شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
١	14.4/.4/11	امنیت سیستمهای کامپیوتری		

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

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.

- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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.

ب) گمراه کنندگی - متن آشکار - متن رمز شده

الف) انتشار - متن آشكار - متن رمز شده

د) گمراه کنندگی - متن رمز شده - متن آشکار

ج) انتشار - 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 راه حل نمره ندارد.

۴. كدام يك از اعداد زير ريشه اوليه (Primitive Root) دارند؟ (ممكن است چند گزينه صحيح باشد)

25 (ء 27 ج) 25 (ء طف) 6

پاسخ: اثبات می شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1,2,4,p^k,2 imes p^k\}$. بنابراین همه گزینه های فوق ریشه اولیه دارند.

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

ب) انتشار - آشکار - متن رمز

الف) انتشار - رمز - كليد

د) گمراه کنندگی - رمز - کلید

ج) گمراه کنندگی - آشکار - متن رمز

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

كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

P (د S (ج E (ب F (الف)

پاسخ: گزینهی "S" صحیح میباشد.

- ۷. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- 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.

ىاسخ:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمني دارد.
- ببله 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

9	۸. کدام گزینه در مورد PGP صحیح است	
نجام میشود بعد فشرده سازی و بعد امضا	الف) در PGP اول عملیات رمزنگاری	
ی انجام می شود بعد رمزنگاری و بعد امضا	ب) در PGP اول عملیات فشردهساز	

ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن

د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

یاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، 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؟

4 (ب د) 6 3 (~ الف) 5

یاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، یارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

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

ان رقم آخر عدد 3^{90} چند است 3^{90} است

ج) 8 د) 7 6 (ت الف) 9

پاسخ: 🕰 دقت کنید که در واقع ما به دنبال پاسخ (10 mod 10) 3^{90} هستم. میدانیم که:

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

🗀 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 علی بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

ب) یک مساله از نوع روشهای غیرتعاملی است.

الف) یک مساله از نوع اثبات دانایی صفر است.

د) یک مساله تسهیم راز است.

ج) همه گزینهها صحیح است.

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

١٢. كدام گزينه صحيح است؟ (شايد چند مورد صحيح باشد)

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن ١٣. تعداد ريشه اوليه عدد 60 كدام گزينه است؟ ₂ (ج د) 4 6 (ب الف) 8 **پاسخ:** این عدد ریشه اولیه ندارد. ۱۴. برای این که Alice پیامی را برای Bob امضا کند، می بایست آن را با رمز کند و برای Bob ارسال کند. د) کلید عمومی Bob ج) كليد محرمانه Bob ب) كليد محرمانه Alice الف) كليد عمومي Alice پاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می کند. ۱۵. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد. - الف امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچگونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند. - 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. - در یک سامانه رمزگذاری، ما بهصورت غیرعمد می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر 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 <u>بهصورت عمدی می</u>خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ايمني دارد. مابقي گزينهها صحيح است. ۱۶. مقدار ($\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد. ۱۷. برای این که Alice پیامی را برای Bob رمز کند، می بایست آن را با رمز کند و برای Bob ارسال کند. د) کلید عمومی Bob ج) کلید عمومی Alice ب) كليد محرمانه Alice الف) كليد محرمانه Bob پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می کند. ۸۱. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حملهای صورت پذیرفت؟ د) حمله نوع دوم ج) حمله نوع سوم ب) هیچکدام الف) 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.

الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.

• تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می دهد.

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

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

● توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

 $\binom{n}{2}$ برابر با روزاری ارتباط، برابر با نفر برای برقراری ارتباط، برابر با روزاری ارتباط، برابر با

د) هیچکدام از گزینهها صحیح نیست

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؟

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

د) کلید عمومی باید نسبت به n اول باشد.

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

ج) متن اصلی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای 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) هيچ كدام 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 كليد مي بايست برابر با طول متن اصلى 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

.۲۳ این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها اشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a یعنی a a در مجموعه کامل از مجموعه اولیه است. پس داریم:

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

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

الف) لايه كاربرد ب) لايه پيوند داده ج) لايه شبكه د) لايه 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 \mathbb{Z}_{17}^* (ممکن است چند گزینه صحیح باشد)

10 (د) 17 (ج على على الله) 7 الله) 7

پاسخ: اگر $\{x_1,x_2,\dots,x_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد x_n در مجموعه کاهش یافته مانده ها یعنی $\{ar_1,ar_2,\dots,ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر x_n باشد. پس پاسخ اعداد 10 و 7 است.

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

۲۷. طول واقعی کلید DES برابر است با

الف) ۶۴ (ع بر ۲۳ ج) ۸۶ (ج

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.

یاسخ: 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 مشتری نظیر الگوریتمهای رمزنگاری مورد پشتیبانی جلوگیری می شود؟ در تمام مراحل یکپارچگی پیامها حفظ می شود در تمام مراحل پیامها با کلید نامتقارن رمز می شود در مراحل انتهایی، کل پیامهای مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می شود. هیچ کدام

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

۳۰. اثبات کنید که اگر p=pq باشد، آن گاه (p-1)(q-1) ((p-1)(q-1) (سوال تشریحی) پاسخ: این مورد در کلاس توضیح داده شد.



شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
٢	14.47.411	امنیت سیستمهای کامپیوتری		

- 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 راه حل 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)

7 (د) 71 (الف) 17 جا

پاسخ: اگر $\{r_1, r_2, \dots, r_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آن گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1, ar_2, \dots, ar_{\phi(n)}\}$ باشد. پس پاسخ اعداد 10 و 7 است.

- ٣. پروتكل توافق كليد ديفي-هلمن را توضيح دهيد؟ (سوال تشريحي) **پاسخ:** پاسخ اين سوال در اسلايدها است.
 - ۴. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حملهای صورت پذیرفت؟

الف) حمله نوع اول ب) حمله نوع دوم ج) هيچ كدام 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 می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

یاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

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

الف) گمراه کنندگی - رمز - کلید ج) انتشار - آشکار - متن رمز داندگی - آشکار - متن رمز داندگی - آشکار - متن رمز

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

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

یاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 ECDHShared Session Key

بعد از این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

٨. تعداد ريشه اوليه عدد 60 كدام گزينه است؟

پاسخ: این عدد ریشه اولیه ندارد.

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

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

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

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

۱۱. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.

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

الف) حمله نوع دوم ب) هيچكدام 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. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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. كدام قسمت الكوريتم DES باعث غير خطى شدن سامانه مي شود (به طور دقيق).

S (د) P (ج E (ب F (الف)

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.

یاسخ:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمني دارد.
- ببله 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.
 - ۱۷. برای این که Alice پیامی را برای Bob رمز کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد محرمانه Bob ب) كليد عمومي Bob ج) كليد محرمانه Bob د) كليد عمومي

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

۱۸. کدام شرط در مورد RSA الزامی است؟

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

الف) متن اصلی باید نسبت به n اول باشد.

د) کلید عمومی باید نسبت به n اول باشد.

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

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

۱۹. اثبات کنید که اگر p=pq باشد، آنگاه (p-1)(q-1) ((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 كليد مي بايست برابر با طول متن اصلى باشد.

- ب) کلید باید به صورت کاملا تصادفی تولید شود.
- ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان 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)

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

ب) یک مساله از نوع روشهای غیرتعاملی است.

الف) یک مساله تسهیم راز است.

د) یک مساله از نوع اثبات دانایی صفر است.

ج) همه گزینهها صحیح 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 كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.

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

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

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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

۲۴. طول واقعی کلید DES برابر است با

الف) ۶۴ (ب سر) ۳۲ ج) ۵۶ د) ۴۸ د)

پاسخ: گزینهی "۵۶" صحیح میباشد.

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

- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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، آن گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

3 (د) 3 (ح) 5 (ج) 4 (لف)

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

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

ب) گمراه کنندگی - متن رمز شده - متن آشکار

د) انتشار - متن رمز شده - متن آشکار

الف) گمراه کنندگی - متن آشکار - متن رمز شده

ج) انتشار - متن آشکار - متن رمز شده

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

۲۹. رقم آخر عدد 3^{90} چند است؟

7 (ه 9 (الف) 9

پاسخ: 🕰 دقت کنید که در واقع ما به دنبال پاسخ (10 3^{90} هستم. میدانیم که:

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

🗀 آنگاه براحتی می توانیم بنویسیم که:

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

۳۰. برای این که Alice پیامی را برای Bob امضا کند، می بایست آن را با رمز کند و برای Bob ارسال کند.

ج) کلید عمومی Alice د) کلید عمومی

ب) کلید محرمانه Bob

الف) كليد محرمانه Alice

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

ماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
٣	14.4/.4/11	امنیت سیستمهای کامپیوتری		

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

الف) لايه انتقال ب) لايه شبكه ج) لايه كاربرد 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.

 3^{90} . رقم آخر عدد 3^{90} چند است

7 (د) 8 (ج) 8 (الف) 8

پاسخ: 🛍 دقت کنید که در واقع ما به دنبال پاسخ (10 mod 10) هستم. می دانیم که:

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

🖾 آن گاه 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؟

4 (ه و الف) 2 (ج الف) 6

یاسخ: 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 علی بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

ب) یک مساله از نوع روشهای غیرتعاملی است.

الف) همه گزینهها صحیح است.

د) یک مساله از نوع اثبات دانایی صفر است.

ج) یک مساله تسهیم راز است.

یاسخ: 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

یاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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

 Shared Session Key بعد از این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند. ۸. کدام گزینه در مورد PGP صحیح است؟ الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی **یاسخ:** همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی و بعد عملیات رمزگذاری. ۹. برای این که Alice پیامی را برای Bob رمز کند، می بایست آن را با رمز کند و برای Bob ارسال کند. د) کلید محرمانه Alice ج) كليد محرمانه Bob ب) کلید عمومی Alice الف) كليد عمومي Bob پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می کند. ۱۰. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **یاسخ:** برابر با ۸ میشود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد. ١١. كدام گزينه صحيح است؟ (شايد چند مورد صحيح باشد) الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد. ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند. $\binom{n}{2}$ برابر با روزاری ارتباط، برابر با نفر برای برقراری ارتباط، برابر با روزاری ارتباط، برابر با د) هیچکدام از گزینهها صحیح نیست یاسخ: 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 می دهد. • توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند. از سوی دیگر، 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 د) 6 2 (₇ 25 (ت $m{y}$ پاسخ: اثبات می شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1,2,4,p^k,2 imes p^k\}$. 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 د) 7 ج) 10 ب) 17 پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \dots, r_{\phi(n)}\}$ مجموع کاهشیافته ماندهها باشد، آن گاه مجموعه حاصل شده از ضرب عدد $\mathbb{Z}_n^* = \{r_1, r_2, \dots, r_{\phi(n)}\}$ مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ باشد.

Server Key Exchange Init

Client Public Key for ECDH

• Server Public Key for ECDH

• Server Public Key for signature (Host Key)

این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آن گاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a و a نسبت به همدیگر اول باشند، آن گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها اگر a در مجموعه کاهش یافته مانده ها باشد، آن گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a یعنی a یک جایگشت کامل از مجموعه اولیه است. پس داریم:

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

14. كدام قسمت الكوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

E (ع E (ج P (ب S الف)

پاسخ: گزینهی "S" صحیح میباشد.

۱۶. اثبات کنید که اگر p=pq باشد، آن گاه (p-1)(q-1) ((p-1)(q-1) ۱۶) (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) هيچ كدام

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 این که Alice پیامی را برای Bob امضا کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد عمومي Alice ب) كليد عمومي Bob ج) كليد محرمانه عمومي

یاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می کند.

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

4 (ه 5 (ب 3 الف) 3

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

یارامتر d را به عنوان کلید محرمانه در نظر می گیریم، به گونهای که:

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

5 پس ابتدا $\phi(n)$ را محاسبه می کنیم که برابر با $\phi(35)=\phi(35)=\phi(35)=0$ خواهد شد. سپس باید معکوس عدد e=5 در پیمانه $\phi(n)$ محاسبه کنیم که برابر با خواهد شد.

- ۲۰. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟
 - الف) طول كليد مي بايست برابر با طول متن اصلي باشد.
 - ب) کلید باید به صورت کاملا تصادفی تولید شود.
 - ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد است.
- د) شکستن این رمز عملانیاز 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 متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

- ۲۱. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 <u>بهصورت عمدی می</u>خواهیم 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) هيچكدام 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 (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل 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 بالف) گمراه کنندگی متن آشکار متن رمز شده
 - ج) انتشار متن آشکار 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 صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.

پاسخ: در یک سامانه رمزگذاری، ما به صورت عمدی می خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه ها صحیح است.

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

الف) گمراه کنندگی - رمز - کلید بالف) گمراه کنندگی - رمز - کلید

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

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

۲۷. كدام شرط در مورد RSA الزامي است؟

ب) کلید عمومی باید نسبت به n اول باشد.

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

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

ج) متن اصلی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

۲۸. طول واقعی کلید DES برابر است با

94 (ع ج) 48 (ج با 48 ما با 48

پاسخ: گزینهی "۵۶" صحیح میباشد.

۲۹. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.

- 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.

یاسخ:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمني دارد.
- ببله 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.
 - ٣٠. كدام گزينه صحيح است؟ (شايد چند گزينه ياسخ باشد)
 - الف) الگوریتمهای کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.
 - ب) دریک 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.

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

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
*	14.47.4711	امنیت سیستمهای کامپیوتری		

- 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 راه حل نمره ندارد.
 - ۲. کدام گزینه صحیح نیست؟ (میتوانید چند گزینه را انتخاب کنید).
- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به صورت عمدی می خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه ها صحیح است.

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

الف) حمله نوع اول ب) حمله نوع سوم ج) هيچكدام 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: یاسخ این سوال در اسلایدها است.
 - $^{\circ}$. رقم آخر عدد 90 چند است؟

پاسخ: 🕰 دقت کنید که در واقع ما به دنبال پاسخ (10 3^{90} هستم. میدانیم که:

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

🔼 آن گاه براحتی می توانیم بنویسیم که:

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

- ۶. كدام گزينه صحيح است؟ (شايد چند گزينه 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.

٧. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.

- ۔ **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.
- ۔ دوریک سامانه رمزگذاری، ما بهصورت غیرعمد میخواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه اطلاعاتی در مورد متن اصلی یی 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 گزینه ها 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: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

9. این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** a اگر دو عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a یعنی a 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 كليد مي بايست برابر با طول متن اصلى باشد.
 - ب) کلید باید به صورت کاملا تصادفی تولید شود.
 - ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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 متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانهای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

ىدھد.	ِده و در اختیار طرف مقابل نیز قرار م	Key Ag): یک سمت کلید را تولید کر	الف) توافق كليد (greement
	ند تولید کلید مشارکت میکنند.	Key Establis): هر دو سمت، در فراین	ehment) برقراری کلید (shment
	$\binom{n}{2}$ ارتباط، برابر با	های نامتقارن بین n نفر برای برقراری	ج) تعداد كليد در الگوريتم
		حيح نيست	د) هیچکدام از گزینهها ص
ید (Key Establishment):	ه استفاده از سازوکارهای برقراری کلی	صحیح نیست. در اسلایدها داشتیم ک	پاسخ: هیچکدام از گزینهها ه
ردهد.	ه و در اختیار طرف مقابل نیز قرار می	Key T): یک سمت کلید را تولید کرد	ransport) تبادل کلید
	ید کلید مشارکت میکنند.	Key Ag): هر دو سمت، در فرایند تول	• توافق كليد (greement
ی الگوریتمهای متقارن است نه نامتقار	از سوی دیگر، تعداد کلید برای		
		عیح است؟	۱۲. کدام گزینه در مورد PGP صح
	ری و بعد امضا	مزنگاری انجام میشود بعد فشردهساز	الف) در PGP اول عملیات ره
	ِی و بعد امضا	شردهسازی انجام میشود بعد رمزنگار	ب) در PGP اول عمليات ف
	بعد رمزکردن	بضا انجام میشود بعد فشردهسازی و	ج) در PGP اول عمليات اه
	فشردهسازى	ىضا انجام مىشود بعد رمزكردن و بعد	د) در PGP اول عملیات ام
ند فشردهسازی و بعد عملیات رمزگذار _؟	نای دیجیتال بر روی پیام میخورد، به	ں نیز مطرح شد، در PGP اول یک امض	پاسخ: همانطور که در کلاس
		ِای ما به ارمغان میآورد؟	PGP .۱۳ امنیت را در کدام لایه بر
د) لايه پيوند داده	ج) لايه شبكه	ب) لايه كاربرد	الف) لايه انتقال
		برد (Application Layer) است.	ياسخ: گزينه صحيح لايه كار،
			۱۴. کدام شرط در مورد RSA الزاه
		G	33 3 3 1
ه $\phi(n)$ اول باشد.	ب) متن اصلی باید نسبت بد	ت به $\phi(n)$ اول باشد.	الف) کلید عمومی باید نسبن
ه n اول باشد.	د) متن اصلی باید نسبت به	ت به n اول باشد.	ج) کلید عمومی باید نسبن
	ای که	للید عمومی در نظر می گیریم، به گونها	پاسخ: پارامتر e را به عنوان ک
	$1 < e < \phi(n), (e, \cdot)$	$\phi(n)) = 1.$	
		ست با	۱۵. طول واقعی کلید DES برابر ا
WY (3	ج) ۴۸	ب) ۵۶	الف) ۶۴
		مى باشد.	یاسخ: گزینهی "۵۶" صحیح
د.	رمز کند و برای Bob ارسال کن	ای Bob رمز کند، میبایست آن را با .	
د) کلید محرمانه Alice	ج) کلید محرمانه Bob	ب) کلید عمومی Alice	الف) كليد عمومي Bob
	ده و برای او ارسال می کند.	پیام m را با کلید عمومی Bob رمز کر	پاسخ: Alice برای رمزکردن،
	, قسمت وابسته باشد.	که هر بین از متن باید به چندین	۱۷. ویژگی به این معنا است

۱۱. كدام گزينه صحيح است؟ (شايد چند مورد صحيح باشد)

الف) انتشار - رمز - کلید ج) انتشار - آشکار - متن رمز ج) انتشار - آشکار - متن رمز

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

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

3 (ه 5 (ب 4 الف) 4

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

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

١٩. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى أن عبارت صحيح /غلط را بنويسيد.

- 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.

یاسخ:

- الف این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- ببله 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.
 - ۲۰. اثبات کنید که اگر p=pq باشد، آن گاه (p-1)(q-1) (سوال تشریحی) پاسخ: این مورد در کلاس توضیح داده شد.
 - ۲۱. اعضای مجموعه $^*_{17}$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

پاسخ: اگر $\{r_1,r_2,\ldots,r_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آن گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1,ar_2,\ldots,ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1,ar_2,\ldots,ar_{\phi(n)}\}$ باشد. پس پاسخ اعداد 10 و 7 است.

