱۰. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن رمز شده - متن آشکار　　ب) انتشار - متن آشکار - متن رمز شده
ج) انتشار - متن رمز شده - متن آشکار　　د) گمراه کنندگی - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۱۱. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۲. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول　　ب) حمله نوع دوم　　ج) هیچ‌کدام　　د) حمله نوع سوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۳. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۴. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.
ب) کلید باید به صورت کاملا تصادفی تولید شود.
ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۵. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۱۶. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 4 ب) 6 ج) 8 د) 2

پاسخ: این عدد ریشه اولیه ندارد.

۱۷. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله از نوع روش‌های غیرتعاملی است.
ب) یک مساله تسهیم راز است.
ج) همه گزینه‌ها صحیح است.
د) یک مساله از نوع اثبات دانایی صفر است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۱۸. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۹. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.
ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$
د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۲۰. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

- ه سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- و دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۲۱. رقم آخر عدد 3^{90} چند است؟

الف) 6 ب) 8 ج) 9 د) 7

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲۲. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Bob ب) کلید محرمانه Alice ج) کلید محرمانه Bob د) کلید عمومی Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲۳. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) E ب) P ج) F د) S

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۲۴. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice ب) کلید محرمانه Bob ج) کلید محرمانه Alice د) کلید عمومی Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۲۵. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 4 ب) 6 ج) 5 د) 3

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۲۶. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۷. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به n اول باشد.
ب) کلید عمومی باید نسبت به n اول باشد.
ج) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
د) متن اصلی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲۸. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۲۹. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 25
ب) 27
ج) 6
د) 2

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۳۰. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۱. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) F ب) P ج) S د) E

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۲. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۳. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 6 ب) 5 ج) 4 د) 3

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۴. طول واقعی کلید DES برابر است با .....

الف) ۳۲ ب) ۴۸ ج) ۶۴ د) ۵۶

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۵. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۶. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۷. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) همه گزینه‌ها صحیح است.
ب) یک مساله از نوع روش‌های غیرتعاملی است.
ج) یک مساله تسهیم راز است.
د) یک مساله از نوع اثبات دانایی صفر است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۸. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.
ب) کلید باید به صورت کاملا تصادفی تولید شود.
ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.
د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۹. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه پیوند داده
ب) لایه شبکه
ج) لایه کاربرد
د) لایه انتقال

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۱۰. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به n اول باشد.
ب) کلید عمومی باید نسبت به n اول باشد.
ج) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
د) متن اصلی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۱۱. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۲. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام
ب) حمله نوع سوم
ج) حمله نوع اول
د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۳. در SSH چگونه از حمله تغییر قابلیت‌های مشترک نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init

- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۱۴. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۵. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 2 ب) 6 ج) 8 د) 4

پاسخ: این عدد ریشه اولیه ندارد.

۱۶. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن آشکار - متن رمز شده
ب) گمراه کنندگی - متن آشکار - متن رمز شده
ج) انتشار - متن رمز شده - متن آشکار
د) گمراه کنندگی - متن رمز شده - متن آشکار

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۱۷. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا
ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا
ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن
د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۱۸. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.
ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.
ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.
د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۱۹. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۲۰. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 7 ب) 10 ج) 34 د) 17

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۲۱. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۲۲. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۲۳. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام ب) حمله نوع دوم ج) حمله نوع اول د) حمله نوع سوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۴. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob ب) کلید عمومی Alice ج) کلید عمومی Bob د) کلید محرمانه Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲۵. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۲۶. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 25 ب) 2 ج) 6 د) 27

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۲۷. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۸. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - آشکار - متن رمز
ب) انتشار - رمز - کلید
ج) گمراه کنندگی - رمز - کلید
د) انتشار - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۲۹. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice
ب) کلید محرمانه Bob
ج) کلید محرمانه Alice
د) کلید عمومی Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۳۰. رقم آخر عدد 3^{90} چند است؟

الف) 6 ب) 9 ج) 7 د) 8

پاسخ: ✍ دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

✍ آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۱. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲. طول واقعی کلید DES برابر است با .....

الف) ۶۴ ب) ۴۸ ج) ۳۲ د) ۵۶

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۳. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۴. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۵. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 6 ب) 2 ج) 25 د) 27

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۶. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۷. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) E　　ب) P　　ج) S　　د) F

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۸. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۹. رقم آخر عدد 3^{90} چند است؟

الف) 6　　ب) 7　　ج) 9　　د) 8

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۱۰. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۱۱. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۱۲. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۳. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) همه گزینه‌ها صحیح است.

ب) یک مساله تسهیم راز است.

ج) یک مساله از نوع اثبات دانایی صفر است.

د) یک مساله از نوع روش‌های غیرتعاملی است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۱۴. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه پیوند داده

ب) لایه انتقال

ج) لایه شبکه

د) لایه کاربرد

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۱۵. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 2

ب) 6

ج) 8

د) 4

پاسخ: این عدد ریشه اولیه ندارد.

۱۶. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به n اول باشد.

ب) متن اصلی باید نسبت به $\phi(n)$ اول باشد.

ج) کلید عمومی باید نسبت به n اول باشد.

د) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۱۷. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم　　ب) حمله نوع اول　　ج) حمله نوع دوم　　د) هیچ‌کدام

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۸. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 6　　ب) 3　　ج) 5　　د) 4

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۱۹. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول　　ب) هیچ‌کدام　　ج) حمله نوع سوم　　د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۰. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۱. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Bob　　ب) کلید عمومی Alice　　ج) کلید محرمانه Alice　　د) کلید محرمانه Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۲۲. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۳. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۲۴. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن رمز شده - متن آشکار　　ب) گمراه کنندگی - متن آشکار - متن رمز شده
ج) گمراه کنندگی - متن رمز شده - متن آشکار　　د) انتشار - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۲۵. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice　　ب) کلید محرمانه Bob　　ج) کلید عمومی Alice　　د) کلید عمومی Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲۶. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - آشکار - متن رمز
ب) انتشار - رمز - کلید
ج) انتشار - آشکار - متن رمز
د) گمراه کنندگی - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۲۷. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۸. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا
ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا
ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن
د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۲۹. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 10
ب) 17
ج) 7
د) 34

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۳۰. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۱. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله از نوع روش‌های غیرتعاملی است.
ب) یک مساله از نوع اثبات دانایی صفر است.
ج) همه گزینه‌ها صحیح است.
د) یک مساله تسهیم راز است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۲. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن رمز شده - متن آشکار
ب) گمراه کنندگی - متن رمز شده - متن آشکار
ج) انتشار - متن آشکار - متن رمز شده
د) گمراه کنندگی - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۳. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۴. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۵. طول واقعی کلید DES برابر است با .....

الف) ۳۲
ب) ۵۶
ج) ۴۸
د) ۶۴

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۶. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 7
ب) 10
ج) 34
د) 17

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۷. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۸. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۹. رقم آخر عدد 3^{90} چند است؟

الف) 9 ب) 8 ج) 7 د) 6

پاسخ: ✍ دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

✍ آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۱۰. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 27 ب) 6 ج) 2 د) 25

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۱۱. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۲. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول ب) هیچ‌کدام ج) حمله نوع سوم د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۳. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 6 ب) 2 ج) 4 د) 8

پاسخ: این عدد ریشه اولیه ندارد.

۱۴. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) انتشار - رمز - کلید ب) گمراه کنندگی - رمز - کلید

ج) انتشار - آشکار - متن رمز د) گمراه کنندگی - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۱۵. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۱۶. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۱۷. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۱۸. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۱۹. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۲۰. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۲۱. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۲۲. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به n اول باشد.
ب) متن اصلی باید نسبت به $\phi(n)$ اول باشد.
ج) کلید عمومی باید نسبت به n اول باشد.
د) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲۳. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) S
ب) P
ج) F
د) E

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۲۴. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice
ب) کلید محرمانه Bob
ج) کلید عمومی Bob
د) کلید عمومی Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲۵. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۲۶. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۷. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob　　ب) کلید عمومی Alice　　ج) کلید محرمانه Alice　　د) کلید عمومی Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۲۸. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام　　ب) حمله نوع دوم　　ج) حمله نوع اول　　د) حمله نوع سوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۹. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه پیوند داده　　ب) لایه انتقال　　ج) لایه کاربرد　　د) لایه شبکه

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۳۰. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 5　　ب) 4　　ج) 3　　د) 6

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۱. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - آشکار - متن رمز
ب) انتشار - رمز - کلید
ج) گمراه کنندگی - رمز - کلید
د) انتشار - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۲. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) F
ب) E
ج) S
د) P

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۳. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۴. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۵. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 8
ب) 4
ج) 2
د) 6

پاسخ: این عدد ریشه اولیه ندارد.

۶. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول
ب) حمله نوع دوم
ج) هیچ‌کدام
د) حمله نوع سوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۷. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.
ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.
ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.
د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۸. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob
ب) کلید محرمانه Alice
ج) کلید عمومی Alice
د) کلید عمومی Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۹. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا
ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۱۰. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 5 ب) 6 ج) 4 د) 3

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۱۱. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۲. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۱۳. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۴. رقم آخر عدد 3^{90} چند است؟

الف) 7 ب) 6 ج) 9 د) 8

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۱۵. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Bob　　ب) کلید محرمانه Bob　　ج) کلید عمومی Alice　　د) کلید محرمانه Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۱۶. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۷. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.　　ب) متن اصلی باید نسبت به $\phi(n)$ اول باشد.

ج) کلید عمومی باید نسبت به n اول باشد.　　د) متن اصلی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۱۸. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 25　　ب) 27　　ج) 6　　د) 2

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۱۹. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۲۰. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول　　ب) هیچ‌کدام　　ج) حمله نوع سوم　　د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۱. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها

یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۲۲. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) همه گزینه‌ها صحیح است.
ب) یک مساله از نوع اثبات دانایی صفر است.
ج) یک مساله تسهیم راز است.
د) یک مساله از نوع روش‌های غیرتعاملی است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۲۳. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۲۴. طول واقعی کلید DES برابر است با .....

الف) ۵۶
ب) ۴۸
ج) ۶۴
د) ۳۲

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۲۵. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 10
ب) 34
ج) 7
د) 17

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۲۶. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.
ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$
د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۲۷. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۲۸. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۲۹. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه شبکه　　ب) لایه کاربرد　　ج) لایه انتقال　　د) لایه پیوند داده

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۳۰. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن آشکار - متن رمز شده　　ب) گمراه کنندگی - متن رمز شده - متن آشکار

ج) انتشار - متن رمز شده - متن آشکار　　د) انتشار - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۱. رقم آخر عدد 3^{90} چند است؟

الف) 9 ب) 6 ج) 8 د) 7

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم ب) هیچ‌کدام ج) حمله نوع اول د) حمله نوع سوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۳. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن آشکار - متن رمز شده ب) انتشار - متن آشکار - متن رمز شده
ج) انتشار - متن رمز شده - متن آشکار د) گمراه کنندگی - متن رمز شده - متن آشکار

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۴. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 4 ب) 5 ج) 3 د) 6

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۵. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 7 ب) 10 ج) 34 د) 17

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۶. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) F ب) P ج) E د) S

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۷. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۸. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۹. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۰. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 6 ب) 2 ج) 4 د) 8

پاسخ: این عدد ریشه اولیه ندارد.