۲۲. کدام گزینه در مورد مساله غار علی بابا 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.

یاسخ: 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؟

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 – متن آشکار – متن آشکار – متن رمز شده – متن آشکار – متن آ

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)

25 (ع ب) 27 ج) 6 (ج 27 ب) 25 (ع ب) 25 (ع ب)

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

٢٧. كدام قسمت الكوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

P (ه F (ب S الف)

پاسخ: گزینهی "S" صحیح میباشد.

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

الف) هيچكدام 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 (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.

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

Alice جرمانه Bob برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می کند.

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
۵	14.4/.4/11	امنیت سیستمهای کامپیوتری		

ج) ٤

د) P

كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مىشود(به طور دقيق).

F (ب

الف) S

پاسخ: گزینهی "S" صحیح میباشد.

۲. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

2 (s	4 (ج	6 (ب	الف) 8
		رد.	پاسخ: این عدد ریشه اولیه ندا
است.	حی) پاسخ: پاسخ این سوال در اسلایدها		
	و الموال $\phi(r)$? (سوال تشریحی) پاسخ: این مورد د $\phi(r)$		
	مکن است چند گزینه صحیح باشد)		
27 (د	25 (_ج	و) 6	الف) 2
گزینههای فوق ریشه اولیه دارند.	آرند. $\{1,2,4,p^k,2 imes p^k\}$. بنابراین همه	اعداد این مجموعه ریشه اولیه د	پاسخ: اثبات میشود که فقط
خر ملاک است، هر کس پاسخ درستی	حی) پاسخ: برابر با ۸ میشود. جواب آ	1 را محاسبه کنید؟ (سوال تشری	 معکوس عدد پنج در مبنای 3
		راه حل نمره ندارد.	نوشته باشد قابل قبول است و
	ا با رمز کند و برای Bob ارسال کند.	ی Bob رمز کند، میبایست آن ر	۷. برای این که Alice پیامی را برا
د) کلید محرمانه Alice	ج) کلید عمومی Alice	ب) کلید عمومی Bob	الف) كليد محرمانه Bob
	ز کرده و برای او ارسال م <i>ی ک</i> ند.	یام m را با کلید عمومی Bob رم	پاسخ: Alice برای رمزکردن، پ
		بح است؟	۸. کدام گزینه در مورد PGP صحب
		زنگاری انجام میشود بعد فشرده	
		ـردهسازی انجام میشود بعد رمز 	
		ضا انجام میشود بعد فشردهساز ضا انجام میشود بعد رمزکردن و	
فشرده سازی و بعد عملیات رمزگذاری.	امضای دیجیتال بر روی پیام میخورد، بعد	نیز مطرح شد، در PGP اول یک	پاسخ: همانطور که در کلاس
وضيح دهيد؟ (سوال تشريحي) پاسخ:	ا روند تولید کلید عمومی و خصوصی را نیز ت	را در RSA توضیح دهید؟ حتم n	nوند امضای یک پیام به مانند n
		ست.	پاسخ این سوال در اسلایدها ا
	$\mod n$ اول باشند، آنگاه خواهیم داشت		
عدد a در مجموعه کاهش یافته ماندهها	شد، آنگاه مجموعه حاصل شده از ضرب د		
	، اولیه است. پس داریم:	ا یک جایگشت کامل از مجموعه	$\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ يعنى
$\prod_{i=1}^{\phi(n)} (ar_i \mod r$	$r_i = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right) \left(\prod_{i=1}^{\phi(n)} r_i\right) = 0$	$\left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1$	\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: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

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

الف) حمله نوع اول ب) حمله نوع دوم ج) هيچ كدام 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 صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچگونه اطلاعاتی در مورد متن اصلی پی ببرد.

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

۱۴. طول واقعی کلید DES برابر است با

الف) ۴۸ (ج) ۶۴ (ب) ۴۸

یاسخ: گزینهی "۵۶" صحیح میباشد.

- ۱۵. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- 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.

ياسخ:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمني دارد.
- ببله 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

- ١٤. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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.

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

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

 3^{90} چند است 3^{90} چند است

پاسخ: 🛍 دقت کنید که در واقع ما به دنبال پاسخ (10 3^{90} هستم. میدانیم که:

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

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

- ۲۰. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.
 - ۲۱. کدام گزینه در مورد مساله غار علی بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

الف) همه گزیندها صحیح است. ب) یک مساله از نوع روشهای غیرتعاملی است. ج) یک مساله از نوع اثبات دانایی صفر است. د) یک مساله از نوع اثبات دانایی صفر است. پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است. Turing توسط چه نوع حملهای صورت پذیرفت؟ درمزشکنی ماشین Enigma توسط په 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 می بایست برابر با طول متن اصلی باشد.
 - ب) کلید باید به صورت کاملا تصادفی تولید شود.
- ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

- ۲۴. كدام گزينه صحيح است؟ (شايد چند گزينه 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 \mathbb{Z}_{17}^* (ممکن است چند گزینه صحیح باشد)

7 (د) 71 (ج) 34 (ب) 10 (الف) 17 (ج) 17 (ب) 10 (ب) 17 (ب) 17 (ب) 17 (ب) 17 (ب) 17 (ب) 17 (ب) 18 (ب) 1

پاسخ: اگر $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1, ar_2, \dots, ar_{\phi(n)}\}$ باشد. پس پاسخ اعداد 10 و 7 است.

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

الف) كليد محرمانه Alice ب) كليد عمومي Bob ج) كليد محرمانه Bob

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

- ۲۷. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)
- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با روزاری ارتباط، برابر با نفر برای برقراری ارتباط، برابر با روزاری ارتباط، برابر با
 - 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 می کنند.
 از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن
 - ۲۸. PGP امنیت را در کدام لایه برای ما به ارمغان می آورد؟
 - الف) لایه کاربرد ب) لایه شبکه ج) لایه انتقال داده

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

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

6 (د) 4 (ج) 5 (ب) 3 الف) 3

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

پارامتر d را به عنوان کلید محرمانه در نظر می گیریم، به گونه ای که:

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

5 پس ابتدا $\phi(n)$ را محاسبه می کنیم که برابر با $\phi(35)=24$ خواهد شد. سپس باید معکوس عدد e=5 در پیمانه $\phi(n)=24$ برابر با 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.
 - ب) گمراه کنندگی متن آشکار متن رمز شده

د) انتشار - متن آشکار - متن رمز شده

الف) انتشار - متن رمز شده - متن آشکار

ج) گمراه کنندگی - متن رمز شده - متن آشکار

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



شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
۶	14.47.411	امنیت سیستمهای کامپیوتری		

- ۱. اثبات کنید که اگر p=pq باشد، آنگاه (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 می شود؟ در تمام مراحل یکپارچگی پیامها حفظ می شود در تمام مراحل پیامها با کلید نامتقارن رمز می شود در مراحل انتهایی، کل پیامهای مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می شود. هیچ کدام

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

٣. رمزشكني ماشين Enigma توسط Turing، توسط چه نوع حملهاي صورت پذيرفت؟

الف) هيچكدام 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. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه اطلاعاتی در مورد متن اصلی یی 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 <u>بهصورت عمدی می</u>خواهیم 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) هيچ كدام

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 GP	صحیح است؟		
الف) در PGP اول عملي	، رمزنگاری انجام میشود بعد فشرده،	ی و بعد امضا	
	، فشرده سازی انجام می شود بعد رمزن		
	، امضا انجام میشود بعد فشردهسازی		
	، امضا انجام میشود بعد رمزکردن و ب		
			خورد، بعد فشردهسازی و بعد عملیات رمزگذاری
۷. کدام گزینه صحیح است	(شاید چند گزینه پاسخ باشد)		
	تقارن نسبت به الگوريتم كليد نامتقار	با طول کلید کمتر امنیت بیشتری	ـتر ي دارند.
	- بتمهای کلید متقارن نسبت به الگوریت		
	گوریتمهای کلید متقارن مبتنی بر نظر		, •
	د نامتقارن در صورت داشتن سازوکار		كانال امن نداريم.
	ت ت بسیاری از الگوریتمهای کلید متقارر		
	غار علیبابا که در کلاس مطرح شد، ه		
الف) یک مساله تسهیم			ع اثبات دانایی صفر است.
ج) يک مساله از نوع ر	شهای غیرتعاملی است.	د) همه گزینهها صحیح	حیح است.
پاسخ: فقط این گزینه ص	عیح است: یک مساله از نوع اثبات دان	ے صفر است.	
			باشد؟ (ممكن است چند گزينه صحيح باشد)
الف) 10	ب) 34	ج) 17	د) 7
$\ldots, r_{\phi(n)}$ پاسخ: اگر	مجموع کاهشیافته ماند $\mathbb{Z}_n^* = \{r_1, r_n\}$	عا باشد، آنگاه مجموعه حاصل ش	ل شده از ضرب عدد a در مجموعه کاهش یافت
			. باشد. پس پاسخ اعداد 10 و 7 است (a ,
	؟ (میتوانید چند گزینه را انتخاب کنی		
			حاسباتی دشمن، نتواند بر اساس متن رمز شد
	نرا که هیچگونه اطلاعاتی از متن اصل _و		
			عملا از نظر محاسباتی پیچیده و طولانی باشد.
	رط امن شناخته شده، سامانه ernam		
			کنیم. حملهگر در صورت مشاهده متن رمز، نبایا
	ی در مورد متن اصلی پی ببرد. پی در مورد متن اصلی پی ببرد.	, <u> </u>	33.5
	ی ر کرر نذاری، ما بهصورت عمدی میخواهیه	ک نوب: به متن اصلی اضافه کنیم.	النيم. مانقي گذينهها صحيح است.
J == JC =	٠٠٠ الري: مع المعامل ا	ے ویر جہ بندی ، حدی ، حد ع	تعييها، معابعي عريداند عد ليا

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

د) لايه كاربرد ج) لايه پيوند داده ب) لايه انتقال الف) لايه شبكه

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

۱۲. كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

e (ب s (ج الف) P

پاسخ: گزینهی "S" صحیح میباشد.

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

د) F

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

5 پس ابتدا $\phi(n)$ را محاسبه می کنیم که برابر با $\phi(35)=\phi(35)=\phi(35)=0$ خواهد شد. سپس باید معکوس عدد e=5 در پیمانه $\phi(n)$ محاسبه کنیم که برابر با خواهد شد.

این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها اگر a یعنی a عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a یعنی a یعنی a یعنی a یعنی a یک جایگشت کامل از مجموعه اولیه است. پس داریم:

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

1۵. كدام گزينه صحيح است؟ (شايد چند مورد صحيح باشد)

- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با الگوریتمهای نامتقارن بین n نفر برای برقراری ارتباط، برابر با (ج
 - د) هیچکدام از گزینهها صحیح نیست

پاسخ: هیچ کدام 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت مے ،کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

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

الف) كليد محرمانه Alice ب) كليد عمومي Bob ج) كليد محرمانه Bob

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

- ۱۷. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) پاسخ: پاسخ این سوال در اسلایدها است.
- ۱۸. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.
 - ۱۹. كدام شرط در مورد RSA الزامي است؟
 - الف) کلید عمومی باید نسبت به n اول باشد. γ اول باشد.
 - ج) کلید عمومی باید نسبت به $\phi(n)$ اول باشد. $\phi(n)$ اول باشد.

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

- ٠٠. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- 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.

یاسخ:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمنى دارد.
- ببله 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 حمله گر 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 راه حل نمره ندارد.
 - ۲۲. برای این که Alice پیامی را برای Bob رمز کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

Bob ج) کلید عمومی Bob باکلید عمومی الف) کلید عمومی Bob برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می کند.

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 ج) انتشار - متن رمز شده - متن آشکار - متن رمز شده متن آشکار - متن رمز شده انتشار - متن آشکار - متن آشکار - متن رمز شده انتشار - متن رمز شده - متن آشکار - متن آشکار - متن رمز شده - متن آشکار - متن آشکا

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 بالف) 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؟

2 (د) 4 (ج) 6 ب) 8 الف)

پاسخ: این عدد ریشه اولیه ندارد.

 3^{90} وقم آخر عدد 3^{90} چند است?

7 (ع ج) 6 (ج ب) 9 الف) 9 (ع الف) 9

پاسخ: 🕰 دقت کنید که در واقع ما به دنبال پاسخ (mod 10) 3^{90} هستم. میدانیم که:

ullet بعنی چهار عدد مثبت وجود دارد که کمتر از 0 است و نسبت به آن اول هست. $\phi(10)=4$

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

🔼 آنگاه براحتی می توانیم 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) ۹۶ ج) ۴۲ ب

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: یاسخ این سوال در اسلایدها است.

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

- الف) طول كليد مي بايست برابر با طول متن اصلى 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان 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)

27 (ء 25 (ج 25) عند 25 (ج 27) عند 25 (ج 27) عند 25 (ج 27) عند 27 (عند 27) عند

 $m{y}$ پاسخ: اثبات می شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1,2,4,p^k,2 imes p^k\}$. بنابراین همه گزینههای فوق ریشه اولیه دارند.

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
٧	14.47.411	امنیت سیستمهای کامپیوتری		

- 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.
 - 7. كدام قسمت الكوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

S (a $E (\tau)$ $P (\tau)$ F (this in F)

پاسخ: گزینهی "S" صحیح میباشد.

- ٣. كدام گزينه صحيح است؟ (شايد چند گزينه 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 این که Alice پیامی را برای Bob رمز کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد محرمانه Alice ب) كليد عمومي Bob ج) كليد محرمانه Bob

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

- ه. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.
 - ۶. ویژگی به این معنا است که هر بین از متن باید به چندین قسمت وابسته باشد.

الف) انتشار - آشکار - متن رمز بالف) انتشار - آشکار - متن رمز جائید بالف) کنندگی - آشکار - متن رمز جائید بالف کنندگی - رمز - کلید بالف کنندگی - رمز - رمز - کلید بالف کنندگی - رمز - رمز - رمز - رمز

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

- ۷. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟
 - الف) طول كليد مي بايست برابر با طول متن اصلى 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

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

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. ٩. تعداد ريشه اوليه عدد 60 كدام گزينه است؟ د) 6 ج) 4 ب) 8 الف) 2 **پاسخ:** این عدد ریشه اولیه ندارد. ١٠. رمزشكني ماشين Enigma توسط Turing، توسط چه نوع حملهاي صورت پذيرفت؟ ج) هیچکدام د) حمله نوع سوم ب) حمله نوع اول الف) 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. ۱۱. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد. ● 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. • الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمني 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد. 3^{90} چند است 3^{90} چند است د) 8 ج) 7 9 (ب الف) 6 پاسخ: 🛍 دقت کنید که در واقع ما به دنبال پاسخ (10 3^{90} هستم. میدانیم که: • $\phi(10)=4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست. (3,10) = 1 عدد سه و ده نسبت به هم اول هستند، یعنی • $3^4=1\pmod{10}$ برطبق قضیه اویلر-فرما داریم: • 🛍 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؟ (می توانید چند گزینه را انتخاب کنید).

ب) همه گزینهها صحیح است.

الف) یک مساله تسهیم راز است.

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.

- 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. حمله گر 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 a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها اگر a عدد a در مجموعه کاهش یافته مانده ها اگر a یعنی a عدد a در مجموعه کامل از مجموعه اولیه است. پس داریم:

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

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

الف) لايه انتقال ب) لايه كاربرد ج) لايه پيوند داده د) لايه شبكه

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

۱۶. كدام گزينه صحيح است؟ (شايد چند مورد صحيح باشد)

- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با روتباط، برابر با نفر برای برقراری ارتباط، برابر با روتباط، برابر با روتباط، برابر با
 - 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

۱۷. کدام گزینه در مورد PGP صحیح است؟

- الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی 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) هيچ کدام 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 راه حل نمره ندارد.

۲۰. طول واقعی کلید DES برابر است با

الف) ۵۶ ج) ۳۲ ح. ۵۶

پاسخ: گزینهی "۵۶" صحیح میباشد.

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

6 (د) 2 ج25 الف) 25

پاسخ: اثبات می شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1,2,4,p^k,2 imes p^k\}$. 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 با انتشار - متن رمز شده - متن آشکار

د) گمراه کنندگی - متن رمز شده - متن آشکار

ج) انتشار - متن آشکار - متن رمز شده

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

۴۵. اگر در الگوریتم RSA مقدار n=35 و مقدار e=5 باشد، آن گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد

4 (ه 5 (الف) 5

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

5 پس ابتدا $\phi(n)$ را محاسبه می کنیم که برابر با $\phi(35)=24$ خواهد شد. سپس باید معکوس عدد e=5 در پیمانه $\phi(n)=0$ را محاسبه کنیم که برابر با 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 pq باشد، آنگاه (p-1)(q-1) ((p-1)(q-1) باشد، آنگاه (p-1)(q-1) باشد، آنگاه ((p-1)(q-1) باشد، آنگاه ((p-1)(q-1) باشد، آنگاه ((p-1)(q-1)

۲۶. برای این که Alice پیامی را برای Bob امضا کند، می بایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد محرمانه Bob ب) كليد عمومي Alice ج) كليد محرمانه Bob د) كليد عمومي

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

۲۷. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.

- الف امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.
- در یک سامانه رمزگذاری، ما بهصورت غیرعمد میخواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 <u>بهصورت عمدی می</u>خواهیم 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: خدمت <i>گ</i> زار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:
• 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 ECDHServer Public Key for ECDH

• Shared Session Key

بعد از این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

۲۹. كدام شرط در مورد RSA الزامي است؟

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

یاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای 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 الف) 34 الف) 45 میل الف 34 الف) 45 میل الف 34 میل الف 34

پاسخ: اگر $\{r_1, r_2, \dots, r_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1, ar_2, \dots, ar_{\phi(n)}$ باشد. پس یاسخ اعداد 10 و 7 است.

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
٨	14.4/.4/11	امنیت سیستمهای کامپیوتری		

۱. اثبات کنید که اگر p=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؟

8 (د) 8 (ج) 4 (ج) 6 (الف)

پاسخ: این عدد ریشه اولیه ندارد.

۳. رقم آخر عدد 3^{90} چند است؟

6 (ع ج 7 (ج ع الف) 9

پاسخ: 🛍 دقت کنید که در واقع ما به دنبال پاسخ (10 3^{90} هستم. میدانیم که:

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

🛍 آنگاه براحتی میتوانیم بنویسیم که:

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

- ۴. كدام گزينه صحيح است؟ (شايد چند گزينه 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.

یاسخ: 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) هيچكدام 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. كدام گزينه صحيح است؟ (شايد چند مورد صحيح باشد)
- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با روزاری ارتباط، برابر با نفر برای برقراری ارتباط، برابر با روزاری ارتباط، برابر با
 - 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

ئزينه صحيح باشد)	(ممکن است چند گ	Primitive Ro) دارند؟ ۱	ریشه اولیه (oot	یک از اعداد زیر	۷. کدام
------------------	-----------------	------------------------	-----------------	-----------------	---------

27 (ء ع الف) 2 ج) 6 (ج

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

۸. كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

P (ه F (ج E (ب S

پاسخ: گزینهی "S" صحیح میباشد.

- ٩. كدام گزينه صحيح نيست؟ (ميتوانيد چند گزينه را انتخاب كنيد).
- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.

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)

10 (د) 34 (ج) 7 الف) 17

پاسخ: اگر $\{r_1,r_2,\ldots,r_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1,ar_2,\ldots,ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1,ar_2,\ldots,ar_{\phi(n)}\}$ 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان 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. ϕ

ج) متن اصلی باید نسبت به n اول باشد.

ب) 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 می dیریم، به dونهای که

للید محرمانه برابر با کدام گزینه خواهد شد؟	و مقدار $e=5$ باشد، آنگاه d یا همان ک	n=35 مقدار RSA مقدار ۱۴
--	---	-------------------------

5 (د) 3 (ج) 6 (ب) 4

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

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

- ١٥. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچگونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- ب امنیت محاسباتی (Computational Security) یعنی در صورتی که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
 - 🦰 تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- د در یک سامانه رمزگذاری، ما بهصورت غیرعمد می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 اَگاهی 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 گزینه ها صحیح است.
- ۱۶. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.
 - ۱۷. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
 - 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.

یاسخ:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمني دارد.
- ببله 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 حمله گر 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) هيچ كدام 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.

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

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

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

باسخ: a (سوال تشریحی) $a^{\phi(n)} = 1 \mod n$ این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: a عدد a در مجموعه کاهش یافته مانده ها اگر a عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a یعنی a 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 علی بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

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 می شود بعد فشرده سازی و بعد امضا

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

ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن

د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور 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: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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

• Shared Session Key			
با كليد عمومي خودش امضا مي كند.	ن چکیده تولید شد، خدمتگزار آن را	بعد از این که ایر	
سیعی از پراکنده است.	است ساختاری آماری رو حجم و	وی ویژگی را دارد که به این معنا	 طبق گفته شانون یک سامانه ق
رمز شده	ب) انتشار - متن اَشكار - متن	ر شده - متن آشکار	الف) گمراه کنندگی - متن رمز
ار – متن رمز شده	د) گمراه کنند <i>گی</i> - متن آشک	متن آشکار	ج) انتشار - متن رمز شده -
	.د.	أشكار - متن رمز شده" صحيح ميباش	پاسخ: گزینهی "انتشار - متن
وضیح دهید؟ (سوال تشریحی) پاسخ	تولید کلید عمومی و خصوصی را نیز تر		
	-		پاسخ این سوال در اسلایدها اس
عر ملاک است، هر کس پاسخ درستی	پاسخ: برابر با ۸ میشود. جواب آخ		
			نوشته باشد قابل قبول است و
	رمز کند و برای Bob ارسال کند.	ی Bob رمز کند، میبایست آن را با	۲. برای این که Alice پیامی را برای
د) کلید عمومی Alice	ج) کلید عمومی Bob	ب) كليد محرمانه Alice	الف) كليد محرمانه Bob
	ه و برای او ارسال م <i>ی ک</i> ند.	یام m را با کلید عمومی Bob رمز کردد	پاسخ: Alice برای رمزکردن، پ
		با	 طول واقعی کلید DES برابر اس
۵۶ (۵	ج) ۴۸	ب) ۶۴	الف) ۳۲
		ىباشد.	پاسخ: گزینهی "۵۶" صحیح م
		ی ما به ارمغان می آورد؟	 PGP امنیت را در کدام لایه برای
د) لایه شبکه	ج) لايه انتقال	ب) لايه پيوند داده	الف) لايه كاربرد
		د (Application Layer) است.	پاسخ: گزینه صحیح لایه کاربره

• Server Public Key for ECDH

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
٩	14.47.411	امنیت سیستمهای کامپیوتری		

- ۱. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) پاسخ: پاسخ این سوال در اسلایدها است.
- ۲. اثبات کنید که اگر p=pq باشد، آنگاه p=(p-1)(q-1) (سوال تشریحی) پاسخ: این مورد در کلاس توضیح داده شد.
 - ٣. كدام قسمت الكوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

P (د E (ج F (ب S الف)

پاسخ: گزینهی "S" صحیح میباشد.

- ۴. كدام گزينه صحيح است؟ (شايد چند مورد صحيح باشد)
- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با (یا تعداد کلید در الگوریتمهای نامتقارن بین n نفر برای برقراری ارتباط، برابر با
 - د) هیچکدام از گزینهها صحیح نیست

پاسخ: هیچ کدام 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

- ۵. کدام گزینه صحیح نیست؟ (می توانید چند گزینه را انتخاب کنید).
- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم 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 این که Alice پیامی را برای Bob امضا کند، می ایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد عمومي Bob ب) كليد محرمانه Bob ج) كليد عمومي Bob د) كليد محرمانه

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

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

الف) كليد محرمانه Bob ب) كليد عمومي Bob ج) كليد محرمانه Bob د) كليد عمومي

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

- ۸. کدام گزینه در مورد PGP صحیح است؟
- الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمز کردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام میخورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

٩. تعداد ريشه اوليه عدد 60 كدام گزينه است؟

6 (ع ع الف) 4 ج) 8 (ج

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 بالک کاید

ج) گمراه کنندگی - رمز - کلید دان متن رمز علید داندگی - 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) هيچ كدام 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.

١٣. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.

- الف امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 <u>بهصورت عمدی می</u>خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینهها صحیح است.

- ۱۴. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- 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.

ىاسخ:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمنى دارد.
- ببله 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.
 - ۱۵. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حملهای صورت پذیرفت؟

بوده است.	بخشی از متن متن اصلی معلوم	های نسل دو (GSM) است. در هر دو، ب	Enigma و A5/2 در شبکه
		(شاید چند گزینه پاسخ باشد)	۱۶. كدام گزينه صحيح است؟
ِی دارند.	با طول کلید کمتر امنیت بیشتر	تقارن نسبت به الگوريتم كليد نامتقارن	الف) الگوريتمهاي كليد ه
تری احتیاج دارند.	کلید نامتقارن به تعداد کلید کم	بتمهای کلید متقارن نسبت به الگوریتم َ	ب) در یک شبکه، الگور،
		گوریتمهای کلید متقارن مبتنی بر نظریه	
		د نامتقارن در صورت داشتن سازوکاری ب	
		ن بسیاری از الگوریتمهای کلید متقارن ه	
و حجم وسیعی از پراکنده است.	نا است ساختاری اماری رډ	انه قوی ویژگی را دارد که به این مع	۱۷. طبق گفته شانون یک سام
ىتن رمز شده - متن آشكار	ب) گمراه کنندگی - م	- متن رمز شده	الف) انتشار - متن آشكار
ىتن آشكار - متن رمز شده	د) گمراه کنندگی - م	ده - متن آشکار	ج) انتشار - متن رمز شد
	اشد.	متن آشکار - متن رمز شده" صحیح میب	پاسخ: گزینهی "انتشار - ،
است، هر کس پاسخ درستی نوشته باشد قابل	۳۲ میشود. جواب آخر ملاک	نید؟ (سوال تشریحی) پاسخ: برابر با ′	مقدار $\phi(80)$ را محاسبه ک $\phi(80)$
		دارد.	قبول است و راه حل نمره ن
جلوگیری میشود؟ در تمام مراحل یکپارچگی	های رمزنگاری مورد پشتیبانی -	فيير قابليتهاى مشترى نظير الگوريتم	۱۹. در SSH چگونه از حمله ت
امهای مبادله شده به صورت امضا شده از سرور	یشود در مراحل انتهایی، کل پیا	ام مراحل پیامها با کلید نامتقارن رمز می	پیامها حفظ میشود در تم
			خدمتگزار برای مشتری ارد
		ن تابع استفاده می کند، و با استفاده از و	پاسخ: خدمتگزار از همار
• Client Identification Id: SSH-2.0-li	bssh_0.9.3		
• Server Identification Id: SSH-2.0-C	OpenSSH_8.2p1 Ubuntu-4u	buntu0.5	
 Client Key Exchange Init 			
 Server Key Exchange Init 			
• Server Public Key for signature (H	lost Key)		
• Client Public Key for ECDH			
• Server Public Key for ECDH			
• Shared Session Key			
زار آن را با کلید عمومی خودش امضا می کند.	این چکیده تولید شد، خدمتگز	بعد از این که ا	
		ه برای ما به ارمغان میآورد؟	۲۰. PGP امنیت را در کدام لاید
د) لايه كاربرد	ج) لايه انتقال	ب) لايه پيوند داده	الف) لايه شبكه
		کاربرد (Application Layer) است.	ىاسخ: گزىنە صحىح لايە ك
دام گزینه خواهد شد؟	یا همان کلید محرمانه برابر با ک	d او مقدار $e=5$ باشد، آنگاه $n=35$	
3 (ა	4 (ج	ب) 6	الف) 5
نظر می گیریم، به گونهای که	نر e را به عنوان کلید عمومی در	پنج است. همانطور که میدانید، پارامت	پاسخ: گزینه صحیح عدد
		//))	
	$1 < e < \phi(n), (e, \epsilon)$	$\phi(n) = 1.$	

۵١

الف) حمله نوع سوم ب) حمله نوع اول ج) حمله نوع دوم د) هيچ كدام

پاسخ: دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین

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

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

پس ابتدا $\phi(n)$ را محاسبه می کنیم که برابر با $\phi(35)=24$ خواهد شد. سپس باید معکوس عدد e=5 در پیمانه $\phi(n)=24$ را محاسبه کنیم که برابر با $\phi(n)=0$ 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 راه حل نمره ندارد.
- رسوال تشریحی) پاسخ: a این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آن گاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها باشد، آن گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها باشد، آن گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a یعنی a بایگشت کامل از مجموعه اولیه است. پس داریم:

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

3^{90} چند است? رقم آخر عدد 3^{90}

8 (د) 9 (ج) 9 (الف) 7

پاسخ: 🕰 دقت کنید که در واقع ما به دنبال پاسخ (10 mod 10) هستم. میدانیم که:

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

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

۲۵. كدام شرط در مورد RSA الزامي است؟

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

ج) کلید عمومی باید نسبت به n اول باشد. α

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می dیریم، به dونهای که

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

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

الف) یک مساله از نوع روشهای غیرت	است.	یک مساله از نوع اثبات دانایی ·	صفر است.
ج) یک مساله تسهیم راز است.		همه گزینهها صحیح است.	
پاسخ: فقط این گزینه صحیح است: ب	ساله از نوع اثبات دانایی صفر		
کدام یک از اعداد زیر ریشه اولیه (oot	Primit) دارند؟ (ممكن است	ئزينه صحيح باشد)	
الف) 2	(25	27 (ა
الف) 2		25	

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

۲۸. طول واقعی کلید DES برابر است با

.۲۷

الف) ۴۸ (ج) ۳۲ (ج) ۵۶ (د)

پاسخ: گزینهی "۵۶" صحیح میباشد.

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

- الف) طول کلید می بایست برابر با طول متن اصلی باشد.
 - ب) کلید باید به صورت کاملا تصادفی تولید شود.
- ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان 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)

10 (د) 34 (ج ج) 7 (ب الف)

پاسخ: اگر $\{r_1, r_2, \dots, r_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1, ar_2, \dots, ar_{\phi(n)}\}$ باشد. پس پاسخ اعداد 10 و 7 است.

ماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
١٠	14.4/.4/11	امنیت سیستمهای کامپیوتری		

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

ب) یک مساله از نوع روشهای غیرتعاملی است.

الف) یک مساله از نوع اثبات دانایی صفر است.

د) همه گزینهها صحیح است.

ج) یک مساله تسهیم راز 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 می آورد؟

ج) لايه شبكه د) لايه كاربرد

الف) لايه انتقال ب) لايه پيوند داده

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

۳. طول واقعی کلید DES برابر است با

الف) ۵۶ ج) ۳۲ ج

پاسخ: گزینهی "۵۶" صحیح میباشد.

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

الف) كليد محرمانه Bob ب) كليد عمومي Alice ج) كليد عمومي Bob عند عمومي الف

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

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

ب) گمراه کنندگی - متن آشکار - متن رمز شده

الف) گمراه کنندگی - متن رمز شده - متن آشکار

د) انتشار - متن رمز شده - متن آشکار

ج) انتشار - متن آشکار - متن رمز شده

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

- ۶. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 گزینه ها صحیح است.

٧. كدام گزينه صحيح است؟ (شايد چند گزينه 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 می شود (به طور دقیق).
 - F (ع S (ج P (ب E (لف)

پاسخ: گزینهی "S" صحیح میباشد.

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

الف) طول کلید می بایست 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان 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 بالف) گمراه کنندگی - 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)

17 (د) 34 (ج) 7 (ب) 10 الف)

پاسخ: اگر $\{r_1,r_2,\dots,r_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1,ar_2,\dots,ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1,ar_2,\dots,ar_{\phi(n)}$ باشد. پس پاسخ اعداد 10 و 7 است.

- ۱۲. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- 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.

پاسح:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمنى دارد.
- ببله 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 حمله گر 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 راه حل نمره ندارد.
 - ۱۴. کدام گزینه صحیح نیست؟ (می توانید چند گزینه را انتخاب کنید).

- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.
- وند 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: m یاسخ این سوال در اسلایدها است.
- ۱۷. این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آن گاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها باشد، آن گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a یعنی a علی 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. كدام شرط در مورد RSA الزامي است؟

ب) کلید عمومی باید نسبت به n اول باشد.

الف) متن اصلی باید نسبت به n اول باشد.

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

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

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای 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)

$$25$$
 (د) 6 (ج) 27 ب) 27

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

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

 \mathbf{y} سخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

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

- ۲۲. كدام گزينه صحيح است؟ (شايد چند مورد صحيح باشد)
- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با (رتباط، برابر با نفر برای برقراری ارتباط، برابر با با تعداد کلید در الگوریتمهای نامتقارن بین n
 - د) هیچکدام از گزینهها صحیح نیست

پاسخ: هیچ کدام 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

- ۲۳. کدام گزینه در مورد PGP صحیح است؟
- الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور 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 p=pq باشد، آن گاه (p-1)(q-1) ((p-1)(q-1) وسوال تشریحی) پاسخ: این مورد در کلاس توضیح داده شد.

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

الف) هيچكدام ب) حمله نوع سوم ج) حمله نوع اول 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 مشتری نظیر الگوریتمهای رمزنگاری مورد پشتیبانی جلوگیری می شود؟ در تمام مراحل یکپارچگی پیامها حفظ می شود در تمام مراحل پیامها با کلید نامتقارن رمز می شود در مراحل انتهایی، کل پیامهای مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می شود. هیچ کدام

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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

			• Shared Session Key
رقم آخر عدد 3^{90} چند است؟	بعد از این ده این چ	ئیده تولید شد، خدمتگزار آن را با کلی	بد عمومی حودش امصا می دند
الف) 8	ب) 9	6 (₇	7 (১
پاسخ: ﷺ دقت کنید که در واقع ا • 4 = (10)م. یعنی چهار عدد ه • عدد سه و ده نسبت به هم اول • برطبق قضیه اویلر-فرما داریم: ☐ آنگاه براحتی میتوانیم بنویس	ثبت وجود دارد که کمتر از 10 است هستند، یعنی $1=(3,10)$ $3^4=1\pmod{10}$	و نسبت به آن اول هست.	
تعداد ریشه اولیه عدد 60 کدام گزینه	است؟		
الف) 4	2 (ب	6 (₇	8 (১
پاسخ: این عدد ریشه اولیه ندارد. برای این <i>ک</i> ه Alice پیامی را برای 30b	I امضا کند، میبایست آن را با	. رمز کند و برای Bob ارسال کند.	
الف) كليد عمومي Alice	ب) کلید عمومی Bob	ج) کلید محرمانه Bob	د) کلید محرمانه Alice

.۲۷

۸۲.

.۲۹

الف) حمله نوع اول

• Server Public Key for ECDH

د) حمله نوع دوم

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

یاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می کند.

ب) 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.

ج) حمله نوع سوم



شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
11	14.4/.4/11	امنیت سیستمهای کامپیوتری		

- 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؟

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

الف) متن اصلی باید نسبت به n اول باشد.

د) کلید عمومی باید نسبت به n اول باشد.

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

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

- ٣. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- 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.

ياسخ:

- الف این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- ببله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری بر مخفی ماندن کلید باشد، حتی اگر حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.
 - ۴. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.
- دوریک سامانه رمزگذاری، ما بهصورت غیرعمد می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 <u>بهصورت عمدی می</u>خواهیم 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

د) انتشار - رمز - کلید

ج) گمراه کنندگی - آشکار - متن رمز

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

9. 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 راه حل نمره ندارد.

.۷ این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) پاسخ: اگر $a^{\phi(n)} = 1 \mod n$ اگر $a^{\phi(n)} = 1 \mod n$ در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $a^{\phi(n)} = 1 \mod n$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

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

٨. كدام گزينه صحيح است؟ (شايد چند مورد صحيح باشد)

- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با روتباط، برابر با نفر برای برقراری ارتباط، برابر با ج
 - 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

۹. برای این که Alice پیامی را برای Bob امضا کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد عمومي Bob ب) كليد محرمانه Bob ج) كليد عمومي Bob د) كليد محرمانه

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

- ۱۰. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟
 - الف) طول کلید می بایست برابر با طول متن اصلی باشد.
 - ب) کلید باید به صورت کاملا تصادفی تولید شود.
 - ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۱. طول واقعی کلید DES برابر است با

الف) ۴۸ (ج) ۵۶ (ج) ۴۸ (الف)

پاسخ: گزینهی "۵۶" صحیح میباشد.

- ۱۲. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل 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.
 - ۹۲. اگر در الگوریتم RSA مقدار n=35 مقدار و مقدار و باشد، آن گاه d باشد، آن گاه d باشد، آن گاه و مقدار کارند خواهد شد؛

6 (ء ع الف) 5 ج) الف) 5 الف

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

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

۱۵. اثبات کنید که اگر p = pq باشد، آنگاه (p-1)(q-1) (سوال تشریحی) پاسخ: این مورد در کلاس توضیح داده شد.

 3^{90} رقم آخر عدد 3^{90} چند است 3^{90}

7 (ع ج) 8 (ج ب 9 (طف) 7 (ع الف) 6 (طف)

یاسخ: که در واقع ما به دنبال یاسخ (10 mod علی میدانیم که: علی میدانیم که: اسخ: است. میدانیم که: است. میدانیم که:

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

🗀 آنگاه براحتی می توانیم 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)

یاسخ: اثبات می شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1,2,4,p^k,2 imes p^k\}$. 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 باکش شده کنندگی - متن آشکار - متن رمز شده

ج) انتشار - متن آشکار - متن رمز شده - متن آشکار

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

۱۹. برای این که Alice پیامی را برای Bob رمز کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد عمومي Alice ب) كليد محرمانه Bob ج) كليد محرمانه عمومي

یاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می کند.