۱۱. طول واقعی کلید DES برابر است با .....

الف) ۳۲ ب) ۴۸ ج) ۵۶ د) ۶۴

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۱۲. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم ب) هیچ‌کدام ج) حمله نوع اول د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۳. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۱۴. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۵. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
ب) متن اصلی باید نسبت به $\phi(n)$ اول باشد.
ج) متن اصلی باید نسبت به n اول باشد.
د) کلید عمومی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۱۶. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۱۷. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) انتشار - رمز - کلید
ب) گمراه کنندگی - رمز - کلید
ج) گمراه کنندگی - آشکار - متن رمز
د) انتشار - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۱۸. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه پیوند داده
ب) لایه کاربرد
ج) لایه انتقال
د) لایه شبکه

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۱۹. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۲۰. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob
ب) کلید عمومی Alice
ج) کلید محرمانه Alice
د) کلید عمومی Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲۱. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.
ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$
د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۲۲. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۲۳. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 27 ب) 2 ج) 25 د) 6

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۲۴. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice ب) کلید محرمانه Bob ج) کلید محرمانه Alice د) کلید عمومی Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۲۵. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله از نوع روش‌های غیرتعاملی است. ب) یک مساله تسهیم راز است.

ج) همه گزینه‌ها صحیح است. د) یک مساله از نوع اثبات دانایی صفر است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۲۶. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۲۷. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۲۸. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۲۹. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۳۰. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۱. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۲. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) انتشار - رمز - کلید
ب) گمراه کنندگی - رمز - کلید
ج) گمراه کنندگی - آشکار - متن رمز
د) انتشار - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۳. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۴. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۵. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) P
ب) E
ج) F
د) S

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۶. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم　　ب) هیچ‌کدام　　ج) حمله نوع دوم　　د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۷. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۸. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۹. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice　　ب) کلید محرمانه Alice　　ج) کلید عمومی Bob　　د) کلید محرمانه Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۱۰. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۱۱. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۱۲. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice　　ب) کلید عمومی Bob　　ج) کلید محرمانه Bob　　د) کلید عمومی Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۱۳. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 6 ب) 3 ج) 5 د) 4

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۱۴. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۵. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۶. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 6 ب) 27 ج) 2 د) 25

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۱۷. طول واقعی کلید DES برابر است با .....

الف) ۳۲ ب) ۶۴ ج) ۴۸ د) ۵۶

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۱۸. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۱۹. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 7 ب) 17 ج) 10 د) 34

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۲۰. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۲۱. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به n اول باشد.

ب) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.

ج) کلید عمومی باید نسبت به n اول باشد.

د) متن اصلی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲۲. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله از نوع روش‌های غیرتعاملی است.

ب) یک مساله از نوع اثبات دانایی صفر است.

ج) یک مساله تسهیم راز است.

د) همه گزینه‌ها صحیح است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۲۳. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۴. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۲۵. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن آشکار - متن رمز شده
ب) گمراه کنندگی - متن رمز شده - متن آشکار
ج) انتشار - متن آشکار - متن رمز شده
د) انتشار - متن رمز شده - متن آشکار

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۲۶. رقم آخر عدد 3^{90} چند است؟

الف) 6
ب) 8
ج) 9
د) 7

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲۷. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۲۸. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه کاربرد
ب) لایه پیوند داده
ج) لایه انتقال
د) لایه شبکه

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۲۹. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم
ب) هیچ‌کدام
ج) حمله نوع دوم
د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۳۰. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 2
ب) 4
ج) 8
د) 6

پاسخ: این عدد ریشه اولیه ندارد.

۱. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob　　ب) کلید عمومی Alice　　ج) کلید عمومی Bob　　د) کلید محرمانه Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۳. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 34　　ب) 10　　ج) 17　　د) 7

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۴. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) همه گزینه‌ها صحیح است.　　ب) یک مساله تسهیم راز است.

ج) یک مساله از نوع اثبات دانایی صفر است.　　د) یک مساله از نوع روش‌های غیرتعاملی است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۵. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۶. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم　　ب) حمله نوع دوم　　ج) هیچ‌کدام　　د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۷. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۸. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 2　　ب) 4　　ج) 6　　د) 8

پاسخ: این عدد ریشه اولیه ندارد.

۹. رقم آخر عدد 3^{90} چند است؟

الف) 7 ب) 8 ج) 6 د) 9

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۱۰. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۱۱. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۲. طول واقعی کلید DES برابر است با .....

الف) ۳۲ ب) ۵۶ ج) ۶۴ د) ۴۸

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۱۳. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه پیوند داده ب) لایه شبکه ج) لایه کاربرد د) لایه انتقال

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۱۴. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) E　　ب) S　　ج) F　　د) P

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۱۵. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۱۶. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice　　ب) کلید محرمانه Bob　　ج) کلید عمومی Bob　　د) کلید محرمانه Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۱۷. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۸. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۱۹. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 5　　ب) 4　　ج) 6　　د) 3

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۲۰. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - آشکار - متن رمز
ب) انتشار - آشکار - متن رمز
ج) انتشار - رمز - کلید
د) گمراه کنندگی - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۲۱. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۲۲. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۲۳. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۲۴. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به $\phi(n)$ اول باشد.
ب) متن اصلی باید نسبت به n اول باشد.
ج) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
د) کلید عمومی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲۵. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 25
ب) 6
ج) 27
د) 2

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۲۶. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۷. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام　　ب) حمله نوع سوم　　ج) حمله نوع دوم　　د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۸. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۲۹. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن آشکار - متن رمز شده　　ب) گمراه کنندگی - متن آشکار - متن رمز شده

ج) گمراه کنندگی - متن رمز شده - متن آشکار　　د) انتشار - متن رمز شده - متن آشکار

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۳۰. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۱. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۲. در SSH چگونه از حمله تغییر قابلیت‌های مشترک نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۳. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۴. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه انتقال　　ب) لایه پیوند داده　　ج) لایه کاربرد　　د) لایه شبکه

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۵. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 2　　ب) 4　　ج) 8　　د) 6

پاسخ: این عدد ریشه اولیه ندارد.

۶. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 7 ب) 17 ج) 34 د) 10

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۷. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۸. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام ب) حمله نوع دوم ج) حمله نوع سوم د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۹. طول واقعی کلید DES برابر است با .....

الف) ۵۶ ب) ۶۴ ج) ۳۲ د) ۴۸

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۱۰. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۱۱. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۲. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به n اول باشد. ب) متن اصلی باید نسبت به n اول باشد.
ج) کلید عمومی باید نسبت به $\phi(n)$ اول باشد. د) متن اصلی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۱۳. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.
ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.
ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.
د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۱۴. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن آشکار - متن رمز شده
ب) انتشار - متن رمز شده - متن آشکار
ج) گمراه کنندگی - متن رمز شده - متن آشکار
د) گمراه کنندگی - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۱۵. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۶. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) E
ب) S
ج) P
د) F

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۱۷. رقم آخر عدد 3^{90} چند است؟

الف) 8
ب) 6
ج) 7
د) 9

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۱۸. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 4
ب) 5
ج) 3
د) 6

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۱۹. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Bob
ب) کلید عمومی Alice
ج) کلید محرمانه Bob
د) کلید محرمانه Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲۰. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۲۱. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 6 ب) 2 ج) 27 د) 25

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۲۲. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۲۳. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - آشکار - متن رمز ب) انتشار - رمز - کلید

ج) انتشار - آشکار - متن رمز د) گمراه کنندگی - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۲۴. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice ب) کلید عمومی Bob ج) کلید محرمانه Bob د) کلید عمومی Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۲۵. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام ب) حمله نوع دوم ج) حمله نوع اول د) حمله نوع سوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۶. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۲۷. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله از نوع اثبات دانایی صفر است.

ب) یک مساله تسهیم راز است.

ج) همه گزینه‌ها صحیح است.

د) یک مساله از نوع روش‌های غیرتعاملی است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۲۸. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۲۹. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۳۰. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۱. طول واقعی کلید DES برابر است با .....

الف) ۴۸ ب) ۳۲ ج) ۵۶ د) ۶۴

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۲. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۳. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۴. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) همه گزینه‌ها صحیح است. ب) یک مساله تسهیم راز است.

ج) یک مساله از نوع روش‌های غیرتعاملی است. د) یک مساله از نوع اثبات دانایی صفر است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۵. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۶. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۷. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۸. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 17 ب) 34 ج) 7 د) 10

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۹. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۱۰. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - رمز - کلید
ب) انتشار - رمز - کلید
ج) انتشار - آشکار - متن رمز
د) گمراه کنندگی - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۱۱. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) F
ب) E
ج) S
د) P

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۱۲. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۱۳. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 25
ب) 27
ج) 2
د) 6

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۱۴. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob
ب) کلید محرمانه Alice
ج) کلید عمومی Alice
د) کلید عمومی Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۱۵. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول　　ب) حمله نوع سوم　　ج) هیچ‌کدام　　د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۶. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه کاربرد　　ب) لایه پیوند داده　　ج) لایه شبکه　　د) لایه انتقال

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۱۷. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۸. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۱۹. رقم آخر عدد 3^{90} چند است؟

الف) 7　　ب) 8　　ج) 6　　د) 9

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲۰. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 6　　ب) 2　　ج) 4　　د) 8

پاسخ: این عدد ریشه اولیه ندارد.

۲۱. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۲۲. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۲۳. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۲۴. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۲۵. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۶. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن رمز شده - متن آشکار

ب) گمراه کنندگی - متن آشکار - متن رمز شده

ج) گمراه کنندگی - متن رمز شده - متن آشکار

د) انتشار - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۲۷. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به n اول باشد.
ب) متن اصلی باید نسبت به $\phi(n)$ اول باشد.
ج) متن اصلی باید نسبت به n اول باشد.
د) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲۸. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 6
ب) 4
ج) 3
د) 5

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۲۹. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام
ب) حمله نوع دوم
ج) حمله نوع سوم
د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۳۰. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Bob
ب) کلید عمومی Alice
ج) کلید محرمانه Bob
د) کلید محرمانه Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۱. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به n اول باشد.
ب) متن اصلی باید نسبت به $\phi(n)$ اول باشد.
ج) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
د) متن اصلی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.
ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$
د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۳. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۴. طول واقعی کلید DES برابر است با .....

الف) ۴۸
ب) ۶۴
ج) ۵۶
د) ۳۲

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۵. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم
ب) حمله نوع دوم
ج) هیچ‌کدام
د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۶. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۷. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله از نوع روش‌های غیرتعاملی است.
ب) همه گزینه‌ها صحیح است.
ج) یک مساله تسهیم راز است.
د) یک مساله از نوع اثبات دانایی صفر است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۸. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) P　　ب) F　　ج) S　　د) E

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۹. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 8　　ب) 4　　ج) 6　　د) 2

پاسخ: این عدد ریشه اولیه ندارد.