درست مے کند:	ورودیهای زیر مقدار چکیده پیام را	سال میشود. هیچکدام ن تابع استفاده میکند، و با استفاده از	خدمتگزار برای مشتری ار یاسخ: خدم <i>تگ</i> زار از هما
• Client Identification Id: SSH-2.		, ., ., .,	, yyy
• Server Identification Id: SSH-2.	_	untu0.5	
Client Key Exchange Init	o openeori_on_probania rab		
Server Key Exchange Init			
Server Public Key for signature	(Host Key)		
 Client Public Key for ECDH 	, (1100t 1cy)		
• Server Public Key for ECDH			
• Shared Session Key			
ن را با کلید عمومی خودش امضا می کند.	Ĭ 1:5	S. 1.1 v.	
ن را با کلید عمومی حودس امضا می کند.		بعد آر آین د توسط Turing، توسط چه نوع حمله E	nioma سائد عاشد ۲۱
	ای صورت پدیرفت:	ع وسط په نوع حمد د	۱۱۰ رمرسکنی مسین ۱۱۱۹۱۱۱
د) حمله نوع اول	ج) حمله نوع سوم	ب) هیچکدام	الف) حمله نوع دوم
Known Plaintext A)، رمزشکنی ماشین) یک یا چند متن اصلی معلوم (ttack	ر زمینه حمله نوع دوم یا حمله بر اساس	پاسخ: دو مثال مشهور، د
		های نسل دو (GSM) است. در هر دو	
		ه برای ما به ارمغان میآورد؟	PGP .۲۲ امنیت را در کدام لای
د) لايه پيوند داده	ج) لايه كاربرد	ب) لايه انتقال	الف) لايه شبكه
	ج) کیک کربری		
		کاربرد (Application Layer) است.	- ,
اده شد)	سحیح است؟ (این مورد امروز درس د	، غار علیبابا که در کلاس مطرح شد، ه	۲۳ . کدام گزینه در مورد مساله
ت دانایی صفر است.	ب) یک مساله از نوع اثبان	_ع است.	الف) همه گزینهها صحیح
د) یک مساله تسهیم راز است. د)		ج) یک مساله از نوع روشهای غیرتعاملی است.	
	یے صفر است،	حیح است: یک مساله از نوع اثبات دانا	ىاسخ: فقط ادن گزىنه ص
	<i>y</i>		پ ع ۲۴. کدام گزینه صحیح است؟
دارند.	ن با طول کلید کمتر امنیت بیشتری ه	ت پ رت پ ع . متقارن نسبت به الگوریتم کلید نامتقارر	
		 یتمهای کلید متقارن نسبت به الگوریت	
	یه اعداد است.	گوریتمهای کلید متقارن مبتنی بر نظر	ج) امنیت بسیاری از الاً
امن نداريم.	ی به مانند گواهینامه، نیازی به کانال	بد نامتقارن در صورت داشتن سازوکار _ک	د) در الگوریتمهای کلی
، گزینهها درست است.) مبتنی بر نظریه اعداد است.)، همه	ت بسیاری از الگوریتمهای کلید متقارر [.]	پاسخ: به جز گزینه (امنید
		کدام گزینه است؟	۲۵. تعداد ریشه اولیه عدد 60
4 (د	ج) 6	ب) 8	الف) 2
	•		11.6 1.
			پاسخ: این عدد ریشه اولی
	۶۴	صحیح است ۱	۲۶. کدام گزینه در مورد PGP

۰۲. در SSH چگونه از حمله تغییر قابلیتهای مشتری نظیر الگوریتمهای رمزنگاری مورد پشتیبانی جلوگیری می شود؟ در تمام مراحل یکپارچگی

پیامها حفظ می شود در تمام مراحل پیامها با کلید نامتقارن رمز می شود در مراحل انتهایی، کل پیامهای مبادله شده به صورت امضا شده از سرور

- الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمزکردن د) در PGP اول عملیات امضا انجام می شود بعد رمز کردن و بعد فشرده سازی **پاسخ:** همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی و بعد عملیات رمزگذاری. الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده
 - ۲۷. كدام گزينه صحيح نيست؟ (مي توانيد چند گزينه را انتخاب كنيد).
- سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر 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. كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مىشود(به طور دقيق).

S (ب د) E P (ج الف) F

ياسخ: گزينهي "S" صحيح ميباشد.

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)

ب) 17 د) 10 ج) 7 الف) 34

پاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \dots, r_{\phi(n)}\}$ مجموع کاهشیافته ماندهها باشد، آن گاه مجموعه حاصل شده از ضرب عدد $\mathbb{Z}_n^* = \{r_1, r_2, \dots, r_{\phi(n)}\}$ مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ باشد.

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

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

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
17	14.4/.4/11	امنیت سیستمهای کامپیوتری		

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

4 (د) 3 (ج) 5 (ب) 6

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

پس ابتدا $\phi(n)$ را محاسبه می کنیم که برابر با $\phi(35)=24$ خواهد شد. سپس باید معکوس عدد e=5 در پیمانه $\phi(n)=24$ را محاسبه کنیم که برابر با $\phi(n)=0$ خواهد شد.

- ٢. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 می آورد؟

الف) لايه ييوند داده ب) لايه شبكه ج) لايه كاربرد د) لايه انتقال

ياسخ: گزينه صحيح لايه كاربرد (Application Layer) است.

۴. کدام گزینه در مورد مساله غار علی بابا 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 د) حمله نوع اول ج) هيچكدام ب) 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 در مورد PGP صحیح است؟ الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا

ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن

د) در PGP اول عملیات امضا انجام می شود بعد رمز کردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام میخورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

۷. کدام شرط در مورد RSA الزامی است؟

ب) کلید عمومی باید نسبت به n اول باشد. الف) 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 می گیریم، به گونهای که

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

۸. برای این که Alice پیامی را برای Bob رمز کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

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

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

٩. كدام گزينه صحيح است؟ (شايد چند مورد صحيح باشد)

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

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

 $\binom{n}{2}$ برابر با روتباط، برابر با نفر برای برقراری ارتباط، برابر با ج

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 می دهد.

• توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

۱۰. اثبات کنید که اگر p=pq باشد، آن گاه (p-1)(q-1) ((p-1)(q-1) هد. اثبات کنید که اگر (p-1)(q-1) باشد، آن گاه را باشد داده شد.

١١. كدام قسمت الكوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

P (ج S (۵ E (ب الف) F

پاسخ: گزینهی "S" صحیح میباشد.

۱۲. كدام گزينه صحيح است؟ (شايد چند گزينه پاسخ باشد)

- الف) الگوریتمهای کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.
- ب) دریک 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. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- 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.

یاسخ:

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

۱۴. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

2 (ء (ج 8 (ب 4 الف) 4

پاسخ: این عدد ریشه اولیه ندارد.

- ۱۵. کدام گزینه صحیح نیست؟ (میتوانید چند گزینه را انتخاب کنید).
- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 بانتشار - متن رمز شده - متن آشکار بانتشار - 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 كليد مي بايست برابر با طول متن اصلى 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

ُخر ملاک است، هر کس پاسخ درستی	پاسخ: برابر با ۸ میشود. جواب ا	را محاسبه کنید؟ (سوال تشریحی)	۱۸. معکوس عدد پنج در مبنای 13	
		اه حل نمره ندارد.	نوشته باشد قابل قبول است و ر	
	سمت وابسته باشد.	ه هر بین از متن باید به چندین ق	۱۹. ویژگی به این معنا است کا	
متن رمز	ب) گمراه کنندگی - آشکار -	ید	الف) گمراه کنندگی - رمز - کا	
	د) انتشار - رمز - کلید		ج) انتشار - آشکار - متن رمز	
		ل - رمز - کلید" صحیح میباشد.	پاسخ: گزینهی "گمراه کنندگ _ی	
۲۰. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) پاسخ: پاسخ این سوال در اسلایدها است.				
) Bob امضا کند، میبایست آن را با		
د) کلید عمومی Bob	ج) كليد محرمانه Bob	ب) كليد محرمانه Alice	الف) كليد عمومي Alice	
	ه و برای Bob ارسال می کند.	را با کلید خصوصی خودش رمز کرد m	a پاسخ: Alice برای امضا، پیام	
ممكن است چند گزينه صحيح باشد)		عدد ضرب کنیم تا مجموعه جدید یک		

پاسخ: اگر a عدد a در مجموع کاهش یافته مانده ها باشد، آن گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a عدد a در مجموعه کاهش یافته مانده ها یعنی a 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)

25 (ع ج 27 ج) 25 الف) 2

یاسخ: اثبات می شود 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 می شود؟ در تمام مراحل یکپارچگی پیامها حفظ می شود در تمام مراحل پیامها با کلید نامتقارن رمز می شود در مراحل انتهایی، کل پیامهای مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می شود. هیچکدام

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

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

الف) حمله نوع دوم ب) حمله نوع سوم ج) هيچكدام 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 3⁹⁰ چند است؟

7 (ء 9 (ج 8 (ب 6 الف)

پاسخ: 🕰 دقت کنید که در واقع ما به دنبال پاسخ (10 mod 10) هستم. می دانیم که:

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

🛍 آنگاه براحتی میتوانیم بنویسیم که:

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

۲۷. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.

۲۸. طول واقعی کلید DES برابر است با

الف) ۴۸ (ج که ۲۳ د) ۳۲ د) ۳۲ الف

پاسخ: گزینهی "۵۶" صحیح میباشد.

- البخ این سوال در اسلایدها است. m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصوصی را نیز توضیح دهید؟ (سوال تشریحی) پاسخ: یاسخ این سوال در اسلایدها است.
- ورسوال تشریحی) پاسخ: $a^{\phi(n)} = 1 \mod n \mod n$ این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ در مجموعه کاهش یافته مانده ها اگر $a^{\phi(n)} = 1 \mod n$ در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $a^{\phi(n)} = 1 \mod n$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

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

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
١٣	14.47.411	امنیت سیستمهای کامپیوتری		

برای این که Alice پیامی را برای Bob امضا کند، می بایست آن را با رمز کند و برای Bob ارسال کند.

د) کلید محرمانه Alice

ج) کلید عمومی Alice

ب) کلید عمومی Bob

الف) كليد محرمانه Bob

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

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

ب) یک مساله تسهیم راز است.

الف) همه گزینهها صحیح است.

د) یک مساله از نوع اثبات دانایی صفر است.

ج) یک مساله از نوع روشهای غیرتعاملی 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.

ب) انتشار - متن آشکار - متن رمز شده

الف) گمراه کنندگی - متن رمز شده - متن آشکار

د) گمراه کنندگی - متن آشکار - متن رمز شده

ج) انتشار - متن رمز شده - متن آشکار

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

۴. کدام گزینه صحیح نیست؟ (می توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.

- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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) هيچ كدام

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.

9. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.

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

الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.

- ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با روتباط، برابر با تعداد کلید در الگوریتمهای نامتقارن بین n نفر برای برقراری ارتباط، برابر با
 - 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 می دهد.

• توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، 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) هيچ كدام 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.

- ٩. كدام گزينه صحيح است؟ (شايد چند گزينه 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 الگوریتههای کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینهها درست است.

- ١٠. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- 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.

یاسخ:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمنى دارد.
- ب بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری بر مخفی ماندن کلید باشد، حتی اگر حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.
- این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها اگر a عدد a در مجموعه کاهش یافته مانده ها اگر a عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a یعنی a عدد a در مجموعه کاهل از مجموعه اولیه است. پس داریم:

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

١٢. كدام قسمت الكوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

S (د P (ج F (ب E (الف)

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 این که Alice پیامی را برای Bob رمز کند، میبایست آن را با رمز کند و برای Bob ارسال کند.
- الف) كليد عمومي Alice ب) كليد محرمانه Alice ج) كليد عمومي Bob د) كليد محرمانه ط

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

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 p=pq باشد، آن گاه (p-1)(q-1) ((p-1)(q-1) ۱۶) (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 می شود؟ در تمام مراحل یکپارچگی پیامها حفظ می شود در تمام مراحل پیامها با کلید نامتقارن رمز می شود در مراحل انتهایی، کل پیامهای مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می شود. هیچکدام

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

۱۸. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

8 (ه ع الف) 4 (الف) 4 (ع الف) 4 (ع ا

پاسخ: این عدد ریشه اولیه ندارد.

PGP .۱۹ امنیت را در کدام لایه برای ما به ارمغان می آورد؟

الف) لايه شبكه ب) لايه كاربرد ج) لايه انتقال داده

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

- ۲۰. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى أن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 <u>بهصورت عمدی می</u>خواهیم 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 كليد مي بايست برابر با طول متن اصلى باشد.
 - ب) کلید باید به صورت کاملا تصادفی تولید شود.
 - ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان 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 راه حل نمره ندارد.

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

7 (د) 7 (ح) 10 (ب) 34 (لف)

پاسخ: اگر $\{r_1, r_2, \dots, r_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1, ar_2, \dots, ar_{\phi(n)}\}$ باشد. پس پاسخ اعداد 10 و 7 است.

۲۴. کدام گزینه در مورد PGP صحیح است؟

- الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور 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؟

9 (ه و الف) 6 ج 8 (ج و الف) 6

یاسخ: 🖾 دقت کنید که در واقع ما به دنبال پاسخ (10 mod 10) هستم. می دانیم که:

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

🗀 آنگاه براحتی میتوانیم بنویسیم که:

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

۴۶. اگر در الگوریتم RSA مقدار n=35 و مقدار e=5 باشد، آن گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد

6 (د) 5 ج) 4 (ج) 5 الف)

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

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

۲۷. كدام شرط در مورد RSA الزامي است؟

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

د) متن اصلی باید نسبت به n اول باشد.

الف) کلید عمومی باید نسبت به n اول باشد.

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

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

۲۸. طول واقعی کلید DES برابر است با

84 (ع ج) ۳۲ (ج مرب ۴۸ (لف)

ياسخ: گزينهي "۵۶" صحيح ميباشد.

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

6 (د 27 ج 27 ع الف) 25 الف

پاسخ: اثبات می شود 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.

ب) انتشار - آشکار - متن رمز

د) گمراه کنندگی - رمز - کلید

الف) انتشار - رمز - كليد

ج) گمراه کنندگی - آشکار - متن رمز

ياسخ: گزينهي "گمراه كنندگي - رمز - كليد" صحيح ميباشد.

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
14	14.4/.4/11	امنیت سیستمهای کامپیوتری		

1. كدام شرط در مورد RSA الزامي است؟

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

الف) متن اصلی باید نسبت به n اول باشد.

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

ج) کلید عمومی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می dیریم، به dونهای که

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

طول واقعی کلید DES برابر است با

الف) ۴۸ (ب کا ۲۳ کا ۲۸ کا ۳۲ کا ۲۳ ک

پاسخ: گزینهی "۵۶" صحیح میباشد.

- ۳. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) یاسخ: 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 اصلى با كليد 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان 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 بکلید با کشار - رمز - کلید

ج) انتشار - آشکار - متن رمز درز - کلید

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

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

3 (ه 5 (ج 6 (ب 4 الف)

یاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

5 پس ابتدا $\phi(n)$ را محاسبه می کنیم که برابر با $\phi(35)=\phi(35)=\phi(35)=0$ خواهد شد. سپس باید معکوس عدد e=5 در پیمانه $\phi(n)$ را محاسبه کنیم که برابر با خواهد شد.

- ۷. کدام گزینه در مورد PGP صحیح است؟
- الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام میخورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

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

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

٩. تعداد ريشه اوليه عدد 60 كدام گزينه است؟

پاسخ: این عدد ریشه اولیه ندارد.

- ۱۰. کدام گزینه صحیح نیست؟ (میتوانید چند گزینه را انتخاب کنید).
- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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.

این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آن گاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها باشد، آن گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها باشد، آن گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a یعنی a بعنی a بایگشت 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 این که Alice پیامی را برای Bob رمز کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

		د (Application Layer) است.	
	رمز کند و برای Bob ارسال کند.	ی Bob امضا کند، میبایست آن را با	۱۱۴. برای این که Alice پیامی را برا:
د) کلید عمومی Bob	ج) کلید عمومی Alice	ب) كليد محرمانه Alice	الف) كليد محرمانه Bob
	ه و برای Bob ارسال می کند.	را با کلید خصوصی خودش رمز کرد m	پاسخ: Alice برای امضا، پیام
		عث غیر خطی شدن سامانه میشود(به	
E (3	F (ج	P (ب	الف) S
		باشد.	پاسخ: گزینهی "S" صحیح م _ح
سیعی از پراکنده است.	است ساختاری آماری رو حجم وس	۰۰ فوی ویژگی را دارد که به این معنا ا	
ِمز شده	ب) انتشار - متن آشکار - متن ر	ز شده - متن آشکار	الف) گمراه کنندگی - متن رم
ِ - متن رمز شده	د) گمراه کنندگی - متن آشکار	متن آشکار	ج) انتشار - متن رمز شده -
	د.	آشکار - متن رمز شده" صحیح میباش	پاسخ: گزینهی "انتشار - متن
			۱۷. كدام گزينه صحيح است؟ (شا
هد.	، و در اختیار طرف مقابل نیز قرار می د	Key A): یک سمت کلید را تولید کرده	
		Key Establ): هر دو سمت، در فرایند	
		مای نامتقارن بین n نفر برای برقراری ار	
			د) هیچکدام از گزینهها صح
:(Key Establishment	ستفاده از سازوکارهای برقراری کلید ([:]	حیح نیست. در اسلایدها داشتیم که ا	پاسخ: هیچکدام از گزینهها ص
		ٔ Key): یک سمت کلید را تولید کرده و	
		Key A): هر دو سمت، در فرایند تولید	
گوریتمهای متقارن است نه نامتقارن	از سوی دیگر، تعداد کلید برای ال		
ر ملاک است، هر کس پاسخ درستی	پاسخ: برابر با ۸ میشود. جواب آخ	1 را محاسبه کنید؟ (سوال تشریحی)	3 معکوس عدد پنج در مبنای 3
		راه حل نمره ندارد.	نوشته باشد قابل قبول است و
			الم آخر عدد 3^{90} چند است? ابت 3^{90}
9 (ა	ج) 7	6 (ب	الف) 8
	: هستم. مىدانيم كه:	$3^{90} \pmod{10}$ واقع ما به دنبال پاسخ $3^{90} \pmod{10}$	پاسخ: 🕮 دقت کنید که در
	ست و نسبت به آن اول هست.	عدد مثبت وجود دارد که کمتر از 10 اس	یعنی چهار. $\phi(10)=4$
		(3,10)=1 م اول هستند، یعنی	• عدد سه و ده نسبت به ه
		$3^4 = 1 \pmod{10}$ داریم:	• برطبق قضيه اويلر-فرما

الف) کلید محرمانه Alice ب) کلید عمومی Bob

ج) لايه انتقال

پاسخ: Alice برای رمز کردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می کند.

ب) لایه کاربرد

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

الف) لايه شبكه

د) کلید محرمانه Bob

د) لايه پيوند داده

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

- ۲۰. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- ب امنیت محاسباتی (Computational Security) یعنی در صورتی که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
 - 🤧 تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- دوریک سامانه رمزگذاری، ما بهصورت غیرعمد میخواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 گزینه ها صحیح است.

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

الف) حمله نوع دوم ب) هيچ كدام ج) 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 (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.
 - ٢٣. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
 - 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.

یاسخ:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمنى دارد.
- ببله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری بر مخفی ماندن کلید باشد، حتی اگر حمله گر 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) دریک 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؟

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: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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)

د) 17

- Client Public Key for ECDH
- Server Public Key for ECDH
- Shared Session Key

بعد از این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

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

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

ت) 34

ب) یک مساله از نوع اثبات دانایی صفر است.

الف) یک مساله از نوع روشهای غیرتعاملی است.

د) همه گزینهها صحیح است.

ج) یک مساله تسهیم راز است.

الف) 10

. \mathbb{Z}_{27}^* 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)

7 (ج

پاسخ: اگر $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1, ar_2, \dots, ar_{\phi(n)}\}$ باشد. پس پاسخ اعداد 10 و 7 است.

۲۹. اثبات کنید که اگر p=pq باشد، آن گاه (p-1)(q-1) ((p-1)(q-1) ۱۹) باشد، آن گاه (p-1)(q-1) ۱۹ باشد، آن گاه (p-1)(q-1)

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.

شماره برگه		تاريخ	درس	نام	شماره دانشجویی		نام و نام خانوادگی	ذ
۱۵	14.4/.1	پیوتری ۲/۱۱	درس ت سیستمهای کامب	امنب				
. محرمانه Bob		رمانه Alice	رمز کند و برای ج) کلید محر	Bob	ب) کلید عمومی	1	این که Alice پیامی) کلید عمومی Alice	الف)
							خ: Alice برای رمزکره م یک از اعداد زیر ریش	

27 (ع ج) 6 (ج ع ب) 25 الف)

پاسخ: اثبات می شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1,2,4,p^k,2 imes p^k\}$. 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 \mathbb{Z}_{17}^* را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد \mathbb{Z}_{17}^*

17 (د) 7 (ج با 10 (ب عند 10 الف) 34 (الف) 34 (الف) 17 (د) 17 (د) 17 (د) 18 (د) 19 (د)

پاسخ: اگر $\{r_1, r_2, \dots, r_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1, ar_2, \dots, ar_{\phi(n)}$ 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؟

١.

٠٢.

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

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

د) متن اصلی باید نسبت به n اول باشد.

ج) کلید عمومی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

۶. برای این که Alice پیامی را برای Bob امضا کند، می بایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد محرمانه Bob ب) كليد عمومي Alice ب) كليد عمومي Alice الف) كليد محرمانه عمومي

یاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می کند.

- ۷. کدام گزینه در مورد PGP صحیح است؟
- الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشردهسازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

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

الف) انتشار - رمز - کلید با نتشار - آشکار - متن رمز با نتشار - آشکار - متن رمز با گمراه کنندگی - آشکار - متن رمز با گمراه کنندگی - آشکار - متن رمز با گمراه کنندگی - رمز - کلید

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

طول واقعى كليد DES برابر است با

الف) ۵۶ ج) ۳۲ د 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 صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به صورت عمدی می خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه ها صحیح است.

- ۱۱. كدام گزينه صحيح است؟ (شايد چند مورد صحيح باشد)
- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با روز الگوریتمهای نامتقارن بین n نفر برای برقراری ارتباط، برابر با
 - 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

- ۱۲. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.
- دریک سامانه رمزگذاری، ما بهصورت غیرعمد میخواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 راه حل نمره ندارد.
 - ۱۴. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حملهای صورت پذیرفت؟

	د) حمله نوع اول	ج) حمله نوع دوم	ب) هیچکدام	الف) حمله نوع سوم
ماشين	Known Plaintext <i>A</i>)، رمزشکنی	ں یک یا چند متن اصلی معلوم (Attack	ینه حمله نوع دوم یا حمله بر اساس	پاسخ: دو مثال مشهور، در زم
	، است.	ِ، بخشی از متن متن اصلی معلوم بوده	ی نسل دو (GSM) است. در هر دو	Enigma و A5/2 در شبکههای
ارچگی	ٔیری میشود؟ در تمام مراحل یکپ	ههای رمزنگاری مورد پشتیبانی جلوگ	ر قابلیتهای مشتری نظیر الگوریت	۱۵. در SSH چگونه از حمله تغییر
از سرور	ی مبادله شده به صورت امضا شده	میشود در مراحل انتهایی، کل پیامها	مراحل پیامها با کلید نامتقارن رمز ه	پیامها حفظ می شود در تمام
				خدمتگزار برای مشتری ارسال
	درست می کند:	ز ورودیهای زیر مقدار چکیده پیام را ه	بع استفاده می کند، و با استفاده از	یاسخ: خدمتگزار از همان تا

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

۱۶. كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مىشود(به طور دقيق).

F (ه E (ج P الف) P

پاسخ: گزینهی "S" صحیح میباشد.

۱۷. اثبات کنید که اگر p = pq باشد، آن گاه (p-1)(q-1) ((p-1)(q-1) ؛ (سوال تشریحی) پاسخ: این مورد در کلاس توضیح داده شد.

۱۸. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.

PGP . ۱۹ امنیت را در کدام لایه برای ما به ارمغان می آورد؟

الف) لايه شبكه ب) لايه كاربرد ج) لايه پيوند داده د) لايه انتقال

ياسخ: گزينه صحيح لايه كاربرد (Application Layer) است.

- ۲۰. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟
 - الف) طول كليد مى بايست برابر با طول متن اصلى 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۲۱. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.



باید مبتنی بر مخفی ماندن کلید باشد، حتی اگر حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۲۲. رقم آخر عدد 3^{90} چند است؟

6 (د) 9 (ج) 9 (ج) 8 (ب) 7 (لف) 7

پاسخ: 🕰 دقت کنید که در واقع ما به دنبال پاسخ (10 mod 10) هستم. میدانیم که:

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

🗀 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) هيچ كدام ج) حمله نوع سوم دي 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.

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 دارنجی انتشار - متن رمز شده - متن آشکار

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

در الگوریتم RSA مقدار e=5 و مقدار e=5 باشد، آن گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

 $4 \ (چ \ 6 \ (ب \ 5 \)$ الف $5 \ (خ \ 7 \)$ 3 (ع

 \mathbf{y} سخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

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

۲۶. كدام گزينه صحيح است؟ (شايد چند گزينه 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.

یاسخ: 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 علی بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

ب) یک مساله از نوع اثبات دانایی صفر است.

الف) همه گزینهها صحیح است.

د) یک مساله تسهیم راز است.

ج) یک مساله از نوع روشهای غیرتعاملی است.

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

ورسوال تشریحی) پاسخ: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها اگر a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a یعنی a یعنی a 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؟

8 (د) 8 (ج) 4 (ب) 2

پاسخ: این عدد ریشه اولیه ندارد.

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



شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
18	14.47.411	امنیت سیستمهای کامپیوتری		

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

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

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

7 (د) 10 (ج) 34 (ب) 17 الف)

پاسخ: اگر $\{r_1,r_2,\dots,r_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1,ar_2,\dots,ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1,ar_2,\dots,ar_{\phi(n)}$ باشد. پس پاسخ اعداد 10 و 7 است.

- ۳. برای این که 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 الف)

یاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می کند.

- ۴. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.
 - ۵. کدام گزینه صحیح نیست؟ (می توانید چند گزینه را انتخاب کنید).
- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه اطلاعاتی در مورد متن اصلی پی ببرد.

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

- 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.

یاسخ:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمني دارد.
- ببله 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 حمله گر 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 می شود بعد فشرده سازی و بعد امضا
 - ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
 - ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
 - د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام میخورد، بعد فشرده سازی 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.

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

- ١٠. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- ۔ الف امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچگونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 <u>بهصورت عمدی می</u>خواهیم 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، آن گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

$$6$$
 (ه 3 (ج 4 (ب 5 الف)

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

5 برابر با 24 و محاسبه می کنیم که برابر با 24 و $\phi(35) = 24$ سپس باید معکوس عدد e = 5 در پیمانه 24 را محاسبه کنیم که برابر با 5 و محاسبه کنیم که برابر با 5 و محاسبه کنیم که برابر با 5 و معرد شد.

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

الف) طول کلید می بایست 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.

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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۳. اثبات کنید که اگر p=pq باشد، آن گاه (p-1)(q-1) ((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

پاسخ: گزینهی "۵۶" صحیح میباشد.

۱۵. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۸ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.

16. كدام قسمت الكوريتم DES باعث غير خطى شدن سامانه مي شود (به طور دقيق).

S (د P (\rightarrow P) \rightarrow P \rightarrow P

پاسخ: گزینهی "S" صحیح میباشد.

۱۷. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

2 (ع ج الف) 4 (الف) 4 (عالف) 4

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 باک میاه کنندگی - آشکار - متن رمز

ج) انتشار - آشکار - متن رمز دانتشار - رمز - کلید

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

۱۹. کدام گزینه در مورد مساله غار علی بابا 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 می آورد؟

	پاسخ: گزینه صحیح لایه کاربرد (er	Application Laye) است.		
۲۱.	رمزشکنی ماشین Enigma توسط	Turing، توسط چه نوع حملهای صو	رت پذیرفت؟	
	لف) حمله نوع دوم	ب) حمله نوع سوم	ج) حمله نوع اول	د) هیچکدام
			چند متن اصلی معلوم (intext Attack ر از متن متن اصلی معلوم بوده است.	Known Plai)، رمزشکنی ماشین
			بد کلید عمومی و خصوصی را نیز توضیح	ح دهید؟ (سوال تشریحی) پاسخ:
	پاسخ این سوال در اسلایدها است. برای این که Alice پیامی را برای ob	Bo رمز کند، میبایست آن را با	. رمز کند و برای Bob ارسال کند.	
	لف) كليد محرمانه Bob	ب) كليد محرمانه Alice	ج) کلید عمومی Alice	د) کلید عمومی Bob
		را با کلید عمومی Bob رمز کرده و Turing، توسط چه نوع حملهای صو		
	لف) حمله نوع سوم	ب) هیچکدام	ج) حمله نوع دوم	د) حمله نوع اول
			چند متن اصلی معلوم (intext Attack) از متن متن اصلی معلوم بوده است.	Known Plai)، رمزشکنی ماشین
	6 (ك	ب) 8	ج) 9	7 (ა
		3 ⁴ = 1 (mod 10) ; سیم که:	، و نسبت به آن اول هست.	
.۲۶	کدام شرط در مورد RSA الزامی اس		$3^{90} = 3^{4 \times 22 + 2} = (3^4)^{22}$	
	nلف) کلید عمومی باید نسبت به	اول باشد.	$\phi(n)$ متن اصلی باید نسبت به	اول باشد.

ج) لايه شبكه

د) لايه كاربرد

یاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

ج) متن اصلی باید نسبت به n اول باشد.

الف) لايه پيوند داده

ب) لايه انتقال

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

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

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

6 (د) 27 (ج) 25 (الف)

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

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

- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با رابر برای برقراری ارتباط، برابر با تعداد کلید در الگوریتمهای نامتقارن بین n نفر برای برقراری ارتباط، برابر با
 - 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

رسوال تشریحی) پاسخ: اگر دو عدد ه و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: اگر دو عدد a و عدد a نسبت به همدیگر اول باشند، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها اگر a و عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a یعنی a و عدد a در مجموعه 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. كدام گزينه صحيح است؟ (شايد چند گزينه 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.

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

، برگه	شماره	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
١	٧	14.4/.4/11	امنیت سیستمهای کامپیوتری		

۱. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.

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

الف) لايه شبكه ب) لايه پيوند داده ج) لايه انتقال د) لايه كاربرد

ياسخ: گزينه صحيح لايه كاربرد (Application Layer) است.

- ۳. اثبات کنید که اگر p=pq باشد، آنگاه (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؟

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

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

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

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

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

الف) حمله نوع اول ب) حمله نوع سوم ج) هيچكدام 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 كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با (رتباط، برابر با نفر برای برقراری ارتباط، برابر با (رتباط، برابر با ایم تعداد کلید در الگوریتم های نامتقارن بین n
 - 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

هریحی) پاسخ: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها اگر a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a یعنی a یک جایگشت کامل از مجموعه اولیه است. پس داریم:

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

- ٩. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.
 - ۱۰. کدام شرط در مورد RSA الزامی است؟

ب) کلید عمومی باید نسبت به n اول باشد.

الف) متن اصلی باید نسبت به n اول باشد.

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

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

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای 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 صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.

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.

د) انتشار - متن رمز شده - متن آشکار

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

۱۳. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.

- الف امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 <u>بهصورت عمدی می</u>خواهیم 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 علی بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

ب) یک مساله از نوع اثبات دانایی صفر است.

الف) همه گزینهها صحیح است.

د) یک مساله از نوع روشهای غیرتعاملی است.

ج) یک مساله تسهیم راز 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) هيچكدام 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 می شود بعد فشرده سازی و بعد امضا

ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن

د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور 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.

ب) انتشار - آشکار - متن رمز

الف) گمراه کنندگی - آشکار - متن رمز

د) گمراه کنندگی - رمز - کلید

ج) انتشار - رمز - کلید

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

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: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند. ۱۹. برای این که Alice پیامی را برای Bob امضا کند، می بایست آن را با رمز کند و برای Bob ارسال کند. ب) کلید محرمانه Bob د) کلید محرمانه Alice ج) کلید عمومی Alice الف) كليد عمومي Bob یاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می کند. 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) 34 (ج د) 17 ر) 10 الف) 7 یاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \dots, r_{\phi(n)}\}$ مجموع کاهشیافته ماندهها باشد، آن گاه مجموعه حاصل شده از ضرب عدد $\mathbb{Z}_n^* = \{r_1, r_2, \dots, r_{\phi(n)}\}$ مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ 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) **یاسخ:** 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 راه حل نمره ندارد. 3^{90} عدد 3^{90} چند است? ج) 9 د) 7 6 (ت الف) 8 پاسخ: 🛍 دقت کنید که در واقع ما به دنبال پاسخ (10 3^{90} هستم. می دانیم که: • $\phi(10)=4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست. (3,10) = 1 عدد سه و ده نسبت به هم اول هستند، یعنی • $3^4 = 1 \pmod{10}$ برطبق قضیه اویلر-فرما داریم: • 🔼 آن گاه براحتی می توانیم بنویسیم که:

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

۲۴. كدام گزينه صحيح است؟ (شايد چند گزينه 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؟

۲۶.	پاسخ: این عدد ریشه اولیه ندارد. طول واقعی کلید DES برابر است با .			
	الف) ۴۸	ب) ۵۶	ج) ۲۲	۶۴ (۵
۲۷.	پاسخ: گزینهی "۵۶" صحیح میباشد کدام قسمت الگوریتم DES باعث غی		دقیق).	
	الف) S	E (ب	P (E	F (۵
۸۲.	پاسخ: گزینهی "S" صحیح میباشد. برای این که Alice پیامی را برای Bob		ِمز کند و برای Bob ارسال کند.	
	الف) كليد عمومي Alice	ب) كليد محرمانه Alice	ج) کلید عمومی Bob	د) کلید محرمانه Bob
۲۹.	m برای رمزکردن، پیام Alice پاسخ: Alice برای رمزکردن، پیام کدام یک از اعداد زیر ریشه اولیه (\cot			
	6 (الف	ب) 27	2 (_ج	25 (ა
٣.	پاسخ: اثبات می شود که فقط اعداد ا		نابراین همه گزینهه $\{1,2,4,p^k,2\}$	ای فوق ریشه اولیه دارند.

2 (ج

د) 4

.۳۰. کدام گزینه در مورد رمز .

6 (ب

الف) 8

- الف) طول كليد مي بايست برابر با طول متن اصلى باشد.
 - ب) کلید باید به صورت کاملا تصادفی تولید شود.
- ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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 می شود (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. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
١٨	14.47.411	امنیت سیستمهای کامپیوتری		

است؟	I صحیح	د GP	در مور	گزينه	كدام	٠,
------	--------	------	--------	-------	------	----

الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا

- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمزکردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور 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 علی بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

ب) یک مساله از نوع روشهای غیرتعاملی است.

الف) یک مساله از نوع اثبات دانایی صفر است.

د) همه گزینهها صحیح است.

ج) یک مساله تسهیم راز است.

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

- ٣. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- 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) F

- الف این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- ببله 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.
 - ۴. كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

S (ه P (ب P ب

یاسخ: گزینهی "S" صحیح می باشد.

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

5 (ه 3 (ج 6 (ب 4 الف)

 \mathbf{y} ورا به عنوان کلید عمومی در نظر می گیریم، به گونهای که می دانید، پارامتر \mathbf{e} را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

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

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

پس ابتدا $\phi(n)$ را محاسبه می کنیم که برابر با $\phi(35)=24$ خواهد شد. سپس باید معکوس عدد e=5 در پیمانه $\phi(n)=24$ را محاسبه کنیم که برابر با $\phi(n)=0$ خواهد شد.

. کدام شرط در مورد RSA الزامی است؟	. در مورد RSA الزامي اد	شرط	كدام	۶.
------------------------------------	-------------------------	-----	------	----

ب) متن اصلی باید نسبت به n اول باشد.

د) کلید عمومی باید نسبت به n اول باشد.

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

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

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

رمزشكني ماشين Enigma توسط Turing، توسط چه نوع حملهاي صورت پذيرفت؟

الف) حمله نوع سوم ب) حمله نوع دوم ج) هيچ كدام 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 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: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

۱۰. يروتكل توافق كليد ديفي-هلمن را توضيح دهيد؟ (سوال تشريحي) **ياسخ**: ياسخ اين سوال در اسلايدها است.

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

25 (د) 27 ج) 27 عن 27 د) 25 الف)

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

 3^{90} عدد 3^{90} چند است?

8 (اف) 8 ج) 9 ج

پاسخ: 🛍 دقت کنید که در واقع ما به دنبال پاسخ (10 mod 10) هستم. می دانیم که:

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

🛍 آنگاه براحتی میتوانیم بنویسیم که:

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

١٣. كدام گزينه صحيح است؟ (شايد چند گزينه 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 الگوریتههای کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینهها درست است.

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

- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با روتباط، برابر با نفر برای برقراری ارتباط، برابر با ج
 - د) هیچکدام از گزینهها صحیح نیست

پاسخ: هیچ کدام 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

۱۵. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۸ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.

PGP . ۱۶ امنیت را در کدام لایه برای ما به ارمغان می آورد؟

الف) لايه شبكه ب) لايه انتقال ج) لايه كاربرد داده

ياسخ: گزينه صحيح لايه كاربرد (Application Layer) است.