۱۰. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۱۱. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول　　ب) هیچ‌کدام　　ج) حمله نوع سوم　　د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۲. رقم آخر عدد 3^{90} چند است؟

الف) 6　　ب) 8　　ج) 7　　د) 9

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۱۳. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۱۴. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۱۵. در SSH چگونه از حمله تغییر قابلیت‌های مشترک نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۱۶. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 17 ب) 10 ج) 7 د) 34

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۱۷. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۱۸. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Bob　　ب) کلید عمومی Alice　　ج) کلید محرمانه Alice　　د) کلید محرمانه Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۱۹. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن رمز شده - متن آشکار　　ب) انتشار - متن رمز شده - متن آشکار

ج) گمراه کنندگی - متن آشکار - متن رمز شده　　د) انتشار - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۲۰. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۱. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 4　　ب) 6　　ج) 5　　د) 3

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۲۲. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice　　ب) کلید عمومی Bob　　ج) کلید محرمانه Bob　　د) کلید عمومی Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۲۳. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod{n}$$

۲۴. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۵. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - آشکار - متن رمز
ب) انتشار - آشکار - متن رمز
ج) گمراه کنندگی - رمز - کلید
د) انتشار - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۲۶. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 25
ب) 2
ج) 27
د) 6

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۲۷. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه انتقال
ب) لایه پیوند داده
ج) لایه شبکه
د) لایه کاربرد

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۲۸. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.
ب) کلید باید به صورت کاملا تصادفی تولید شود.
ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.
د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۲۹. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۳۰. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 2 ب) 6 ج) 8 د) 4

پاسخ: این عدد ریشه اولیه ندارد.

۲. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - آشکار - متن رمز
ب) گمراه کنندگی - رمز - کلید
ج) انتشار - رمز - کلید
د) انتشار - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۳. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۴. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به n اول باشد.
ب) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
ج) متن اصلی باید نسبت به $\phi(n)$ اول باشد.
د) کلید عمومی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۵. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 27 ب) 2 ج) 6 د) 25

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۶. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۷. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۸. طول واقعی کلید DES برابر است با .....

الف) ۵۶ ب) ۴۸ ج) ۶۴ د) ۳۲

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۹. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۱۰. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 10 ب) 17 ج) 7 د) 34

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۱۱. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۱۲. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice ب) کلید محرمانه Bob ج) کلید عمومی Bob د) کلید عمومی Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۱۳. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام ب) حمله نوع دوم ج) حمله نوع اول د) حمله نوع سوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۴. رقم آخر عدد 3^{90} چند است؟

الف) 6 ب) 8 ج) 9 د) 7

پاسخ: ✍ دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

✍ آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۱۵. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) E ب) P ج) F د) S

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۱۶. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه پیوند داده ب) لایه کاربرد ج) لایه انتقال د) لایه شبکه

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۱۷. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۸. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۱۹. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice ب) کلید محرمانه Alice ج) کلید محرمانه Bob د) کلید عمومی Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲۰. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۲۱. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم　　ب) هیچ‌کدام　　ج) حمله نوع اول　　د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۲. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۲۳. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۴. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن آشکار - متن رمز شده　　ب) گمراه کنندگی - متن آشکار - متن رمز شده

ج) گمراه کنندگی - متن رمز شده - متن آشکار　　د) انتشار - متن رمز شده - متن آشکار

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۲۵. در SSH چگونه از حمله تغییر قابلیت‌های مشترک نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشترک ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۲۶. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله از نوع روش‌های غیرتعاملی است.　　ب) یک مساله تسهیم راز است.

ج) یک مساله از نوع اثبات دانایی صفر است.　　د) همه گزینه‌ها صحیح است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۲۷. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۲۸. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۹. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 5 ب) 4 ج) 3 د) 6

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۳۰. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۱. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۲. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۳. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۴. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله تسهیم راز است.

ب) همه گزینه‌ها صحیح است.

ج) یک مساله از نوع اثبات دانایی صفر است.

د) یک مساله از نوع روش‌های غیرتعاملی است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۵. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۶. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۷. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۸. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 2 ب) 8 ج) 6 د) 4

پاسخ: این عدد ریشه اولیه ندارد.

۹. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۱۰. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۱۱. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 6 ب) 3 ج) 5 د) 4

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۱۲. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) انتشار - آشکار - متن رمز
ب) گمراه کنندگی - آشکار - متن رمز
ج) گمراه کنندگی - رمز - کلید
د) انتشار - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۱۳. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice
ب) کلید محرمانه Bob
ج) کلید عمومی Alice
د) کلید عمومی Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۱۴. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۱۵. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.
ب) کلید باید به صورت کاملا تصادفی تولید شود.
ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.
د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۶. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم
ب) حمله نوع اول
ج) حمله نوع دوم
د) هیچ‌کدام

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۷. رقم آخر عدد 3^{90} چند است؟

الف) 6
ب) 7
ج) 9
د) 8

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

✍ آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۱۸. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۱۹. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 10 ب) 34 ج) 7 د) 17

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۲۰. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) E ب) F ج) S د) P

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۲۱. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۲. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۳. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 27 ب) 2 ج) 6 د) 25

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۲۴. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه شبکه ب) لایه انتقال ج) لایه کاربرد د) لایه پیوند داده

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۲۵. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice ب) کلید محرمانه Bob ج) کلید عمومی Alice د) کلید عمومی Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲۶. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن آشکار - متن رمز شده
ب) گمراه کنندگی - متن رمز شده - متن آشکار
ج) انتشار - متن رمز شده - متن آشکار
د) گمراه کنندگی - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۲۷. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۲۸. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
ب) متن اصلی باید نسبت به n اول باشد.
ج) کلید عمومی باید نسبت به n اول باشد.
د) متن اصلی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲۹. طول واقعی کلید DES برابر است با .....

الف) ۳۲
ب) ۶۴
ج) ۴۸
د) ۵۶

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۳۰. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم
ب) هیچ‌کدام
ج) حمله نوع دوم
د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۲. طول واقعی کلید DES برابر است با .....

الف) ۵۶ ب) ۳۲ ج) ۴۸ د) ۶۴

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۳. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۴. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob ب) کلید عمومی Bob ج) کلید عمومی Alice د) کلید محرمانه Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۵. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۶. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۷. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) P ب) F ج) S د) E

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۸. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 34 ب) 7 ج) 17 د) 10

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۹. رقم آخر عدد 3^{90} چند است؟

الف) 6 ب) 8 ج) 7 د) 9

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۱۰. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) همه گزینه‌ها صحیح است.
ب) یک مساله از نوع روش‌های غیرتعاملی است.
ج) یک مساله تسهیم راز است.
د) یک مساله از نوع اثبات دانایی صفر است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۱۱. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.
ب) کلید باید به صورت کاملا تصادفی تولید شود.
ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.
د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۲. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۳. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول ب) حمله نوع سوم ج) حمله نوع دوم د) هیچ‌کدام

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۴. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۵. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.
ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$
د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۱۶. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) انتشار - رمز - کلید
ب) انتشار - آشکار - متن رمز
ج) گمراه کنندگی - رمز - کلید
د) گمراه کنندگی - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۱۷. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 6
ب) 5
ج) 3
د) 4

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۱۸. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۱۹. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3

- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۲۰. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 27 ب) 2 ج) 25 د) 6

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۲۱. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۲۲. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن رمز شده - متن آشکار
ب) انتشار - متن آشکار - متن رمز شده
ج) گمراه کنندگی - متن رمز شده - متن آشکار
د) گمراه کنندگی - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۲۳. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به n اول باشد.
ب) متن اصلی باید نسبت به $\phi(n)$ اول باشد.
ج) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
د) متن اصلی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲۴. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۲۵. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob　　ب) کلید عمومی Bob　　ج) کلید عمومی Alice　　د) کلید محرمانه Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲۶. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۲۷. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه کاربرد　　ب) لایه انتقال　　ج) لایه پیوند داده　　د) لایه شبکه

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۲۸. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 2　　ب) 4　　ج) 6　　د) 8

پاسخ: این عدد ریشه اولیه ندارد.

۲۹. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام　　ب) حمله نوع سوم　　ج) حمله نوع اول　　د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۳۰. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

نام و نام خانوادگی	شماره دانشجویی	نام درس	تاریخ	شماره برگه
		امنیت سیستم‌های کامپیوتری	۱۴۰۳/۰۲/۱۱	۳۸

۱. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۲. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice ب) کلید عمومی Alice ج) کلید محرمانه Bob د) کلید عمومی Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۳. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام ب) حمله نوع دوم ج) حمله نوع اول د) حمله نوع سوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۴. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۵. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۶. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) F ب) S ج) P د) E

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۷. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۸. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 2 ب) 25 ج) 27 د) 6

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۹. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن رمز شده - متن آشکار
ب) انتشار - متن آشکار - متن رمز شده
ج) گمراه کنندگی - متن آشکار - متن رمز شده
د) گمراه کنندگی - متن رمز شده - متن آشکار

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۱۰. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه انتقال ب) لایه شبکه ج) لایه پیوند داده د) لایه کاربرد

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۱۱. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Bob ب) کلید عمومی Alice ج) کلید محرمانه Bob د) کلید محرمانه Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۱۲. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۱۳. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله از نوع اثبات دانایی صفر است.
ب) یک مساله از نوع روش‌های غیرتعاملی است.
ج) همه گزینه‌ها صحیح است.
د) یک مساله تسهیم راز است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۱۴. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۱۵. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 8 ب) 6 ج) 4 د) 2

پاسخ: این عدد ریشه اولیه ندارد.

۱۶. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۷. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 17 ب) 10 ج) 34 د) 7

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۱۸. رقم آخر عدد 3^{90} چند است؟

الف) 8 ب) 7 ج) 6 د) 9

پاسخ: ✍ دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

✍ آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۱۹. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - رمز - کلید ب) انتشار - رمز - کلید
ج) گمراه کنندگی - آشکار - متن رمز د) انتشار - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۲۰. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۱. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.
ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.
ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.
د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۲۲. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به n اول باشد. ب) متن اصلی باید نسبت به n اول باشد.
ج) متن اصلی باید نسبت به $\phi(n)$ اول باشد. د) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲۳. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم　　ب) حمله نوع اول　　ج) هیچ‌کدام　　د) حمله نوع سوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۴. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۲۵. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۲۶. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۲۷. طول واقعی کلید DES برابر است با .....

الف) ۳۲　　ب) ۴۸　　ج) ۶۴　　د) ۵۶

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۲۸. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۲۹. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۳۰. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 4 ب) 6 ج) 3 د) 5

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۱. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به n اول باشد.
ب) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
ج) کلید عمومی باید نسبت به n اول باشد.
د) متن اصلی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) P
ب) F
ج) S
د) E

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۳. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) انتشار - آشکار - متن رمز
ب) گمراه کنندگی - رمز - کلید
ج) گمراه کنندگی - آشکار - متن رمز
د) انتشار - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۴. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice
ب) کلید محرمانه Alice
ج) کلید عمومی Bob
د) کلید محرمانه Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۵. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۶. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله تسهیم راز است.
ب) یک مساله از نوع روش‌های غیرتعاملی است.
ج) یک مساله از نوع اثبات دانایی صفر است.
د) همه گزینه‌ها صحیح است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۷. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 3
ب) 5
ج) 6
د) 4

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۸. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۹. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن رمز شده - متن آشکار
ب) انتشار - متن رمز شده - متن آشکار
ج) گمراه کنندگی - متن آشکار - متن رمز شده
د) انتشار - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۱۰. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 10
ب) 7
ج) 17
د) 34

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۱۱. طول واقعی کلید DES برابر است با .....

الف) ۴۸
ب) ۵۶
ج) ۶۴
د) ۳۲

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۱۲. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Bob　　ب) کلید محرمانه Alice　　ج) کلید محرمانه Bob　　د) کلید عمومی Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۱۳. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه کاربرد　　ب) لایه انتقال　　ج) لایه پیوند داده　　د) لایه شبکه

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۱۴. رقم آخر عدد 3^{90} چند است؟

الف) 9　　ب) 6　　ج) 8　　د) 7

پاسخ: ✍ دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

✍ آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۱۵. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۶. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۱۷. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۱۸. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۱۹. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۰. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام　　ب) حمله نوع سوم　　ج) حمله نوع دوم　　د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۱. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 2　　ب) 8　　ج) 4　　د) 6

پاسخ: این عدد ریشه اولیه ندارد.

۲۲. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۳. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۲۴. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۲۵. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۶. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۲۷. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 25 ب) 27 ج) 6 د) 2

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۲۸. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۹. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۳۰. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم ب) هیچ‌کدام ج) حمله نوع سوم د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) F　　ب) P　　ج) E　　د) S

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۲. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۳. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۴. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۵. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) همه گزینه‌ها صحیح است.
ب) یک مساله از نوع اثبات دانایی صفر است.
ج) یک مساله تسهیم راز است.
د) یک مساله از نوع روش‌های غیرتعاملی است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۶. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice
ب) کلید محرمانه Bob
ج) کلید عمومی Bob
د) کلید محرمانه Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۷. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به n اول باشد.
ب) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
ج) متن اصلی باید نسبت به n اول باشد.
د) متن اصلی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۸. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام
ب) حمله نوع دوم
ج) حمله نوع سوم
د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۹. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 5
ب) 6
ج) 4
د) 3

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۱۰. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.
ب) کلید باید به صورت کاملا تصادفی تولید شود.
ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.
د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۱. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۲. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه کاربرد　　ب) لایه شبکه　　ج) لایه انتقال　　د) لایه پیوند داده

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۱۳. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۱۴. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۱۵. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 17　　ب) 34　　ج) 10　　د) 7

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۱۶. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم　　ب) حمله نوع دوم　　ج) هیچ‌کدام　　د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۷. رقم آخر عدد 3^{90} چند است؟

الف) 9 ب) 8 ج) 7 د) 6

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۱۸. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod{n}$$

۱۹. طول واقعی کلید DES برابر است با .....

الف) ۳۲ ب) ۴۸ ج) ۵۶ د) ۶۴

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۲۰. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۱. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۲۲. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۳. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) انتشار - رمز - کلید ب) گمراه کنندگی - آشکار - متن رمز

ج) انتشار - آشکار - متن رمز د) گمراه کنندگی - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۲۴. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 6 ب) 4 ج) 8 د) 2

پاسخ: این عدد ریشه اولیه ندارد.

۲۵. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۲۶. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن آشکار - متن رمز شده
ب) انتشار - متن رمز شده - متن آشکار
ج) گمراه کنندگی - متن رمز شده - متن آشکار
د) گمراه کنندگی - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۲۷. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۲۸. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice ب) کلید عمومی Bob ج) کلید محرمانه Bob د) کلید محرمانه Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲۹. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 6 ب) 2 ج) 25 د) 27

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۳۰. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۳. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه انتقال　　ب) لایه پیوند داده　　ج) لایه کاربرد　　د) لایه شبکه

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۴. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۵. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 6　　ب) 4　　ج) 3　　د) 5

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۶. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۷. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۸. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۹. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۰. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله تسهیم راز است.

ب) یک مساله از نوع روش‌های غیرتعاملی است.

ج) همه گزینه‌ها صحیح است.

د) یک مساله از نوع اثبات دانایی صفر است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۱۱. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۲. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۱۳. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice　　ب) کلید عمومی Bob　　ج) کلید محرمانه Alice　　د) کلید محرمانه Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۱۴. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۱۵. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) P　　ب) F　　ج) S　　د) E

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۱۶. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۷. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۱۸. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 8　　ب) 6　　ج) 4　　د) 2

پاسخ: این عدد ریشه اولیه ندارد.

۱۹. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 17 ب) 7 ج) 10 د) 34

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۲۰. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Bob ب) کلید محرمانه Bob ج) کلید محرمانه Alice د) کلید عمومی Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲۱. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم ب) هیچ‌کدام ج) حمله نوع اول د) حمله نوع سوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۲. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن رمز شده - متن آشکار
ب) انتشار - متن آشکار - متن رمز شده
ج) گمراه کنندگی - متن آشکار - متن رمز شده
د) انتشار - متن رمز شده - متن آشکار

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۲۳. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۲۴. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به $\phi(n)$ اول باشد.
ب) کلید عمومی باید نسبت به n اول باشد.
ج) متن اصلی باید نسبت به n اول باشد.
د) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲۵. رقم آخر عدد 3^{90} چند است؟

الف) 9 ب) 6 ج) 7 د) 8

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲۶. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) انتشار - آشکار - متن رمز
ب) گمراه کنندگی - آشکار - متن رمز
ج) گمراه کنندگی - رمز - کلید
د) انتشار - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۲۷. طول واقعی کلید DES برابر است با .....

الف) ۴۸
ب) ۵۶
ج) ۳۲
د) ۶۴

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۲۸. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 25
ب) 2
ج) 6
د) 27

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۲۹. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۳۰. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم
ب) حمله نوع اول
ج) هیچ‌کدام
د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم　　ب) حمله نوع دوم　　ج) حمله نوع اول　　د) هیچ‌کدام

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) انتشار - آشکار - متن رمز　　ب) انتشار - رمز - کلید

ج) گمراه کنندگی - آشکار - متن رمز　　د) گمراه کنندگی - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۳. در SSH چگونه از حمله تغییر قابلیت‌های مشترک نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشترک ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۴. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۵. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

- د در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- ه سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- و دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۶. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۷. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۸. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم　　ب) هیچ‌کدام　　ج) حمله نوع دوم　　د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۹. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) P　　ب) S　　ج) E　　د) F

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۱۰. طول واقعی کلید DES برابر است با .....

الف) ۴۸　　ب) ۳۲　　ج) ۵۶　　د) ۶۴

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۱۱. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۲. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۳. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۴. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله تسهیم راز است.
ب) یک مساله از نوع روش‌های غیرتعاملی است.
ج) همه گزینه‌ها صحیح است.
د) یک مساله از نوع اثبات دانایی صفر است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۱۵. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.
ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.
ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.
د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۱۶. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.
ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$
د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۱۷. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن آشکار - متن رمز شده
ب) انتشار - متن رمز شده - متن آشکار
ج) گمراه کنندگی - متن رمز شده - متن آشکار
د) انتشار - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۱۸. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۹. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice
ب) کلید عمومی Bob
ج) کلید محرمانه Bob
د) کلید عمومی Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲۰. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 3
ب) 4
ج) 5
د) 6

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۲۱. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod{n}$$

۲۲. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 2 ب) 4 ج) 6 د) 8

پاسخ: این عدد ریشه اولیه ندارد.

۲۳. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice ب) کلید عمومی Bob ج) کلید محرمانه Bob د) کلید عمومی Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۲۴. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۲۵. رقم آخر عدد 3^{90} چند است؟

الف) 6 ب) 9 ج) 8 د) 7

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲۶. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۷. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه پیوند داده ب) لایه شبکه ج) لایه کاربرد د) لایه انتقال

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۲۸. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به n اول باشد. ب) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
ج) متن اصلی باید نسبت به $\phi(n)$ اول باشد. د) کلید عمومی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲۹. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 27 ب) 25 ج) 2 د) 6

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۳۰. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 17 ب) 7 ج) 10 د) 34

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۱. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice　　ب) کلید عمومی Bob　　ج) کلید محرمانه Alice　　د) کلید محرمانه Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۳. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 3　　ب) 6　　ج) 5　　د) 4

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۴. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم　　ب) هیچ‌کدام　　ج) حمله نوع سوم　　د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۵. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.

- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۶. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 2 ب) 8 ج) 4 د) 6

پاسخ: این عدد ریشه اولیه ندارد.

۷. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۸. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice ب) کلید عمومی Bob ج) کلید محرمانه Bob د) کلید محرمانه Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۹. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۱۰. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۱۱. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله از نوع اثبات دانایی صفر است. ب) یک مساله از نوع روش‌های غیرتعاملی است.

ج) یک مساله تسهیم راز است. د) همه گزینه‌ها صحیح است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۱۲. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۳. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۴. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۵. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 10 ب) 34 ج) 17 د) 7

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۱۶. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن آشکار - متن رمز شده

ب) انتشار - متن رمز شده - متن آشکار

ج) گمراه کنندگی - متن رمز شده - متن آشکار

د) انتشار - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۱۷. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - رمز - کلید

ب) انتشار - آشکار - متن رمز

ج) انتشار - رمز - کلید

د) گمراه کنندگی - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۱۸. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۹. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول ب) حمله نوع سوم ج) هیچ‌کدام د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۰. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

- ج تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- د در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- ه سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- و دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۲۱. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۲. رقم آخر عدد 3^{90} چند است؟

الف) 7 ب) 9 ج) 6 د) 8

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲۳. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 6 ب) 2 ج) 25 د) 27

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۲۴. طول واقعی کلید DES برابر است با .....

الف) ۴۸ ب) ۵۶ ج) ۶۴ د) ۳۲

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۲۵. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۲۶. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)

- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۲۷. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به $\phi(n)$ اول باشد.
ب) متن اصلی باید نسبت به n اول باشد.
ج) کلید عمومی باید نسبت به n اول باشد.
د) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲۸. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) P
ب) E
ج) F
د) S

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۲۹. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.
ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.
ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.
د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۳۰. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه پیوند داده
ب) لایه کاربرد
ج) لایه انتقال
د) لایه شبکه

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۱. رقم آخر عدد 3^{90} چند است؟

الف) 6 ب) 8 ج) 7 د) 9

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 4 ب) 5 ج) 6 د) 3

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۳. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۴. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۵. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice ب) کلید محرمانه Alice ج) کلید عمومی Bob د) کلید محرمانه Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۶. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۷. طول واقعی کلید DES برابر است با .....