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

الف) حمله نوع اول ب) حمله نوع سوم ج) هيچ كدام 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. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.

- الف امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.

- ب امنیت محاسباتی (Computational Security) یعنی در صورتی که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
 - 🤧 تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- د در یک سامانه رمزگذاری، ما بهصورت غیرعمد می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 <u>بهصورت عمدی می</u>خواهیم 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

۴۸ (۵ ج ۹۶ (ج ۳۲ الف)

پاسخ: گزینهی "۵۶" صحیح میباشد.

.۲۰ این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها اگر $a^{\phi(n)} = 1 \mod n$ عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $a^{\phi(n)} = 1 \mod n$ 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 صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.

پاسخ: در یک سامانه رمزگذاری، ما به صورت عمدی می خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه ها صحیح است.

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

7 (د) 34 (ج) 10 (ب) 17

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

 $^{\circ}$ تعداد ریشه اولیه عدد $^{\circ}$ کدام گزینه است?

6 (ء 4 (ج 8 (ب 2 الف) 2

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.

ب) انتشار - متن رمز شده - متن آشکار
 د) انتشار - متن آشکار - متن رمز شده

الف) گمراه کنندگی - متن رمز شده - متن آشکار ج) گمراه کنندگی - 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 می بایست برابر با طول متن اصلی باشد.
 - ب) کلید باید به صورت کاملا تصادفی تولید شود.
- ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

- 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: یاسخ این سوال در اسلایدها است.
 - ۲۷. اثبات کنید که اگر p=pq باشد، آن گاه (p-1)(q-1) ((p-1)(q-1) وسوال تشریحی) پاسخ: این مورد در کلاس توضیح داده شد.
 - ۲۸. برای این که Alice پیامی را برای Bob رمز کند، می بایست آن را با رمز کند و برای Bob ارسال کند.

Bob ج) کلید عمومی Bob برای (عیر محرمانه Bob ج) کلید عمومی الف) کلید عمومی Bob برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می کند.

۲۹. برای این که Alice پیامی را برای Bob امضا کند، می بایست آن را با رمز کند و برای Bob ارسال کند.

Alice کلید محرمانه Bob ج) کلید محرمانه Bob ج) کلید عمومی (عمومی Bob ج) کلید عمومی الف) کلید محرمانه عمومی فودش مرکزده و برای Bob ارسال می کند. m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می کند.

۳۰. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
۱۹	14.4/.4/11	امنیت سیستمهای کامپیوتری		

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

الف) حمله نوع سوم ب) حمله نوع دوم ج) هيچكدام 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)

17 (د) 34 (ج بر) 7 بي 10 الف)

پاسخ: اگر $\{r_1, r_2, \dots, r_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1, ar_2, \dots, ar_{\phi(n)}$ باشد. پس پاسخ اعداد 10 و 7 است.

۳. این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) **پاسخ:** a اگر افر قضیه را اثبات کنید: اگر دو عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a در a در مجموعه کاهش یافته مانده ها باشد، آنگاه 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. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- 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.
- ببله 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۵. کدام گزینه در مورد مساله غار علی بابا 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.

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

الف) 5 (ب 5 ق) 5 (الف) 5 ((lلb) 5 (الف) 5 (الف) 5 ((llb) 5 ((llb)

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

یارامتر d, ابه عنوان کلید محرمانه در نظر می گیریم، به گونهای که:

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

يس ابتدا $\phi(n)$ را محاسبه مي كنيم كه برابر با $\phi(35)=24$ خواهد شد. سيس بايد معكوس عدد e=5 در پيمانه $\phi(n)=24$ را محاسبه كنيم كه برابر با $\phi(n)=0$ خواهد شد.

٧. تعداد ريشه اوليه عدد 60 كدام گزينه است؟

ج) 6 د) 4 2 (ب الف) 8

یاسخ: این عدد ریشه اولیه ندارد.

- ۸. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) پاسخ: پاسخ این سوال در اسلایدها است.
 - ٩. رمزشكني ماشين Enigma توسط Turing، توسط چه نوع حملهاي صورت يذيرفت؟

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

یاسخ: 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 مشتری نظیر الگوریتمهای رمزنگاری مورد پشتیبانی جلوگیری میشود؟ در تمام مراحل یکپارچگی پیامها حفظ می شود در تمام مراحل پیامها با کلید نامتقارن رمز می شود در مراحل انتهایی، کل پیامهای مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می شود. هیچ کدام

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

۱۱. اثبات کنید که اگر p=pq باشد، آن گاه (p-1)(q-1) ((p-1)(q-1) باشد، آن گاه (p-1)(q-1) باشد، آن گاه روز در کلاس توضیح داده شد.

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

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

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

۱۳. کدام شرط در مورد RSA الزامی است؟

11.

الف) کلید عمومی باید نسبت به n اول باشد. $(a) \qquad \qquad (b) \qquad (a) \qquad \qquad (b) \qquad (a) \qquad \qquad (b) \qquad (a) \qquad \qquad (b) \qquad (b) \qquad (a) \qquad (b) \qquad (b) \qquad (c) \qquad (c) \qquad (c) \qquad (c) \qquad (c) \qquad (d) \qquad (e) \qquad$

۱۴. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.

۱۵. کدام گزینه در مورد PGP صحیح است؟

- الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمز کردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام میخورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

۱۶. طول واقعی کلید DES برابر است با

الف) ۴۸ ج) ۳۲ ج) ۴۸

پاسخ: گزینهی "۵۶" صحیح میباشد.

۱۷. برای این که Alice پیامی را برای Bob امضا کند، می بایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد محرمانه Bob ب) كليد محرمانه Bob ج) كليد عمومي Bob د) كليد عمومي

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

١٨. كدام قسمت الكوريتم DES باعث غير خطى شدن سامانه مىشود(به طور دقيق).

F (ه P (ج E (ب S الف)

پاسخ: گزینهی "S" صحیح میباشد.

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

- الف) طول كليد مي بايست برابر با طول متن اصلى 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۲۰. کدام گزینه صحیح نیست؟ (می توانید چند گزینه را انتخاب کنید).

- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.

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 با کمراه کنندگی - متن رمز شده - متن آشکار

ج) انتشار - متن رمز شده - متن آشکار در شده - متن آشکار - متن رمز شده

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

۲۲. كدام گزينه صحيح است؟ (شايد چند گزينه 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.

 3^{90} جند است? رقم آخر عدد 3^{90} چند است

الف) 6 ج) 8 ج) 8 ط

پاسخ: 🕰 دقت کنید که در واقع ما به دنبال پاسخ (10 mod 10) هستم. می دانیم که:

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

🔼 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 می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.
 - ۲۵. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)
 - الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با روتباط، برابر با نفر برای برقراری ارتباط، برابر با روتباط، برابر با روتباط، برابر با
 - 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 می دهد.

	• توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.	
د کلید برای الگوریتمهای متقارن است نه نامتقارن	از سوی دیگر، تعداد	
وصى را نيز توضيح دهيد؟ (سوال تشريحي) پاسخ:	روند امضای یک پیام به مانند m را در RSA توضیح دهید؟ حتما روند تولید کلید عمومی و خصو	۲.
	پاسخ این سوال در اسلایدها است.	
سيد.	كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح/غلط را بنويد	۲.
اد محاسباتی دشمن، نتواند بر اساس متن رمز شده	۔ <mark>الف</mark> امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیا	
	سیستم را بشکند، چرا که هیچگونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند	
رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.	۔ ب امنیت محاسباتی (Computational Security) یعنی در صورتی که شکستن سیستم	

- **ب** امنیت محاسبانی (Computational Security) یعنی در صورتی که شکستن سیستم رمز عملاً از نظر محاسبانی پیچیده و طولانی باشد. .
 - 🤧 تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- در یک سامانه رمزگذاری، ما بهصورت غیرعمد می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 به صورت عمدی می خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه ها صحیح است.

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

الف) لايه شبکه ب) لايه کاربرد (Application Layer) است.

۲۹. برای این که Alice پیامی را برای Bob رمز کند، می بایست آن را با رمز کند و برای Bob ارسال کند.

Alice جمومی Bob ج) کلید محرمانه Bob ج) کلید محرمانه Bob ج) کلید عمومی Bob جا کلید

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

25 (د 27 (ج ب 6 (ب 25 الف) 27 (ح ب 18 الف) 29 (ح ب الف) 2

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

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
۲٠	14.4/.4/11	امنیت سیستمهای کامپیوتری		

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

ب) گمراه کنندگی - رمز - کلید

الف) انتشار - رمز - كليد

ج) انتشار - آشکار - متن رمز

د) گمراه کنندگی - آشکار - متن رمز

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

۲. برای این که Alice پیامی را برای Bob رمز کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

د) کلید عمومی Alice

ج) کلید محرمانه Alice

ب) کلید محرمانه Bob

الف) كليد عمومي Bob

رمز کردن، پیام m را با کلید عمومی Bob برای رمزکردن، پیام m را با کلید عمومی Alice برای او ارسال می کند.

- ٣. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- 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.

ياسخ:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمني دارد.
- ببله 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 حمله گر 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.

ب) گمراه کنندگی - متن آشکار - متن رمز شده

الف) انتشار - متن آشكار - متن رمز شده

د) گمراه کنندگی - متن رمز شده - متن آشکار

ج) انتشار - متن رمز شده - متن آشکار

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

 3^{90} . رقم آخر عدد 3^{90} چند است

د) 9

ج) 7

ب) 6

لف) 8

پاسخ: 🛍 دقت کنید که در واقع ما به دنبال پاسخ (mod 10) 3^{90} هستم. میدانیم که:

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

🖾 آن گاه 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 راه حل نمره ندارد.

بادله شده به صورت امضا شده از سرور	شود در مراحل انتهایی، کل پیامهای م	راحل پیامها با کلید نامتقارن رمز می	پیامها حفظ میشود در تمام م
		میشود. هیچکدام	خدمتگزار برای مشتری ارسال
ت میکند:	وِدیهای زیر مقدار چکیده پیام را درس	بع استفاده می کند، و با استفاده از ور	پاسخ: خدمتگزار از همان تاب
• Client Identification Id: SSI	H-2.0-libssh_0.9.3		
• Server Identification Id: SSI	H-2.0-OpenSSH_8.2p1 Ubuntu-4	ubuntu0.5	
• Client Key Exchange Init			
• Server Key Exchange Init			
• Server Public Key for signa	ture (Host Key)		
• Client Public Key for ECDF	H		
• Server Public Key for ECDI	Н		
• Shared Session Key			
با كليد عمومي خودش امضا مي كند.	بن چکیده تولید شد، خدمت گزار آن را	بعد از این که ای	
		ً گزینه است؟	۸. تعداد ریشه اولیه عدد 60 کدام
6 (د	ح) 2	4 (ب	الف) 8
		ارد.	یاسخ: این عدد ریشه اولیه ندا
			۹. کدام شرط در مورد RSA الزام.
	ب) کلید عمومی باید نسبت به		الف) کلید عمومی باید نسبت
اول باشد. $\phi(n)$	د) متن اصلی باید نسبت به (اول باشد. n	ج) متن اصلی باید نسبت به
	ی که	ید عمومی در نظر می گیریم، به گونها	پاسخ: پارامتر e را به عنوان کل
	$1 < e < \phi(n), (e,$	$\phi(n)) = 1.$	
شد)	ئیح است؟ (این مورد امروز درس داده ه	علیبابا که در کلاس مطرح شد، صح	۱۰. کدام گزینه در مورد مساله غار
	ب) همه گزینهها صحیح است	ای غیرتعاملی است.	الف) یک مساله از نوع روشه
	د) یک مساله تسهیم راز است	دانایی صفر است.	ج) یک مساله از نوع اثبات د
	صفر است.	است: یک مساله از نوع اثبات دانایی	پاسخ: فقط این گزینه صحیح
.,	رمز کند و برای Bob ارسال کند	ی Bob امضا کند، میبایست آن را با .	۱۱. برای این که Alice پیامی را برا
د) کلید عمومی Bob	ج) کلید عمومی Alice	ب) كليد محرمانه Bob	الف) كليد محرمانه Alice
	رده و برای Bob ارسال م <i>ی</i> کند.	را با کلید خصوصی خودش رمز کر m	پاسخ: Alice برای امضا، پیام
		م ما به ارمغان می آورد؟	PGP .۱۲ امنیت را در کدام لایه یا

۷. در SSH چگونه از حمله تغییر قابلیتهای مشتری نظیر الگوریتمهای رمزنگاری مورد پشتیبانی جلوگیری میشود؟ در تمام مراحل یکپارچگی

الف) لايه انتقال ب) لايه پيوند داده ج) لايه کاربرد د) لايه 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، آن گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

$$5$$
 (د) 3 (ح) 6 الف) 4

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

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

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

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

.۱۶ این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها اگر a عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a یعنی a 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 (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.

۱۸. كدام گزينه صحيح نيست؟ (ميتوانيد چند گزينه را انتخاب كنيد).

- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به صورت عمدی می خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه ها صحیح است.

19. كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

F (ه E (ج P الف) P

پاسخ: گزینهی "S" صحیح میباشد.

- ۲۰. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟
 - الف) طول كليد مي بايست برابر با طول متن اصلى باشد.
 - ب) کلید باید به صورت کاملا تصادفی تولید شود.
 - ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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 متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانهای ویژگی امنیت بدون شرط را دارد. بدین سان می توان 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) هيچ كدام ج) حمله نوع سوم دي 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 p = pq باشد، آن گاه (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. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.
- دوریک سامانه رمزگذاری، ما بهصورت غیرعمد می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 <u>بهصورت عمدی می</u>خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینهها صحیح است.

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

10 (د) 7 (ج 17 (ع) 34

پاسخ: اگر $\{x_1,x_2,\dots,x_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد x_n در مجموعه کاهش یافته مانده ها یعنی $\{ar_1,ar_2,\dots,ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $x_n=1$ باشد. پس پاسخ اعداد 10 و 7 است.

- ۲۶. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)
- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

- 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، 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) هيچ كدام

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) ۵۶ د) ۵۶

پاسخ: گزینهی "۵۶" صحیح میباشد.

- ۳۰. کدام گزینه در مورد PGP صحیح است؟
- الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمزکردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

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

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
71	14.4/.4/11	امنیت سیستمهای کامپیوتری		

۱. کدام شرط در مورد RSA الزامی است؟

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

د) متن اصلی باید نسبت به n اول باشد.

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

ج) کلید عمومی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای 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 می شود بعد فشرده سازی و بعد امضا

- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور 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؟

6 (ه ب) 2 (ب) 8 الف) 8

یاسخ: این عدد ریشه اولیه ندارد.

- ۵. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) پاسخ: پاسخ این سوال در اسلایدها است.
 - ۶. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى أن عبارت صحيح /غلط را بنويسيد.
- 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.

باسخ:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمنى دارد.
- بب 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

 $^{\circ}$ رقم آخر عدد $^{\circ}$ چند است?

الف) 6 ج) 8 ج) 8 د) 9 د)

پاسخ: 🕰 دقت کنید که در واقع ما به دنبال پاسخ (10 mod 10) هستم. می دانیم که:

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

🔼 آن گاه براحتی می توانیم بنویسیم که:

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

- ٨. كدام گزينه صحيح نيست؟ (مي توانيد چند گزينه را انتخاب كنيد).
- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچگونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچگونه اطلاعاتی در مورد متن اصلی یی ببرد.

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

- ٩. كدام گزينه صحيح است؟ (شايد چند مورد صحيح باشد)
- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت مے ،کنند.
 - $\binom{n}{2}$ برابر با (رمی ارتباط، برابر با n نفر برای برقراری ارتباط، برابر با n
 - د) هیچکدام از گزینهها صحیح نیست

پاسخ: هیچ کدام 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت مے ،کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

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

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.



ب) همه گزینهها صحیح است.

ج) 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

د) یک مساله از نوع اثبات دانایی صفر است.

د) حمله نوع اول

الف) یک مساله تسهیم راز است.

الف) حمله نوع سوم

ج) 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؟

ب) هیچکدام

این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آن گاه خواهیم داشت: اگر دو عدد a و a نسبت به همدیگر اول باشند، آن گاه خواهیم داشت: اگر دو عدد اگر دو عدد a نسبت به همدیگر اول باشند، آن گاه خواهیم داشت: اگر دو عدد اگر دو عد اگر دو عدد اگر $\mathbb{Z}_n^* = \{r_1, r_2, \dots, r_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آن گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ 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 این که Alice پیامی را برای Bob امضا کند، می بایست آن را با رمز کند و برای Bob ارسال کند.

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

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

۲۰. اثبات کنید که اگر p=pq باشد، آن گاه (p-1)(q-1) ((p-1)(q-1) هد. اثبات کنید که اگر (p-1)(q-1) باشد، آن گاه ((p-1)(q-1) باشد، آن گاه ((p-1)(q-1)

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

ب) انتشار - متن رمز شده - متن آشکار الف) انتشار - متن آشكار - 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.

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

د) هیچکدام ج) حمله نوع دوم ب) حمله نوع سوم الف) 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. طول واقعی کلید DES برابر است با

ج) ۴۸ د) ۳۲ ب) ۵۶ الف) ۶۴

پاسخ: گزینهی "۵۶" صحیح میباشد.

۲۴. مقدار ($\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.

۲۵. كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

P (ب F (د الف) E ج) S

پاسخ: گزینهی "S" صحیح میباشد.

۲۶. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.

- 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 هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- ب امنیت محاسباتی (Computational Security) یعنی در صورتی که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
 - 🦰 تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- د در یک سامانه رمزگذاری، ما بهصورت غیرعمد می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 گزینه ها صحیح است.

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

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

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

$$27$$
 (ع 25 (ع 25 (ع) 25

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

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

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

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

a	شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
	77	14.4/.4/11	امنیت سیستمهای کامپیوتری		

1. كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

E (د) P (ج F (الف)

پاسخ: گزینهی "S" صحیح میباشد.

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

الف) طول كليد مي بايست برابر با طول متن اصلى باشد.

- ب) کلید باید به صورت کاملا تصادفی تولید شود.
- ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان 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.

ب) انتشار - متن آشکار - متن رمز شده

الف) انتشار - متن رمز شده - متن آشكار

د) گمراه کنندگی - متن آشکار - متن رمز شده

ج) گمراه کنندگی - متن رمز شده - متن آشکار

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

۴. كدام شرط در مورد RSA الزامي است؟

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

الف) کلید عمومی باید نسبت به n اول باشد.

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

ج) متن اصلی باید نسبت به n اول باشد.

یاسخ: یارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

۵. 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: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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)
- Server Public Key for ECDH

• Client Public Key for ECDH

• Shared Session Key

بعد از این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

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

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: یاسخ این سوال در اسلایدها است.

۸. کدام گزینه در مورد مساله غار علی بابا 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 گزینه ها 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 راه حل 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) هيچ كدام 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 p=pq باشد، آن گاه (p-1)(q-1) (سوال تشریحی) پاسخ: این مورد در کلاس توضیح داده شد.

۱۳. كدام گزينه صحيح است؟ (شايد چند گزينه 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 این که 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 کلید محرمانه عمومی

یاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می کند.

10. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

الف	2 (و) 6	ج) 4	8 (د
پاس	مخ: این عدد ریشه اولیه ندارد.			
۱. مقد	دار $\phi(80)$ را محاسبه کنید؟ (سوا	ل تشریحی) پاسخ: برابر با ۳۲ می	شود. جواب آخر ملاک است، هر کس	ی پاسخ درستی نوشته باشد قابل
قبو	ول است و راه حل نمره ندارد.			
ا. اعد	نای مجموعه \mathbb{Z}_{17}^* را در کدام عدد	ضرب کنیم تا مجموعه جدید یک جایا	گشت از مجموعه اصلی باشد؟ (ممکن	است چند گزینه صحیح باشد)
الف	34 (ب) 10	ج) 7	17 (ა
پاس	$\mathbf{z} = \{r_1, r_2, \dots, r_{\phi(n)}\}$ بخ: اگر	مجموع کاهشیافته ماندهها باشد \mathbb{Z}_r^*	،، آنگاه مجموعه حاصل شده از ضرب	عدد a در مجموعه کاهش یافت ،
			لیه است، اگر $(a,n)=1$ باشد. یس یا	

ب) هیچکدام الف) 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.

ج) حمله نوع اول

د) حمله نوع سوم

۱۹. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.

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

- الف امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر 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، ايمني دارد. مابقي گزينهها صحيح است.

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

د) 25 ₂ (ج 6 (ب الف) 27

یاسخ: اثبات می شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1,2,4,p^k,2 imes p^k\}$. بنابراین همه گزینههای فوق ریشه اولیه دارند.

۲۱. طول واقعی کلید DES برابر است با

د) ۵۶ ج) ۶۴ ٤٨ (ت الف) ۳۲

ياسخ: گزينهي "۵۶" صحيح ميباشد.

۲۲. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى أن عبارت صحيح /غلط را بنويسيد.

- 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.

• الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمني دارد.

اصل، امنیت یک الگوریتم رمزگذاری	ز اصل Kerckhoffs است. برطبق این	ست. در واقع این جمله بیان شانون ا	• ب بله این جمله صحیح ا،
و رمزگشایی داشته باشد.	ں کافی راجع به کل فرایند رمزگذاری _۵	ن کلید باشد، حتی اگر حملهگر دانش	باید مبتنی بر مخفی ماند
	رمز کند و برای Bob ارسال کند.	، Bob امضا کند، میبایست آن را با	۲۳. برای این که Alice پیامی را برای
د) کلید محرمانه Alice	ج) کلید عمومی Alice	ب) کلید عمومی Bob	الف) كليد محرمانه Bob
	ده و برای Bob ارسال می کند.	را با کلید خصوصی خودش رمز کرد n	پاسخ: Alice برای امضا، پیام <i>n</i>
		ح است؟	۲۴. کدام گزینه در مورد PGP صحیح
		گاری انجام میشود بعد فشردهسازی	
		دهسازی انجام میشود بعد رمزنگاری 	
		ـا انجام می شود بعد فشرده سازی و بع ـااد ـا	
1		ا انجام میشود بعد رمزکردن و بعد فنا ۱۳۵۸ این میشود بعد رمزکردن و بعد فنا	
قشردهسازی و بعد عملیات رمزنداری.	ی دیجیتال بر روی پیام میخورد، بعد ف	یز مطرح شد، در PGP اول یک امضا:	پاسح: همان طور که در کلاس ن
			۲۵. کدام گزینه صحیح است؟ (شاید
دهد.	ه و در اختیار طرف مقابل نیز قرار می د		
		Key Estal): هر دو سمت، در فرایند	
	$\binom{n}{2}$ رتباط، برابر با	ی نامتقارن بین n نفر برای برقراری ا	
(TT T . 11.1			د) هیچکدام از گزینهها صحب
	استفاده از سازوکارهای برقراری کلید (
ىد.	و در اختیار طرف مقابل نیز قرار میده		
		، Key): هر دو سمت، در فرایند تولید	• نوافق کلید (Agreement
لگوریتمهای متقارن است نه نامتقارن	ار سوی دیگر، تعداد کنید برای ۱۱	ل ما به ارمغان می آورد؟	۲۶. PGP امنیت را در کدام لایه برای
د) لايه شبكه	ج) لايه انتقال	ب) لايه پيوند داده	الف) لايه كاربرد
		l(Application Layer)	یاسخ: گزینه صحیح لایه کاربرد
		(Application Layer)	پسی. درینه صحیح دیه تاربرد ۲۷. رقم آخر عدد 3 ⁹⁰ چند است؟
			١١٠. رقم احر عدد ٥٠ چند است:
د) 8	ج) 7	9 (ب	الف) 9
	3 هستم. میدانیم که:	$2^{90} \pmod{10}$ اقع ما به دنبال پاسخ $2^{90} \pmod{10}$	یاسخ: 🕮 دقت کنید که در و
		۔ عدد مثبت وجود دارد که کمتر از 10 ام	
		(3,10)=1 اول هستند، یعنی $(3,10)=1$	
		$3^4 = 1 \pmod{10}$ اریم:	• برطبق قضیه اویلر-فرما د
		نویسیم که:	🕰 آنگاه براحتی میتوانیم ب
	$3^{90} = 3^{4 \times 22 + 2} = (3^4)^{22} \times (3^$	$(3^2) = 9 \pmod{10}.$	

3 (ع ب 5 (ج 5 الف)

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

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

- ۲۹. کدام گزینه صحیح نیست؟ (می توانید چند گزینه را انتخاب کنید).
- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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.

ورسوال تشریحی) پاسخ: $a^{\phi(n)} = 1 \mod n \mod n$ این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ در مجموعه کاهش یافته مانده ها اگر $a^{\phi(n)} = 1 \mod n$ در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $a^{\phi(n)} = 1 \mod n$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

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

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
۲۳	14.4/.4/11	امنیت سیستمهای کامپیوتری		

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

ب) گمراه کنندگی - رمز - کلید

الف) انتشار - آشكار - متن رمز

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)

6 (ه.) 27 (ع.) 2 (ب.) 2 الف

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

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

ب) یک مساله تسهیم راز است.

الف) یک مساله از نوع روشهای غیرتعاملی است.

د) همه گزینهها صحیح است.

ج) یک مساله از نوع اثبات دانایی صفر 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

یاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

- ۵. كدام گزينه صحيح است؟ (شايد چند گزينه ياسخ 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.

PGP امنیت را در کدام لایه برای ما به ارمغان می آورد؟

د) لايه كاربرد	ج) لايه شبكه	ب) لايه انتقال	الف) لايه پيوند داده
		برد (Application Layer) است.	پاسخ: گزينه صحيح لايه كار،
حجم وسیعی از پراکنده است.	معنا است ساختاری آماری رو ح		
		۸۱ ۱۲ م	الف) گمراه کنندگی - متن آ.
	ب) گمراه کنند <i>گی -</i> متر د) انتشار - متن رمز شد		عداد عمراه سندنی - من اشکار - م ج) انتشار - متن آشکار - م
	باشد.	ن آشکار - متن رمز شده" صحیح م _و	
		ست با	۸. طول واقعی کلید DES برابر ا
۶۴ (۵	ج) ۲۳	ب) ۵۶	الف) ۴۸
		مىباشد.	پاسخ: گزینهی "۵۶" صحیح
	.(.	میتوانید چند گزینه را انتخاب کنید	۹. کدام گزینه صحیح نیست؟ (۵
باتی دشمن، نتواند بر اساس متن رمز شده	صورتی که علی رغم توان زیاد محاسب	UnconditionalSecur!) یعنی در	الف) امنيت بدون شرط (ity
	ی توسط متن رمز درز نمی کند.	که هیچگونه اطلاعاتی از متن اصلے	سیستم را بشکند، چرا
۱ از نظر محاسباتی پیچیده و طولانی باشد.	صورتی که شکستن سیستم رمز عملا	Computational Secur) یعنی در	ب) امنیت محاسباتی (rity
	V یا One Time Pad است.	امن شناخته شده، سامانه ernam	ج) تنها سامانه بدون شرط
. حملهگر در صورت مشاهده متن رمز، نباید	یک نویز به متن اصلی اضافه کنیم.	ى، ما بەصورت غيرعمد مىخواھيم	د) در یک سامانه رمزگذاری
		در مورد متن اصلی پی ببرد.	به هیچگونه اطلاعاتی د
مابقى گزينهها صحيح است.	یک نویز به متن اصلی اضافه کنیم.	ری، ما بهصورت عمدی می خواهیم	پاسخ: در یک سامانه رمزگذار
	ود(به طور دقیق).	اعث غیر خطی شدن سامانه میش	۱۰. كدام قسمت الگوريتم DES ب
P (s	E (ج	F (ب	الف) S
		ىباشد.	پاسخ: گزینهی "S" صحیح م
		سی است؟	۱۱. کدام شرط در مورد RSA الزاه
ببت به n اول باشد.	ب) کلید عمومی باید نس	به n اول باشد.	الف) متن اصلی باید نسبت ب
ببت به $\phi(n)$ اول باشد.	د) کلید عمومی باید نس	به $\phi(n)$ اول باشد.	ج) متن اصلی باید نسبت ب
	نهای که	لید عمومی در نظر م <i>ی گی</i> ریم، به <i>گ</i> و	پاسخ: پارامتر e را به عنوان ک
	$1 < e < \phi(n), (e, \phi(n))$	(n))=1.	
		_	
		ح است و كدام غلط؟ لطفا جلوى آ	
کننده است.	و نسبت به حمله نوع سوم کاملا شک		
		ئیات سامانه رمزگذاری آگاهی دارد	🔸 پ دشمن از تمامی حز

• الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمنى 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد. ۱۳۴

4 (s	2 (₇	ب) 8	الف) 6
(سوال تشریحی پاسخ: $a^{\phi(n)}=1$ هی در مجموعه کاهش یافته ماندهها ع	رسوال تشریحی) پاسخ: این مورد در n $mod \ n$	$\phi(n) = (p-1)(q-1)$ ، آنگاه n عدد n و n نسبت به همدیگر اول مجموع کاهشیافته ماندهها باشد کامل از مجموعه اول	۱۵. این قضیه را اثبات کنید: اگر دو $\mathbb{Z}_n^* = \{r_1, r_2, \dots, r_{\phi(n)}\}$ یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ ی
ىت.	ے) پاسخ: پاسخ این سوال در اسلایدها اس رمز کند و برای Bob ارسال کند.		
د) کلید محرمانه Bob	ج) كليد محرمانه Alice	ب) کلید عمومی Bob	الف) كليد عمومي Alice
	رده و برای او ارسال می کند. با رمز کند و برای Bob ارسال کند.	م m را با کلید عمومی Bob رمز کا Bob امضا کند، میبایست آن را ب	
د) کلید عمومی Alice	ج) كليد محرمانه Bob	ب) كليد محرمانه Alice	الف) كليد عمومي Bob
	کرده و برای Bob ارسال م <i>ی</i> کند.	$_{1}^{\prime}$ را با کلید خصوصی خودش رمز $_{1}^{\prime}$	n برای امضا، پیام Alice پاسخ: Alice برای امضا، پیام ۱۹. رقم آخر عدد 3^{90} چند است
6 (s	ج) 8	9 (ب	الف) 7
		ویسیم که:	يعنى چهار ع. $\phi(10)=4$

١٣. تعداد ريشه اوليه عدد 60 كدام گزينه است؟

قبول است و راه حل نمره ندارد.

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

۲۰. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل

الف) هيچكدام 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.

۴۲. اگر در الگوریتم RSA مقدار n=35 و مقدار e=5 باشد، آن گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

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

۲۳. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.

- الف امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- ب امنیت محاسباتی (Computational Security) یعنی در صورتی که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.
 - 🤫 تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.
- د در یک سامانه رمزگذاری، ما بهصورت غیرعمد می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 گزینه ها صحیح است.

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

الف) حمله نوع اول ب) حمله نوع دوم ج) هيچ كدام 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 می بایست برابر با طول متن اصلی باشد.
 - ب) کلید باید به صورت کاملا تصادفی تولید شود.
 - ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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 می شود (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. بدین سان می توان 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)

پاسخ: اگر $\{r_1, r_2, \dots, r_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1, ar_2, \dots, ar_{\phi(n)}$ باشد. پس پاسخ اعداد 10 و 7 است.

۲۷. کدام گزینه در مورد PGP صحیح است؟

- الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی 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 راه حل نمره ندارد.
 - ۳۰. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)
 - الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با (تباط، برابر با نفر برای برقراری ارتباط، برابر با با n
 - د) هیچکدام از گزینهها صحیح نیست

پاسخ: هیچ کدام 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
74	14.4/.4/1	امنیت سیستمهای کامپیوتری		

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)

17 (د) 10 ج) 10 ج) 34 الف)

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

۲. کدام گزینه در مورد PGP صحیح است؟

- الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

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

ب) انتشار - آشکار - متن رمز

الف) انتشار - رمز - كليد

د) گمراه کنندگی - آشکار - متن رمز

ج) گمراه کنندگی - رمز - کلید

ياسخ: گزينهي "گمراه كنندگي - رمز - كليد" صحيح ميباشد.

۴. كدام گزينه صحيح است؟ (شايد چند گزينه ياسخ 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 الگوریتههای کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینهها درست است.

۵. طول واقعی کلید DES برابر است با

الف) ۵۶ (ج با ۸۷ بالف) ۳۲ د) ۳۲ الف

پاسخ: گزینهی "۵۶" صحیح میباشد.

- کدام گزینه صحیح نیست؟ (میتوانید چند گزینه را انتخاب کنید).
- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.

پاسخ: در یک سامانه رمزگذاری، ما به صورت عمدی می خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه ها 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
۸.		دو (GSM) است. در هر دو، بخشی ا	ند متن اصلی معلوم (aintext Attack ز متن متن اصلی معلوم بوده است.	Known Pla)، رمزشکنی ماشین
	الف) لايه كاربرد	ب) لايه پيوند داده	ج) لايه شبكه	د) لايه انتقال
•	پاسخ: گزینه صحیح لایه کاربرد (yer		. = 1 .1	

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: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

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 بانتشار - متن آشکار - متن رمز شده ج) انتشار - متن رمز شده متن رمز شده دانتشار - متن رمز شده بانتشار - متن رمز شده دانتشار - متن رمز شده بانتشار - متن رمز شده دانتشار - متن رمز شده بانتشار - متن رمز شده بانتشار - متن رمز شده بانتشار - متن آشکار - متن رمز شده بانتشار - متن آشکار - متن رمز شده بانتشار - متن رمز شده بانتشار - متن آشکار - متن آشکار - متن رمز شده بانتشار - متن آشکار - متن آشکار - متن رمز شده بانتشار - متن آشکار - متن رمز شده بانتشار - متن آشکار - متن آشکار - متن آشکار - متن رمز شده بانتشار - متن آشکار - متن آ

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) هيچ كدام 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 (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.

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

- الف) طول كليد مي بايست برابر با طول متن اصلي باشد.
 - ب) کلید باید به صورت کاملا تصادفی تولید شود.
- ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

.۱۵. این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1, ar_2, \dots, r_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

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

16. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

پاسخ: این عدد ریشه اولیه ندارد.

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

ب) یک مساله تسهیم راز است.

الف) یک مساله از نوع روشهای غیرتعاملی است.

د) یک مساله از نوع اثبات دانایی صفر است.

ج) همه گزینهها صحیح 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 راه حل نمره ندارد.

١٩. كدام گزينه صحيح است؟ (شايد چند مورد صحيح باشد)

- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با رابر برای برقراری ارتباط، برابر با تعداد کلید در الگوریتمهای نامتقارن بین n نفر برای برقراری ارتباط، برابر با
 - 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

- ٠٠. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- ۔ الف امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه اطلاعاتی در مورد متن اصلی پی ببرد.

		، سامانه رمزگذاری آگاهی دارد.	- و دشمن از تمامی جزئیات
Vernuı فقط نسبت به حمله نوع اول،	، نویز به متن اصلی اضافه کنیم. m)، ما <u>بهصورت عمدی می</u> خواهیم یک	پاسخ: در یک سامانه رمزگذاری
		يح است.	ایمنی دارد. مابقی گزینهها صح
			۲۱. رقم آخر عدد 3^{90} چند است؟
د) 7	g (ج	ب) 8	الف) 6
	: هستم. میدانیم که:	$3^{90} \pmod{10}$ اقع ما به دنبال پاسخ	پاسخ: 🕮 دقت کنید که در و
	ىت و نسبت به آن اول هست.	دد مثبت وجود دارد که کمتر از 10 اس	يعنى چهار ع $\phi(10)=4$ •
		(3,10) = 1 اول هستند، یعنی	• عدد سه و ده نسبت به هم
			• برطبق قضیه اویلر-فرما دا
		ويسيم كه:	🔑 آنگاه براحتی میتوانیم بن
	$3^{90} = 3^{4 \times 22 + 2} = (3^4)^{22} \times$	$(3^2) - 9 \pmod{10}$	
		(0) V (Mod 10).	
	رمز کند و برای Bob ارسال کند.	Bob رمز کند، میبایست آن را با	۲۲. برای این که Alice پیامی را برای
د) کلید عمومی Alice	ج) كليد محرمانه Bob	ب) كليد محرمانه Alice	الف) كليد عمومي Bob
	و برای او ارسال می کند.	م m را با کلید عمومی Bob رمز کرده	پاسخ: Alice برای رمزکردن، پیا
	، طور دقیق).	ث غیر خطی شدن سامانه میشود(به	۲۳. كدام قسمت الگوريتم DES باعد
S (s	F (ج	P (ب	الف) E
		اشد.	پاسخ: گزینهی "S" صحیح می
••	رمز کند و برای Bob ارسال کند		۲۴. برای این که Alice پیامی را برای
د) کلید عمومی Bob	ج) كليد محرمانه Alice	ب) كليد محرمانه Bob	الف) كليد عمومي Alice
	ه و برای Bob ارسال می کند.	را با کلید خصوصی خودش رمز کرد \imath	پاسخ: Alice برای امضا، پیام <i>n</i>
نه خواهد شد؟	همان کلید محرمانه برابر با کدام گزید	و مقدار $e=5$ باشد، آنگاه d یا ه $n=$	۲۵. اگر در الگوريتم RSA مقدار 35
3 (د	ج) 5	و) 6	الف) 4
گیریم، بهگونهای که	ه را به عنوان کلید عمومی در نظر می	ىت. همانطور که م <i>ى</i> دانيد، پارامتر ^ع	پاسخ: گزینه صحیح عدد پنج ا
	$1 < e < \phi(n), ($	$(e,\phi(n)) = 1.$	
		نه در نظر م <i>ی گ</i> یریم، به گونهای که:	پارامتر d را به عنوان کلید محرما
	$ed \equiv 1 \pmod{8}$	$d \phi(n)$,	

- ه سامانه Vernum نسبت به حمله نوع اول و دوم مقاوم و نسبت به حمله نوع سوم کاملا شکننده است.