الف) ۳۲ ب) ۶۴ ج) ۴۸ د) ۵۶

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۸. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۹. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice ب) کلید عمومی Bob ج) کلید محرمانه Bob د) کلید محرمانه Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۱۰. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۱. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله تسهیم راز است.
ب) یک مساله از نوع روش‌های غیرتعاملی است.
ج) یک مساله از نوع اثبات دانایی صفر است.
د) همه گزینه‌ها صحیح است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۱۲. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۳. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم
ب) حمله نوع دوم
ج) هیچ‌کدام
د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۴. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن آشکار - متن رمز شده
ب) گمراه کنندگی - متن رمز شده - متن آشکار
ج) انتشار - متن رمز شده - متن آشکار
د) گمراه کنندگی - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۱۵. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۶. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه شبکه
ب) لایه کاربرد
ج) لایه پیوند داده
د) لایه انتقال

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۱۷. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۱۸. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) S
ب) F
ج) E
د) P

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۱۹. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 2 ب) 27 ج) 6 د) 25

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۲۰. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۲۱. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۲۲. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - آشکار - متن رمز ب) انتشار - آشکار - متن رمز
ج) انتشار - رمز - کلید د) گمراه کنندگی - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۲۳. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم ب) هیچ‌کدام ج) حمله نوع اول د) حمله نوع سوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۴. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا
ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا
ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن
د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۲۵. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.
ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$
د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۲۶. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۷. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۲۸. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به n اول باشد.
ب) متن اصلی باید نسبت به n اول باشد.
ج) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
د) متن اصلی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲۹. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 8
ب) 2
ج) 6
د) 4

پاسخ: این عدد ریشه اولیه ندارد.

۳۰. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 7
ب) 10
ج) 17
د) 34

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۱. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۲. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 3 ب) 4 ج) 6 د) 5

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۳. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod{n}$$

۴. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۵. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۶. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۷. طول واقعی کلید DES برابر است با .....

الف) ۶۴ ب) ۳۲ ج) ۴۸ د) ۵۶

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۸. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob ب) کلید عمومی Alice ج) کلید عمومی Bob د) کلید محرمانه Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۹. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن رمز شده - متن آشکار ب) انتشار - متن آشکار - متن رمز شده

ج) انتشار - متن رمز شده - متن آشکار د) گمراه کنندگی - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۱۰. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۱. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice ب) کلید محرمانه Alice ج) کلید عمومی Bob د) کلید محرمانه Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۱۲. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۱۳. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 7 ب) 34 ج) 10 د) 17

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۱۴. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) انتشار - رمز - کلید
ب) گمراه کنندگی - رمز - کلید
ج) گمراه کنندگی - آشکار - متن رمز
د) انتشار - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۱۵. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 6 ب) 2 ج) 8 د) 4

پاسخ: این عدد ریشه اولیه ندارد.

۱۶. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) P ب) S ج) F د) E

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۱۷. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا
ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا
ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن
د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۱۸. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۹. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله از نوع اثبات دانایی صفر است.
ب) یک مساله تسهیم راز است.
ج) یک مساله از نوع روش‌های غیرتعاملی است.
د) همه گزینه‌ها صحیح است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۲۰. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۱. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.
ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.
ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.
د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۲۲. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۳. رقم آخر عدد 3^{90} چند است؟

الف) 6
ب) 7
ج) 9
د) 8

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲۴. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 6
ب) 25
ج) 27
د) 2

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۲۵. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه پیوند داده
ب) لایه شبکه
ج) لایه کاربرد
د) لایه انتقال

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۲۶. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5

- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۲۷. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم　　ب) حمله نوع دوم　　ج) حمله نوع اول　　د) هیچ‌کدام

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۸. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به n اول باشد.　　ب) کلید عمومی باید نسبت به n اول باشد.

ج) متن اصلی باید نسبت به $\phi(n)$ اول باشد.　　د) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲۹. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام　　ب) حمله نوع دوم　　ج) حمله نوع سوم　　د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۳۰. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۱. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۲. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۳. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 6 ب) 3 ج) 4 د) 5

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۴. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۵. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 27 ب) 2 ج) 25 د) 6

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۶. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۷. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) انتشار - رمز - کلید ب) گمراه کنندگی - آشکار - متن رمز
ج) گمراه کنندگی - رمز - کلید د) انتشار - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۸. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه پیوند داده ب) لایه شبکه ج) لایه کاربرد د) لایه انتقال

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۹. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن آشکار - متن رمز شده ب) گمراه کنندگی - متن رمز شده - متن آشکار
ج) انتشار - متن آشکار - متن رمز شده د) انتشار - متن رمز شده - متن آشکار

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۱۰. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.
ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$
د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۱۱. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) E ب) F ج) P د) S

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۱۲. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 7 ب) 17 ج) 34 د) 10

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۱۳. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۱۴. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۱۵. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) همه گزینه‌ها صحیح است. ب) یک مساله از نوع روش‌های غیرتعاملی است.

ج) یک مساله از نوع اثبات دانایی صفر است. د) یک مساله تسهیم راز است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۱۶. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم ب) حمله نوع اول ج) حمله نوع سوم د) هیچ‌کدام

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۷. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۸. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob ب) کلید عمومی Bob ج) کلید محرمانه Alice د) کلید عمومی Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۱۹. رقم آخر عدد 3^{90} چند است؟

الف) 6 ب) 7 ج) 8 د) 9

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲۰. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۲۱. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم ب) حمله نوع اول ج) هیچ‌کدام د) حمله نوع سوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۲. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۲۳. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 6 ب) 2 ج) 4 د) 8

پاسخ: این عدد ریشه اولیه ندارد.

۲۴. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod{n}$$

۲۵. طول واقعی کلید DES برابر است با .....

الف) ۴۸ ب) ۳۲ ج) ۵۶ د) ۶۴

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۲۶. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به $\phi(n)$ اول باشد.
ب) کلید عمومی باید نسبت به n اول باشد.
ج) متن اصلی باید نسبت به n اول باشد.
د) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲۷. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟
الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.
ب) کلید باید به صورت کاملا تصادفی تولید شود.
ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.
د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۲۸. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice
ب) کلید عمومی Alice
ج) کلید عمومی Bob
د) کلید محرمانه Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۲۹. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۳۰. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۳. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) P　　ب) F　　ج) E　　د) S

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۴. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۵. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۶. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۷. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۸. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم　　ب) حمله نوع اول　　ج) هیچ‌کدام　　د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۹. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله از نوع روش‌های غیرتعاملی است.　　ب) همه گزینه‌ها صحیح است.

ج) یک مساله از نوع اثبات دانایی صفر است.　　د) یک مساله تسهیم راز است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۱۰. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۱۱. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 2　　ب) 6　　ج) 8　　د) 4

پاسخ: این عدد ریشه اولیه ندارد.

۱۲. در SSH چگونه از حمله تغییر قابلیت‌های مشترک نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۱۳. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) انتشار - آشکار - متن رمز　　ب) گمراه کنندگی - آشکار - متن رمز

ج) گمراه کنندگی - رمز - کلید　　د) انتشار - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۱۴. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 2 ب) 25 ج) 27 د) 6

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۱۵. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob ب) کلید عمومی Bob ج) کلید عمومی Alice د) کلید محرمانه Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۱۶. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 4 ب) 3 ج) 6 د) 5

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۱۷. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۱۸. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۹. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه شبکه ب) لایه انتقال ج) لایه کاربرد د) لایه پیوند داده

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۲۰. رقم آخر عدد 3^{90} چند است؟

الف) 8 ب) 6 ج) 7 د) 9

پاسخ: ✍ دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.

- عدد سه و ده نسبت به هم اول هستند، یعنی $(3,10)=1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

✍ آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲۱. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام　　ب) حمله نوع دوم　　ج) حمله نوع سوم　　د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۲. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۲۳. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۲۴. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۲۵. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن رمز شده - متن آشکار　　ب) انتشار - متن آشکار - متن رمز شده

ج) انتشار - متن رمز شده - متن آشکار　　د) گمراه کنندگی - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۲۶. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod{n}$$

۲۷. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 10 ب) 17 ج) 34 د) 7

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۲۸. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Bob ب) کلید محرمانه Alice ج) کلید عمومی Alice د) کلید محرمانه Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲۹. طول واقعی کلید DES برابر است با .....

الف) ۳۲ ب) ۴۸ ج) ۶۴ د) ۵۶

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۳۰. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به n اول باشد.
ب) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
ج) متن اصلی باید نسبت به $\phi(n)$ اول باشد.
د) کلید عمومی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۱. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۲. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله از نوع اثبات دانایی صفر است.

ب) یک مساله از نوع روش‌های غیرتعاملی است.

ج) یک مساله تسهیم راز است.

د) همه گزینه‌ها صحیح است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۳. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۴. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۵. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 4 ب) 8 ج) 6 د) 2

پاسخ: این عدد ریشه اولیه ندارد.

۶. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 5 ب) 3 ج) 4 د) 6

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۷. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - آشکار - متن رمز
ب) گمراه کنندگی - رمز - کلید
ج) انتشار - رمز - کلید
د) انتشار - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۸. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 7
ب) 34
ج) 17
د) 10

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۹. طول واقعی کلید DES برابر است با .....

الف) ۳۲
ب) ۴۸
ج) ۵۶
د) ۶۴

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۱۰. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۱۱. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init

- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۱۲. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۳. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۱۴. رقم آخر عدد 3^{90} چند است؟

الف) 6 ب) 8 ج) 9 د) 7

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۱۵. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود،

نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۶. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۱۷. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) E ب) F ج) P د) S

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۱۸. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۹. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم ب) هیچ‌کدام ج) حمله نوع اول د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۰. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۱. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice ب) کلید عمومی Bob ج) کلید محرمانه Bob د) کلید محرمانه Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۲۲. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.

ب) کلید عمومی باید نسبت به n اول باشد.

ج) متن اصلی باید نسبت به $\phi(n)$ اول باشد.

د) متن اصلی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲۳. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice ب) کلید عمومی Bob ج) کلید محرمانه Alice د) کلید محرمانه Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲۴. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۲۵. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۲۶. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 27 ب) 6 ج) 25 د) 2

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۲۷. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۸. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه کاربرد ب) لایه پیوند داده ج) لایه انتقال د) لایه شبکه

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۲۹. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن رمز شده - متن آشکار ب) انتشار - متن آشکار - متن رمز شده

ج) گمراه کنندگی - متن رمز شده - متن آشکار د) گمراه کنندگی - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۳۰. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول ب) حمله نوع سوم ج) هیچ‌کدام د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۳. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 17 ب) 34 ج) 7 د) 10

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۴. رقم آخر عدد 3^{90} چند است؟

الف) 8 ب) 7 ج) 9 د) 6

پاسخ: ✍ دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

✍ آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۵. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۶. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۷. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) S　　ب) P　　ج) F　　د) E

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۸. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 6　　ب) 27　　ج) 2　　د) 25

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۹. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۰. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله تسهیم راز است.　　ب) یک مساله از نوع روش‌های غیرتعاملی است.

ج) همه گزینه‌ها صحیح است.　　د) یک مساله از نوع اثبات دانایی صفر است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۱۱. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۱۲. در SSH چگونه از حمله تغییر قابلیت‌های مشترک نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH

- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۱۳. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 8 ب) 4 ج) 6 د) 2

پاسخ: این عدد ریشه اولیه ندارد.

۱۴. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۱۵. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) انتشار - آشکار - متن رمز ب) انتشار - رمز - کلید

ج) گمراه کنندگی - رمز - کلید د) گمراه کنندگی - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۱۶. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن آشکار - متن رمز شده ب) انتشار - متن رمز شده - متن آشکار

ج) گمراه کنندگی - متن رمز شده - متن آشکار د) انتشار - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۱۷. طول واقعی کلید DES برابر است با .....

الف) ۴۸ ب) ۳۲ ج) ۶۴ د) ۵۶

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۱۸. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۱۹. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice ب) کلید محرمانه Alice ج) کلید عمومی Bob د) کلید محرمانه Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲۰. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۲۱. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob　　ب) کلید عمومی Bob　　ج) کلید محرمانه Alice　　د) کلید عمومی Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۲۲. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه انتقال　　ب) لایه کاربرد　　ج) لایه پیوند داده　　د) لایه شبکه

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۲۳. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول　　ب) هیچ‌کدام　　ج) حمله نوع دوم　　د) حمله نوع سوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۴. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 5　　ب) 6　　ج) 4　　د) 3

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۲۵. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۲۶. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۲۷. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۸. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۲۹. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.

ب) متن اصلی باید نسبت به $\phi(n)$ اول باشد.

ج) کلید عمومی باید نسبت به n اول باشد.

د) متن اصلی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۳۰. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم

ب) حمله نوع سوم

ج) هیچ‌کدام

د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۲. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۳. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 2 ب) 27 ج) 25 د) 6

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۴. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۵. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 7 ب) 10 ج) 34 د) 17

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۶. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۷. طول واقعی کلید DES برابر است با .....

الف) ۶۴ ب) ۵۶ ج) ۳۲ د) ۴۸

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۸. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob ب) کلید محرمانه Alice ج) کلید عمومی Alice د) کلید عمومی Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۹. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله تسهیم راز است. ب) یک مساله از نوع اثبات دانایی صفر است.

ج) همه گزینه‌ها صحیح است. د) یک مساله از نوع روش‌های غیرتعاملی است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۱۰. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۱۱. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول ب) هیچ‌کدام ج) حمله نوع دوم د) حمله نوع سوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۲. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 8 ب) 4 ج) 2 د) 6

پاسخ: این عدد ریشه اولیه ندارد.

۱۳. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۴. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن آشکار - متن رمز شده ب) گمراه کنندگی - متن رمز شده - متن آشکار

ج) انتشار - متن رمز شده - متن آشکار د) انتشار - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۱۵. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۶. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice ب) کلید محرمانه Bob ج) کلید عمومی Bob د) کلید عمومی Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۱۷. رقم آخر عدد 3^{90} چند است؟

الف) 7 ب) 6 ج) 9 د) 8

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۱۸. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول ب) حمله نوع سوم ج) هیچ‌کدام د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۹. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۲۰. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به $\phi(n)$ اول باشد. ب) متن اصلی باید نسبت به $\phi(n)$ اول باشد.
ج) متن اصلی باید نسبت به n اول باشد. د) کلید عمومی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲۱. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۲۲. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه پیوند داده　　ب) لایه شبکه　　ج) لایه کاربرد　　د) لایه انتقال

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۲۳. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) انتشار - رمز - کلید　　ب) انتشار - آشکار - متن رمز

ج) گمراه کنندگی - آشکار - متن رمز　　د) گمراه کنندگی - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۲۴. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 4　　ب) 5　　ج) 3　　د) 6

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۲۵. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۶. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۲۷. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۲۸. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۲۹. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۳۰. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) E　　ب) F　　ج) S　　د) P

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۱. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۲. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) همه گزینه‌ها صحیح است.

ب) یک مساله از نوع روش‌های غیرتعاملی است.

ج) یک مساله از نوع اثبات دانایی صفر است.

د) یک مساله تسهیم راز است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۳. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 27 ب) 25 ج) 6 د) 2

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۴. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۵. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۶. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه پیوند داده　　ب) لایه کاربرد　　ج) لایه شبکه　　د) لایه انتقال

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۷. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۸. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob　　ب) کلید عمومی Alice　　ج) کلید عمومی Bob　　د) کلید محرمانه Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۹. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به n اول باشد.　　ب) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.

ج) متن اصلی باید نسبت به $\phi(n)$ اول باشد.　　د) متن اصلی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۱۰. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۱۱. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - رمز - کلید　　ب) گمراه کنندگی - آشکار - متن رمز

ج) انتشار - رمز - کلید　　د) انتشار - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۱۲. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۳. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Bob　　ب) کلید محرمانه Bob　　ج) کلید عمومی Alice　　د) کلید محرمانه Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۱۴. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۱۵. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۶. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۱۷. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۸. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۱۹. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۲۰. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 3 ب) 4 ج) 5 د) 6

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۲۱. طول واقعی کلید DES برابر است با .....

الف) ۵۶ ب) ۴۸ ج) ۶۴ د) ۳۲

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۲۲. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۲۳. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) E ب) F ج) P د) S

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۲۴. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن رمز شده - متن آشکار

ب) گمراه کنندگی - متن آشکار - متن رمز شده

ج) گمراه کنندگی - متن رمز شده - متن آشکار

د) انتشار - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۲۵. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 2 ب) 4 ج) 8 د) 6

پاسخ: این عدد ریشه اولیه ندارد.

۲۶. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 17 ب) 10 ج) 7 د) 34

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۲۷. رقم آخر عدد 3^{90} چند است؟

الف) 7 ب) 9 ج) 6 د) 8

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲۸. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام ب) حمله نوع سوم ج) حمله نوع اول د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۹. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۳۰. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام ب) حمله نوع اول ج) حمله نوع سوم د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice ب) کلید محرمانه Alice ج) کلید عمومی Bob د) کلید محرمانه Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۳. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۴. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 27 ب) 25 ج) 2 د) 6

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۵. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۶. طول واقعی کلید DES برابر است با .....

الف) ۴۸ ب) ۳۲ ج) ۶۴ د) ۵۶

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۷. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول ب) هیچ‌کدام ج) حمله نوع دوم د) حمله نوع سوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۸. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۹. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۰. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله تسهیم راز است.
ب) همه گزینه‌ها صحیح است.
ج) یک مساله از نوع اثبات دانایی صفر است.
د) یک مساله از نوع روش‌های غیرتعاملی است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۱۱. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.
ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$
د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۱۲. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) P
ب) S
ج) F
د) E

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۱۳. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.
ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.
ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.
د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۱۴. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به $\phi(n)$ اول باشد.
ب) متن اصلی باید نسبت به n اول باشد.
ج) کلید عمومی باید نسبت به n اول باشد.
د) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۱۵. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 7
ب) 17
ج) 34
د) 10

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۱۶. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۱۷. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 5 ب) 6 ج) 4 د) 3

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۱۸. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice ب) کلید محرمانه Bob ج) کلید عمومی Alice د) کلید عمومی Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۱۹. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 4 ب) 8 ج) 6 د) 2

پاسخ: این عدد ریشه اولیه ندارد.

۲۰. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - آشکار - متن رمز
ب) انتشار - آشکار - متن رمز
ج) انتشار - رمز - کلید
د) گمراه کنندگی - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۲۱. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن آشکار - متن رمز شده
ب) گمراه کنندگی - متن رمز شده - متن آشکار
ج) گمراه کنندگی - متن آشکار - متن رمز شده
د) انتشار - متن رمز شده - متن آشکار

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۲۲. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۳. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۲۴. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه کاربرد　　ب) لایه پیوند داده　　ج) لایه شبکه　　د) لایه انتقال

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۲۵. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۲۶. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۲۷. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۸. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول　　ب) هیچ‌کدام　　ج) حمله نوع سوم　　د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۹. رقم آخر عدد 3^{90} چند است؟

الف) 8　　ب) 9　　ج) 6　　د) 7

پاسخ: ✍ دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

✍ آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۳۰. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۱. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) E ب) P ج) S د) F

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۲. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۳. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 7 ب) 17 ج) 34 د) 10

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۴. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - رمز - کلید
ب) گمراه کنندگی - آشکار - متن رمز
ج) انتشار - آشکار - متن رمز
د) انتشار - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۵. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 8 ب) 4 ج) 6 د) 2

پاسخ: این عدد ریشه اولیه ندارد.

۶. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به n اول باشد.
ب) متن اصلی باید نسبت به $\phi(n)$ اول باشد.
ج) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
د) متن اصلی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۷. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.

- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۸. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن آشکار - متن رمز شده
ب) انتشار - متن رمز شده - متن آشکار
ج) گمراه کنندگی - متن رمز شده - متن آشکار
د) گمراه کنندگی - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۹. طول واقعی کلید DES برابر است با .....

الف) ۴۸
ب) ۵۶
ج) ۶۴
د) ۳۲

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۱۰. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 2
ب) 25
ج) 27
د) 6

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۱۱. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۱۲. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۳. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۴. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه انتقال
ب) لایه شبکه
ج) لایه کاربرد
د) لایه پیوند داده

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۱۵. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice
ب) کلید عمومی Alice
ج) کلید عمومی Bob
د) کلید محرمانه Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۱۶. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.
ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۷. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۱۸. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۹. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۰. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم　　ب) هیچ‌کدام　　ج) حمله نوع اول　　د) حمله نوع سوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۱. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۲۲. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۲۳. رقم آخر عدد 3^{90} چند است؟

الف) 9　　ب) 6　　ج) 8　　د) 7

پاسخ: ✍ دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲۴. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله تسهیم راز است.
ب) یک مساله از نوع اثبات دانایی صفر است.
ج) همه گزینه‌ها صحیح است.
د) یک مساله از نوع روش‌های غیرتعاملی است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۲۵. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۲۶. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم
ب) حمله نوع دوم
ج) هیچ‌کدام
د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۷. در SSH چگونه از حمله تغییر قابلیت‌های مشترک نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۲۸. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice　　ب) کلید عمومی Bob　　ج) کلید محرمانه Alice　　د) کلید محرمانه Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۲۹. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 3　　ب) 5　　ج) 6　　د) 4

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۳۰. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۱. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول　　ب) حمله نوع دوم　　ج) هیچ‌کدام　　د) حمله نوع سوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۳. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۴. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۵. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۶. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۷. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 27　　ب) 6　　ج) 2　　د) 25

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۸. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به n اول باشد.
ب) متن اصلی باید نسبت به $\phi(n)$ اول باشد.
ج) کلید عمومی باید نسبت به n اول باشد.
د) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۹. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) انتشار - رمز - کلید
ب) گمراه کنندگی - آشکار - متن رمز
ج) گمراه کنندگی - رمز - کلید
د) انتشار - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۱۰. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 4
ب) 8
ج) 2
د) 6

پاسخ: این عدد ریشه اولیه ندارد.

۱۱. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۱۲. طول واقعی کلید DES برابر است با .....

الف) ۴۸
ب) ۵۶
ج) ۶۴
د) ۳۲

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۱۳. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH

- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۱۴. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۵. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۶. رقم آخر عدد 3^{90} چند است؟

الف) 7 ب) 8 ج) 9 د) 6

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۱۷. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۱۸. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۹. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۲۰. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) P　　ب) E　　ج) F　　د) S

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۲۱. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم　　ب) حمله نوع سوم　　ج) هیچ‌کدام　　د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۲. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice　　ب) کلید عمومی Bob　　ج) کلید محرمانه Bob　　د) کلید عمومی Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲۳. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۲۴. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۲۵. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 5　　ب) 6　　ج) 3　　د) 4

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۲۶. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice
ب) کلید محرمانه Bob
ج) کلید عمومی Bob
د) کلید عمومی Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۲۷. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن رمز شده - متن آشکار
ب) انتشار - متن رمز شده - متن آشکار
ج) گمراه کنندگی - متن آشکار - متن رمز شده
د) انتشار - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۲۸. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله از نوع اثبات دانایی صفر است.
ب) همه گزینه‌ها صحیح است.
ج) یک مساله تسهیم راز است.
د) یک مساله از نوع روش‌های غیرتعاملی است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۲۹. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه شبکه
ب) لایه کاربرد
ج) لایه پیوند داده
د) لایه انتقال

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۳۰. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 7
ب) 34
ج) 10
د) 17

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

نام و نام خانوادگی	شماره دانشجویی	نام درس	تاریخ	شماره برگه
		امنیت سیستم‌های کامپیوتری	۱۴۰۳/۰۲/۱۱	۵۵

۱. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم　　ب) حمله نوع اول　　ج) هیچ‌کدام　　د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Bob　　ب) کلید عمومی Alice　　ج) کلید محرمانه Alice　　د) کلید محرمانه Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۳. طول واقعی کلید DES برابر است با .....

الف) ۳۲　　ب) ۵۶　　ج) ۴۸　　د) ۶۴

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۴. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن رمز شده - متن آشکار　　ب) گمراه کنندگی - متن آشکار - متن رمز شده
ج) انتشار - متن آشکار - متن رمز شده　　د) گمراه کنندگی - متن رمز شده - متن آشکار

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۵. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۶. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 5　　ب) 3　　ج) 6　　د) 4

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۷. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها

یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۸. رقم آخر عدد 3^{90} چند است؟

الف) 9 ب) 7 ج) 8 د) 6

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۹. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۰. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۱۱. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله از نوع اثبات دانایی صفر است. ب) یک مساله تسهیم راز است.
ج) همه گزینه‌ها صحیح است. د) یک مساله از نوع روش‌های غیرتعاملی است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۱۲. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم ب) حمله نوع سوم ج) هیچ‌کدام د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۳. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۱۴. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۵. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۱۶. در SSH چگونه از حمله تغییر قابلیت‌های مشترک نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۱۷. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۸. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۱۹. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 6 ب) 4 ج) 8 د) 2

پاسخ: این عدد ریشه اولیه ندارد.

۲۰. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۲۱. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۲۲. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه پیوند داده ب) لایه انتقال ج) لایه کاربرد د) لایه شبکه

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۲۳. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۲۴. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 7 ب) 34 ج) 10 د) 17

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۲۵. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به n اول باشد.
ب) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
ج) متن اصلی باید نسبت به n اول باشد.
د) متن اصلی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲۶. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) P
ب) S
ج) F
د) E

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۲۷. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 2
ب) 27
ج) 6
د) 25

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۲۸. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۹. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice
ب) کلید محرمانه Bob
ج) کلید عمومی Bob
د) کلید محرمانه Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۳۰. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - رمز - کلید
ب) انتشار - آشکار - متن رمز
ج) گمراه کنندگی - آشکار - متن رمز
د) انتشار - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

نام و نام خانوادگی	شماره دانشجویی	نام درس	تاریخ	شماره برگه
		امنیت سیستم‌های کامپیوتری	۱۴۰۳/۰۲/۱۱	۵۶

۱. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۲. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن آشکار - متن رمز شده

ب) انتشار - متن رمز شده - متن آشکار

ج) گمراه کنندگی - متن رمز شده - متن آشکار

د) انتشار - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۳. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۴. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 34

ب) 10

ج) 7

د) 17

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۵. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - رمز - کلید

ب) انتشار - آشکار - متن رمز

ج) انتشار - رمز - کلید

د) گمراه کنندگی - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۶. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۷. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۸. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به $\phi(n)$ اول باشد.

ب) کلید عمومی باید نسبت به n اول باشد.

ج) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.

د) متن اصلی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۹. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۱۰. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 3 ب) 6 ج) 5 د) 4

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۱۱. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۲. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام ب) حمله نوع دوم ج) حمله نوع اول د) حمله نوع سوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۳. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 6 ب) 8 ج) 4 د) 2

پاسخ: این عدد ریشه اولیه ندارد.

۱۴. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۱۵. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۱۶. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۱۷. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۱۸. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله تسهیم راز است.
ب) همه گزینه‌ها صحیح است.
ج) یک مساله از نوع اثبات دانایی صفر است.
د) یک مساله از نوع روش‌های غیرتعاملی است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۱۹. رقم آخر عدد 3^{90} چند است؟

الف) 8
ب) 6
ج) 9
د) 7

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲۰. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه انتقال
ب) لایه شبکه
ج) لایه کاربرد
د) لایه پیوند داده

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۲۱. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۲. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 6
ب) 27
ج) 2
د) 25

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۲۳. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice
ب) کلید عمومی Alice
ج) کلید محرمانه Bob
د) کلید عمومی Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲۴. طول واقعی کلید DES برابر است با .....

الف) ۵۶
ب) ۳۲
ج) ۶۴
د) ۴۸

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۲۵. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice
ب) کلید محرمانه Bob
ج) کلید محرمانه Alice
د) کلید عمومی Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۲۶. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع اول　　ب) هیچ‌کدام　　ج) حمله نوع سوم　　د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۷. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) F　　ب) S　　ج) E　　د) P

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۲۸. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۹. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۳۰. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۱. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 10 ب) 34 ج) 7 د) 17

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۲. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) همه گزینه‌ها صحیح است.
ب) یک مساله تسهیم راز است.
ج) یک مساله از نوع روش‌های غیرتعاملی است.
د) یک مساله از نوع اثبات دانایی صفر است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۳. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 5 ب) 6 ج) 4 د) 3

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۴. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 25 ب) 6 ج) 2 د) 27

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۵. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.
ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.
ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.
د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۶. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه پیوند داده ب) لایه کاربرد ج) لایه انتقال د) لایه شبکه

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۷. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) F ب) E ج) S د) P

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۸. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 2 ب) 6 ج) 8 د) 4

پاسخ: این عدد ریشه اولیه ندارد.

۹. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۱۰. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۱۱. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۱۲. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۳. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام　　ب) حمله نوع اول　　ج) حمله نوع سوم　　د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۴. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۱۵. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به n اول باشد.　　ب) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.

ج) متن اصلی باید نسبت به $\phi(n)$ اول باشد.　　د) کلید عمومی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۱۶. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۱۷. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - آشکار - متن رمز　　ب) انتشار - آشکار - متن رمز

ج) انتشار - رمز - کلید　　د) گمراه کنندگی - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۱۸. رقم آخر عدد 3^{90} چند است؟

الف) 9 ب) 8 ج) 7 د) 6

پاسخ: ✍ دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

✍ آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۱۹. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۲۰. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۱. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice ب) کلید محرمانه Bob ج) کلید محرمانه Alice د) کلید عمومی Bob

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۲۲. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۲۳. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۴. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن رمز شده - متن آشکار ب) انتشار - متن آشکار - متن رمز شده

ج) گمراه کنندگی - متن آشکار - متن رمز شده د) گمراه کنندگی - متن رمز شده - متن آشکار

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۲۵. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob ب) کلید عمومی Alice ج) کلید محرمانه Alice د) کلید عمومی Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲۶. طول واقعی کلید DES برابر است با .....

الف) ۵۶ ب) ۴۸ ج) ۶۴ د) ۳۲

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۲۷. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۸. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۲۹. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۳۰. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام ب) حمله نوع دوم ج) حمله نوع سوم د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 5 ب) 6 ج) 3 د) 4

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۲. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم ب) حمله نوع اول ج) هیچ‌کدام د) حمله نوع سوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۳. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۴. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۵. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۶. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه شبکه　　ب) لایه انتقال　　ج) لایه کاربرد　　د) لایه پیوند داده

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۷. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به $\phi(n)$ اول باشد.　　ب) متن اصلی باید نسبت به n اول باشد.

ج) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.　　د) کلید عمومی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۸. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن آشکار - متن رمز شده　　ب) گمراه کنندگی - متن رمز شده - متن آشکار

ج) انتشار - متن رمز شده - متن آشکار　　د) انتشار - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۹. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۱۰. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۱. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۱۲. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Bob ب) کلید عمومی Alice ج) کلید محرمانه Bob د) کلید محرمانه Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۱۳. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - آشکار - متن رمز ب) گمراه کنندگی - رمز - کلید
ج) انتشار - آشکار - متن رمز د) انتشار - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۱۴. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.
ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.
ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.
د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۱۵. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 17 ب) 34 ج) 10 د) 7

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۱۶. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Alice ب) کلید عمومی Bob ج) کلید محرمانه Alice د) کلید محرمانه Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۱۷. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا
ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا
ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن
د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۱۸. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 27 ب) 25 ج) 6 د) 2

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۱۹. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۰. طول واقعی کلید DES برابر است با .....

الف) ۳۲ ب) ۶۴ ج) ۴۸ د) ۵۶

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۲۱. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۲۲. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۳. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۲۴. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 6 ب) 4 ج) 8 د) 2

پاسخ: این عدد ریشه اولیه ندارد.

۲۵. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله از نوع روش‌های غیرتعاملی است. ب) یک مساله تسهیم راز است.
ج) یک مساله از نوع اثبات دانایی صفر است. د) همه گزینه‌ها صحیح است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۲۶. رقم آخر عدد 3^{90} چند است؟

الف) 7 ب) 9 ج) 6 د) 8

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.

- عدد سه و ده نسبت به هم اول هستند، یعنی $(3,10)=1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

✍ آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲۷. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۲۸. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) E　　ب) F　　ج) S　　د) P

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۲۹. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۳۰. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم　　ب) حمله نوع سوم　　ج) حمله نوع اول　　د) هیچ‌کدام

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به $\phi(n)$ اول باشد.
ب) متن اصلی باید نسبت به n اول باشد.
ج) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
د) کلید عمومی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۲. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۳. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع سوم
ب) حمله نوع اول
ج) هیچ‌کدام
د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۴. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) گمراه کنندگی - متن آشکار - متن رمز شده
ب) گمراه کنندگی - متن رمز شده - متن آشکار
ج) انتشار - متن آشکار - متن رمز شده
د) انتشار - متن رمز شده - متن آشکار

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.

۵. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا
ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا
ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن
د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۶. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 34 ب) 17 ج) 7 د) 10

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۷. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 2 ب) 4 ج) 6 د) 8

پاسخ: این عدد ریشه اولیه ندارد.

۸. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۹. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۰. در SSH چگونه از حمله تغییر قابلیت‌های مشترک نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشترک ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۱۱. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۱۲. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۱۳. رقم آخر عدد 3^{90} چند است؟

الف) 9 ب) 8 ج) 7 د) 6

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۱۴. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۱۵. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۶. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۱۷. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۱۸. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 25 ب) 2 ج) 27 د) 6

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۱۹. طول واقعی کلید DES برابر است با .....

الف) ۴۸ ب) ۵۶ ج) ۶۴ د) ۳۲

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۲۰. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) حمله نوع دوم ب) هیچ‌کدام ج) حمله نوع سوم د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۲۱. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۲۲. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید عمومی Bob ب) کلید محرمانه Bob ج) کلید عمومی Alice د) کلید محرمانه Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۲۳. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۴. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Bob ب) کلید عمومی Bob ج) کلید عمومی Alice د) کلید محرمانه Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲۵. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) یک مساله از نوع اثبات دانایی صفر است. ب) یک مساله از نوع روش‌های غیرتعاملی است.

ج) همه گزینه‌ها صحیح است. د) یک مساله تسهیم راز است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۲۶. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - آشکار - متن رمز
ب) انتشار - رمز - کلید
ج) گمراه کنندگی - رمز - کلید
د) انتشار - آشکار - متن رمز

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۲۷. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه کاربرد
ب) لایه شبکه
ج) لایه پیوند داده
د) لایه انتقال

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۲۸. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۲۹. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 6
ب) 4
ج) 5
د) 3

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۳۰. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) P
ب) S
ج) E
د) F

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

نام و نام خانوادگی	شماره دانشجویی	نام درس	تاریخ	شماره برگه
		امنیت سیستم‌های کامپیوتری	۱۴۰۳/۰۲/۱۱	۶۰

۱. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف) 2 ب) 4 ج) 6 د) 8

پاسخ: این عدد ریشه اولیه ندارد.

۲. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۳. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)

الف) توافق کلید (Key Agreement): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

ج) تعداد کلید در الگوریتم‌های نامتقارن بین n نفر برای برقراری ارتباط، برابر با $\binom{n}{2}$

د) هیچ‌کدام از گزینه‌ها صحیح نیست

پاسخ: هیچ‌کدام از گزینه‌ها صحیح نیست. در اسلایدها داشتیم که استفاده از سازوکارهای برقراری کلید (Key Establishment):

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.

از سوی‌دیگر، تعداد کلید برای الگوریتم‌های متقارن است نه نامتقارن

۴. اعضای مجموعه $\mathbb{Z}_{17}^*$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 10 ب) 17 ج) 7 د) 34

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۵. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام ب) حمله نوع اول ج) حمله نوع سوم د) حمله نوع دوم

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۶. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **ب** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ:

- **الف** این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- **ب** بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله‌گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۷. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟ در تمام مراحل یکپارچگی پیام‌ها حفظ می‌شود در تمام مراحل پیام‌ها با کلید نامتقارن رمز می‌شود در مراحل انتهایی، کل پیام‌های مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می‌شود. هیچ‌کدام

پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

- Client Identification Id: SSH-2.0-libssh_0.9.3
- Server Identification Id: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
- Client Key Exchange Init
- Server Key Exchange Init
- Server Public Key for signature (Host Key)
- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این‌که این چکیده تولید شد، خدمت‌گزار آن را با کلید عمومی خودش امضا می‌کند.

۸. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟

الف) طول کلید می‌بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلی با کلید است.

د) شکستن این رمز عملا نیاز به یک زمان بسیار طولانی و پردازش زیاد دارد.

پاسخ: در رمز One Time Pad یک دنباله کلید (Key Sequence) داریم به اندازه طول متن اصلی. این الگوریتم، بر این اصل استوار است که هر کاراکتر متن اصلی با یک کاراکتر از کلید ترکیب می‌شود (بیت به بیت با یکدیگر XOR شود). اگر از یک دنباله کلید واقعا تصادفی استفاده شود، نتیجه یک متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه‌ای ویژگی امنیت بدون شرط را دارد. بدین‌سان می‌توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۹. کدام گزینه صحیح است؟ (شاید چند گزینه پاسخ باشد)

الف) الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.

ب) در یک شبکه، الگوریتم‌های کلید متقارن نسبت به الگوریتم کلید نامتقارن به تعداد کلید کمتری احتیاج دارند.

ج) امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.

د) در الگوریتم‌های کلید نامتقارن در صورت داشتن سازوکاری به مانند گواهینامه، نیازی به کانال امن نداریم.

پاسخ: به جز گزینه (امنیت بسیاری از الگوریتم‌های کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینه‌ها درست است.

۱۰. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۸ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۱۱. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) همه گزینه‌ها صحیح است.

ب) یک مساله از نوع اثبات دانایی صفر است.

ج) یک مساله تسهیم راز است.

د) یک مساله از نوع روش‌های غیرتعاملی است.

پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است.

۱۲. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا

ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی

پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۱۳. روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) **پاسخ:** پاسخ این سوال در اسلایدها است.

۱۴. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به $\phi(n)$ اول باشد.
ب) متن اصلی باید نسبت به n اول باشد.
ج) کلید عمومی باید نسبت به n اول باشد.
د) متن اصلی باید نسبت به $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

۱۵. طول واقعی کلید DES برابر است با .....

الف) ۶۴
ب) ۴۸
ج) ۵۶
د) ۳۲

پاسخ: گزینه‌ی "۵۶" صحیح می‌باشد.

۱۶. برای این‌که Alice پیامی را برای Bob امضا کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice
ب) کلید محرمانه Bob
ج) کلید عمومی Bob
د) کلید عمومی Alice

پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می‌کند.

۱۷. اثبات کنید که اگر $n = pq$ باشد، آن‌گاه $\phi(n) = (p-1)(q-1)$ ؟ (سوال تشریحی) **پاسخ:** این مورد در کلاس توضیح داده شد.

۱۸. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حمله‌ای صورت پذیرفت؟

الف) هیچ‌کدام
ب) حمله نوع سوم
ج) حمله نوع دوم
د) حمله نوع اول

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین Enigma و A5/2 در شبکه‌های نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۱۹. ویژگی ..... به این معنا است که هر بین از متن ..... باید به چندین قسمت ..... وابسته باشد.

الف) گمراه کنندگی - آشکار - متن رمز
ب) انتشار - آشکار - متن رمز
ج) انتشار - رمز - کلید
د) گمراه کنندگی - رمز - کلید

پاسخ: گزینه‌ی "گمراه کنندگی - رمز - کلید" صحیح می‌باشد.

۲۰. این قضیه را اثبات کنید: اگر دو عدد a و n نسبت به همدیگر اول باشند، آن‌گاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** اگر $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ مجموع کاهش‌یافته مانده‌ها باشد، آن‌گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده‌ها یعنی $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

$$\prod_{i=1}^{\phi(n)} (ar_i \mod n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right)\left(\prod_{i=1}^{\phi(n)} r_i\right) = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

۲۱. برای این‌که Alice پیامی را برای Bob رمز کند، می‌بایست آن را با ..... رمز کند و برای Bob ارسال کند.

الف) کلید محرمانه Alice ب) کلید عمومی Alice ج) کلید محرمانه Bob د) کلید عمومی Bob

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می‌کند.

۲۲. کدام گزینه صحیح نیست؟ (می‌توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.

ب) امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

د) در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه‌ها صحیح است.

۲۳. رقم آخر عدد 3^{90} چند است؟

الف) 6 ب) 7 ج) 9 د) 8

پاسخ: دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:

- $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
- عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
- برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$

آن‌گاه براحتی می‌توانیم بنویسیم که:

$$3^{90} = 3^{4\times 22+2} = (3^4)^{22} \times (3^2) = 9 \pmod{10}.$$

۲۴. PGP امنیت را در کدام لایه برای ما به ارمغان می‌آورد؟

الف) لایه انتقال ب) لایه شبکه ج) لایه پیوند داده د) لایه کاربرد

پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است.

۲۵. کدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می‌شود(به طور دقیق).

الف) F ب) S ج) P د) E

پاسخ: گزینه‌ی "S" صحیح می‌باشد.

۲۶. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می‌شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه‌حل نمره ندارد.

۲۷. اگر در الگوریتم RSA مقدار $n = 35$ و مقدار $e = 5$ باشد، آن‌گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 4 ب) 5 ج) 3 د) 6

پاسخ: گزینه صحیح عدد پنج است. همان‌طور که می‌دانید، پارامتر e را به عنوان کلید عمومی در نظر می‌گیریم، به‌گونه‌ای که

$$1 < e < \phi(n), \quad (e, \phi(n)) = 1.$$

پارامتر d را به عنوان کلید محرمانه در نظر می‌گیریم، به گونه‌ای که:

$$ed \equiv 1 \pmod{\phi(n)},$$

پس ابتدا $\phi(n)$ را محاسبه می‌کنیم که برابر با $\phi(35) = 24$ خواهد شد. سپس باید معکوس عدد $e = 5$ در پیمانه 24 را محاسبه کنیم که برابر با 5 خواهد شد.

۲۸. کدام یک از جملات زیر صحیح است و کدام غلط؟ لطفا جلوی آن عبارت صحیح/غلط را بنویسید.

- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی‌که علی‌رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ‌گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی‌کند.
- **ب** امنیت محاسباتی (Computational Security) یعنی در صورتی‌که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
- **ج** تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- **د** در یک سامانه رمزگذاری، ما به‌صورت غیرعمد می‌خواهیم یک نویز به متن اصلی اضافه کنیم. حمله‌گر در صورت مشاهده متن رمز، نباید به هیچ‌گونه اطلاعاتی در مورد متن اصلی پی ببرد.
- **ه** سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.
- **و** دشمن از تمامی جزئیات سامانه رمزگذاری آگاهی دارد.

پاسخ: در یک سامانه رمزگذاری، ما به‌صورت عمدی می‌خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه‌ها صحیح است.

۲۹. کدام یک از اعداد زیر ریشه اولیه (Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

الف) 6 ب) 27 ج) 25 د) 2

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.

۳۰. طبق گفته شانون یک سامانه قوی ویژگی ..... را دارد که به این معنا است ساختاری آماری ..... رو حجم وسیعی از ..... پراکنده است.

الف) انتشار - متن رمز شده - متن آشکار
ب) انتشار - متن آشکار - متن رمز شده
ج) گمراه کنندگی - متن رمز شده - متن آشکار
د) گمراه کنندگی - متن آشکار - متن رمز شده

پاسخ: گزینه‌ی "انتشار - متن آشکار - متن رمز شده" صحیح می‌باشد.