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

را نیز توضیح دهید؟ (سوال تشریحی) پاسخ: 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. كدام شرط در مورد RSA الزامي است؟

ب) کلید عمومی باید نسبت به n اول باشد.

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

الف) متن اصلی باید نسبت به n اول باشد.

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

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

- ۲۸. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- 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.

ياسخ:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمني دارد.
- ببله 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 حمله گر 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)

2 (د) 6 (ج) 27 (ب) 25 (الف)

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

۳۰. اثبات کنید که اگر p=pq باشد، آن گاه (p-1)(q-1)=(p-1) (سوال تشریحی) پاسخ: این مورد در کلاس توضیح داده شد.

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
۲۵	14.4/.4/11	امنیت سیستمهای کامپیوتری		

كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مىشود(به طور دقيق).

E (ع S (ج P (ب F (الف)

پاسخ: گزینهی "S" صحیح میباشد.

- ۲. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.
 - ۳. اگر در الگوریتم RSA مقدار n=35 و مقدار e=5 باشد، آن گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 6 (ب 5 (ج 5 الف) 6

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

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

طول واقعی کلید DES برابر است با

الف) ۳۲ (ج با ۸۶ د) ۵۶ (ع

ياسخ: گزينهي "۵۶" صحيح ميباشد.

- ۵. اثبات کنید که اگر p=pq باشد، آن گاه (p-1)(q-1) ((p-1)(q-1) ؛ (سوال تشریحی) پاسخ: این مورد در کلاس توضیح داده شد.
 - کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)
 - الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با رقوریتمهای نامتقارن بین n نفر برای برقراری ارتباط، برابر با
 - 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

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

ب) یک مساله از نوع روشهای غیرتعاملی است. د) یک مساله از نوع اثبات دانایی صفر است.

ب) کلید عمومی باید نسبت به n اول باشد.

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

الف) همه گزینهها صحیح است.

ج) یک مساله تسهیم راز 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 می بایست 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

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

الف) لايه پيوند داده ب) لايه شبكه ج) لايه كاربرد داده

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.

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

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای 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) هيچكدام ب) حمله نوع سوم ج) حمله نوع اول 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 مشتری نظیر الگوریتمهای رمزنگاری مورد پشتیبانی جلوگیری می شود؟ در تمام مراحل یکپارچگی پیامها حفظ می شود در تمام مراحل پیامها با کلید نامتقارن رمز می شود در مراحل انتهایی، کل پیامهای مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می شود. هیچکدام

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

باسخ: وند 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.

1۵. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

ى 4 (د) 8 (ج) 6 (ب) 2 (ف)

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 می شود بعد فشرده سازی و بعد امضا

ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمزکردن

د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

یاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

۱۸. كدام گزينه صحيح است؟ (شايد چند گزينه 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. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.

- الف امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.
- دوریک سامانه رمزگذاری، ما بهصورت غیرعمد می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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)

10 (د) 34 (د) 7

پاسخ: اگر $\{r_1,r_2,\dots,r_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1,ar_2,\dots,ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1,ar_2,\dots,ar_{\phi(n)}\}$ 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 صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.

پاسخ: در یک سامانه رمزگذاری، ما به صورت عمدی می خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه ها صحیح است.

.۲۲. این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آن گاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها اگر a عدد a در مجموعه کاهش یافته مانده ها باشد، آن گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a یعنی a 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) هيچكدام 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 این که Alice پیامی را برای Bob رمز کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد محرمانه Bob ب) كليد عمومي Alice ب) كليد عمومي Bob ج) كليد عمومي الف

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

- ۲۵. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- 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.

ىاسخ:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمني 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

پاسخ: اثبات می شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1,2,4,p^k,2 imes p^k\}$. 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 راه حل 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 بالف) گمراه کنندگی - رمز - کلید دی انتشار - آشکار - متن رمز بالمدی دی انتشار - رمز - کلید بالمدی داد با داد بالمدی داد با داد بالمدی داد بالمدی داد بالمدی داد بالمدی داد بالمدی داد بالمد

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

۲۹. برای این که Alice پیامی را برای Bob امضا کند، می بایست آن را با رمز کند و برای Bob ارسال کند.

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

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

۳۰. رقم آخر عدد 3^{90} چند است؟

8 (د) 8 (ج) 7 (ج) 6 (الف)

پاسخ: 🗖 دقت کنید که در واقع ما به دنبال پاسخ (10 3^{90} هستم. میدانیم که:

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

🖒 آنگاه براحتی میتوانیم بنویسیم که:

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

برگه	شماره	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
	78	14.4/.4/11	امنیت سیستمهای کامپیوتری		

- 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.
 - طول واقعی کلید DES برابر است با

لك ٤٤ (ع ج) ٣٢ (ج 4٨ با 4٨ با

پاسخ: گزینهی "۵۶" صحیح میباشد.

- ٣. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 گزینه ها صحیح است.

باسخ: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) باسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه ولیه 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)

یاسخ: اثبات می شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1,2,4,p^k,2 imes p^k\}$. بنابراین همه گزینههای فوق ریشه اولیه دارند.

- 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 می دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با (رتباط، برابر با نفر برای برقراری ارتباط، برابر با (رتباط، برابر با ایم تعداد کلید در الگوریتم های نامتقارن بین n
 - 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 می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

٧. كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مى شود(به طور دقيق).

F (د) S (ج P (ب E

پاسخ: گزینهی "S" صحیح میباشد.

- ۸. کدام گزینه صحیح نیست؟ (میتوانید چند گزینه را انتخاب کنید).
- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچگونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچگونه اطلاعاتی در مورد متن اصلی یی ببرد.

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

۹. رقم آخر عدد 3^{90} چند است؟

8 (ه 9 (ج 7 (ب 6 (الف)

پاسخ: 🕰 دقت کنید که در واقع ما به دنبال پاسخ (10 mod 10) هستم. می دانیم که:

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

🗀 آنگاه براحتی می توانیم 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 می شود؟ در تمام مراحل یکپارچگی پیامها حفظ می شود در تمام مراحل پیامها با کلید نامتقارن رمز می شود در مراحل انتهایی، کل پیامهای مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می شود. هیچ کدام

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

			؟ (شاید چند گزینه پاسخ باشد)	ً. كدام گزينه صحيح است	١
	بشتری دارند.	نامتقارن با طول کلید کمتر امنیت بی	متقارن نسبت به الگوريتم كليد	الف) الگوريتمهاي كليد	
	ه کمتری احتیاج دارند.	الگوریتم کلید نامتقارن به تعداد کلید	ریتمهای کلید متقارن نسبت به	ب) در یک شبکه، الگو	
		، بر نظریه اعداد است.	لگوریتمهای کلید متقارن مبتنی	ج) امنیت بسیاری از ا	
	ه کانال امن نداریم.	مازوکاری به مانند گواهینامه، نیازی <u>ب</u>	لید نامتقارن در صورت داشتن س	د) در الگوریتمهای کا	
ت.	.)، همه گزینهها درست است	، متقارن مبتنی بر نظریه اعداد است	بت بسیاری از الگوریتمهای کلید	پاسخ: به جز گزینه (امنی	
		ط شانون، غلط است؟	One Time Pad پیشنهادی توس	ا. کدام گزینه در مورد رمز $^{ m l}$	١
			ت برابر با طول متن اصلی باشد.	الف) طول كليد مىبايس	
			، کاملا تصادفی تولید شود.	ب) کلید باید به صورت	
		کلید است.	صل از XOR دنباله متن اصلی با	ج) دنباله متن رمز حاه	
		یی و پردازش زیاد دارد.	ملا نیاز به یک زمان بسیار طولان	د) شکستن این رمز ء	
سل استوار است که	صلى. اين الگوريتم، بر اين ام	Key Sed) داریم به اندازه طول متن ام	One T یک دنباله کلید (quence	پاسخ: در رمز Time Pad	
		(بیت به بیت با یکدیگر XOR شود).			
ژگی امنیت بدون شر	ه شانون، چنین سامانهای وی	رتباطی با متن اصلی ندارد. از دیدگا	«تصادفی» خواهد بود، که هیچ ا	نتيجه يک متن رمز واقعاً	
	ارسال کرد.	ود (Eavesdropping)، برای گیرنده	ن این متن رمز را بدون خطر شنو	را دارد. بدینسان میتوا	
	ِ درس داده شد)	ح شد، صحيح است؟ (اين مورد امروز	ه غار علیبابا که در کلاس مطر-	ٔ. کدام گزینه در مورد مسال	١
	هیم راز است.	ب) یک مساله تس	ح است.	الف) همه گزینهها صحی	
ت.	وع روشهای غیرتعاملی اس	د) یک مساله از ن	بات دانایی صفر است.	ج) يک مساله از نوع اڏ	
		بات دانایی صفر است.	حیح است: یک مساله از نوع اثر	پاسخ: فقط این گزینه ص	
			'یه برای ما به ارمغان می آورد؟	. PGP امنیت را در کدام لا	١
اربرد	د) لايه ک	ج) لايه شبكه	ب) لايه انتقال	الف) لايه پيوند داده	

ياسخ: گزينه صحيح لايه كاربرد (Application Layer) است.

1۵. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

6 (ب 2 الف)

یاسخ: این عدد ریشه اولیه ندارد.

۱۶. کدام شرط در مورد RSA الزامی است؟

الف) متن اصلی باید نسبت به n اول باشد.

ج) کلید عمومی باید نسبت به n اول باشد.

یاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

ج) 8

د) 4

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

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

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

د) هیچکدام	ج) حمله نوع دوم	ب) حمله نوع اول	الف) حمله نوع سوم
Known Plainte)، رمزشکنی ماشین	، یا چند متن اصلی معلوم (xt Attack	، حمله نوع دوم یا حمله بر اساس یک	پاسخ: دو مثال مشهور، در زمینه
	شی از متن متن اصلی معلوم بوده اس		
ه خواهد شد؟	همان کلید محرمانه برابر با کدام گزین	و مقدار $e=5$ باشد، آنگاه d یا و $n=1$	۱۸. اگر در الگوریتم RSA مقدار 35 =
4 (۵	ج) 5	ب) 3	الف) 6
گیریم، به گونهای که	$_{\circ}$ را به عنوان کلید عمومی در نظر می $_{\circ}$	ىت. همانطور كه مىدانيد، پارامتر ^چ	پاسخ: گزینه صحیح عدد پنج اس
	$1 < e < \phi(n), ($	$e, \phi(n)) = 1.$	
		نه در نظر می <i>گیریم، به گونهای که:</i>	پارامتر d را به عنوان کلید محرمان
	$ed \equiv 1 \pmod{\frac{1}{2}}$	$d \phi(n)$,	
پیمانه 24 را محاسبه کنیم که برابر با 5	د. سپس باید معکوس عدد $e=5$ در	یم که برابر با $\phi(35) = 24$ خواهد ش	
	صورت پذیرفت؟	ط Turing، توسط چه نوع حملهای <i>ح</i>	خواهد شد. ۱۹. رمزشکنی ماشین Enigma توسط
د) حمله نوع دوم	ج) حمله نوع سوم	ب) هیچکدام	الف) حمله نوع اول
Known Plainte)، رمزشکنی ماشین	، یا چند متن اصلی معلوم (xt Attack	، حمله نوع دوم یا حمله بر اساس یک	پاسخ: دو مثال مشهور، در زمینه
	شی از متن متن اصلی معلوم بوده اس		
			۲۰. پروتکل توافق کلید دیفی-هلمن
	رمز کند و برای Bob ارسال کند	Bob امضا کند، میبایست آن را با	۲۱. برای این که Alice پیامی را برای
د) كليد محرمانه Bob	ج) كليد محرمانه Alice	ب) کلید عمومی Alice	الف) كليد عمومي Bob
	ه و برای Bob ارسال م <i>ی ک</i> ند.	ً را با کلید خصوصی خودش رمز کرد	پاسخ: Alice برای امضا، پیام <i>m</i>
ر ملاک است، هر کس پاسخ درستی	پاسخ: برابر با ۸ میشود. جواب آخ	را محاسبه کنید؟ (سوال تشریحی)	۲۲ . معکوس عدد پنج در مبنای 1 ³ ر
			نوشته باشد قابل قبول است و راه
			۲۳. اثبات کنید که اگر $pq=n$ باشد.
سیعی از پراکنده است.	است ساختاری اماری رو حجم و	ی ویژگی را دارد که به این معنا ا	۲۴ . طبق گفته شانون یک سامانه قو ر
ر - متن رمز شده	ب) گمراه کنندگی - متن آشکا		الف) انتشار - متن رمز شده - من
رمز شده	د) انتشار - متن آشکار - متن	شده - متن آشکار	ج) گمراه کنندگی - متن رمز ،
	د.	نکار - متن رمز شده" صحیح میباش	پاسخ: گزینهی "انتشار - متن آش
	رمز کند و برای Bob ارسال کند.	Bob رمز کند، میبایست آن را با	۲۵. برای این که Alice پیامی را برای

الف) کلید محرمانه Alice ب) کلید محرمانه Bob با کلید محرمانه عمومی د) کلید عمومی Bob پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می کند.

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

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

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

۲۷. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.

۲۸. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا

- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمز کردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی 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)

134 (د) 7 (ج) 17 (الف) 10 (د)

پاسخ: اگر $\{r_1,r_2,\ldots,r_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1,ar_2,\ldots,ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر a السد. 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.

باسخ:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمني 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
77	14.4/.4/11	امنیت سیستمهای کامپیوتری		

ئزینه در مورد مساله غار علیبابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)	ندام	کد	• '
--	------	----	-----

ب) یک مساله از نوع اثبات دانایی صفر است.

الف) یک مساله از نوع روشهای غیرتعاملی است.

د) یک مساله تسهیم راز است.

ج) همه گزینهها صحیح 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 بانتشار - متن رمز شده - متن آشکار بانتشار - 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.

- ٣. پروتكل توافق كليد ديفي-هلمن را توضيح دهيد؟ (سوال تشريحي) پاسخ: پاسخ اين سوال در اسلايدها است.
 - ۴. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- 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 اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمني 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.
 - ۵. طول واقعی کلید DES برابر است با

الف) ۳۲ (ج) ۵۶ ج) ۴۸ د) ۶۴

ياسخ: گزينهي "۵۶" صحيح ميباشد.

9. 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)

17 (د) 34 (ج) 10 (ب) 71 الف)

پاسخ: اگر $\{x_1, x_2, \dots, x_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد $x_n = \{x_1, x_2, \dots, x_{\phi(n)}\}$ مانده ها یعنی $\{x_1, x_2, \dots, x_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $x_n = \{x_1, x_2, \dots, x_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $x_n = \{x_1, x_2, \dots, x_{\phi(n)}\}$ باشد. پس پاسخ اعداد 10 و 7 است.

- ۷. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل 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؟

د) 6 7 (~ 2 (ت الف) 9 پاسخ: 🛍 دقت کنید که در واقع ما به دنبال پاسخ (10 mod 10) هستم. می دانیم که: • $\phi(10)=4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست. (3,10) = 1 عدد سه و ده نسبت به هم اول هستند، یعنی • $3^4=1\pmod{10}$ برطبق قضیه اویلر-فرما داریم: •

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

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

د) 25 2 (ج 6 (ب الف) 27

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

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

- الف) طول كليد مي بايست برابر با طول متن اصلى باشد.
 - ب) کلید باید به صورت کاملا تصادفی تولید شود.

🔼 آن گاه براحتی می توانیم بنویسیم که:

- ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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 می شود (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. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

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

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

١٣. تعداد ريشه اوليه عدد 60 كدام گزينه است؟

د) 8 2 (ب الف) 6 ج) 4

یاسخ: این عدد ریشه اولیه ندارد.

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

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

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

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

١٥. كدام گزينه صحيح است؟ (شايد چند گزينه ياسخ 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 الگوریتههای کلید متقارن مبتنی بر نظریه اعداد است.)، همه گزینهها درست است.

- ۱۶. اثبات کنید که اگر p=pq باشد، آن گاه (p-1)(q-1) ((p-1)(q-1) باشد، آن گاه (p-1)(q-1) باشد، آن گاه روز در کلاس توضیح داده شد.
 - ١٧. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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.

این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آن گاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها باشد، آن گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها باشد، آن گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a یعنی a 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 می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

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

- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با روتباط، برابر با نفر برای برقراری ارتباط، برابر با روتباط، برابر با روتباط، برابر با
 - 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

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

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

۲۲. کدام شرط در مورد RSA الزامی است؟

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

الف) متن اصلی باید نسبت به n اول باشد.

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

ج) کلید عمومی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

٢٣. كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مىشود(به طور دقيق).

E (د) F (ج P (ب S

ياسخ: گزينهي "S" صحيح ميباشد.

۲۴. برای این که Alice پیامی را برای Bob رمز کند، می بایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد محرمانه Alice ب) كليد محرمانه Bob ج) كليد عمومي Bob د) كليد عمومي

یاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می کند.

- ۲۵. کدام گزینه صحیح نیست؟ (میتوانید چند گزینه را انتخاب کنید).
- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه اطلاعاتی در مورد متن اصلی پی ببرد.

رينهها صحيح است.	نویز به متن اصلی اضافه کنیم. مابقی گز)، ما <u>بهصورت عمدی می</u> خواهیم یک	پاسخ: در یک سامانه رمزگذاری
لاک است، هر کس پاسخ درستی	پاسخ: برابر با ۸ میشود. جواب آخر م	را محاسبه کنید؟ (سوال تشریحی)	۲۶. معکوس عدد پنج در مبنای 13
		اه حل نمره ندارد.	نوشته باشد قابل قبول است و ر
	رمز کند و برای Bob ارسال کند.) Bob امضا کند، میبایست آن را با	۲۷. برای این که Alice پیامی را برای
د) کلید عمومی Bob	ج) کلید محرمانه Alice	ب) کلید عمومی Alice	الف) كليد محرمانه Bob
		را با کلید خصوصی خودش رمز کرد m مط Turing، توسط چه نوع حملهای م	
د) حمله نوع سوم	ج) حمله نوع اول	ب) حمله نوع دوم	الف) هيچ كدام

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.

PGP . ۲۹ امنیت را در کدام لایه برای ما به ارمغان می آورد؟

الف) لايه پيوند داده ب) لايه انتقال ج) لايه كاربرد د) لايه شبكه

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

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

6 (د) 3 (ج) 5 الف) 5

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

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

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
۲۸	14.4/.4/11	امنیت سیستمهای کامپیوتری		
		دین قسمت وابسته باشد.	ین از متن باید به چند	ویژگی به این معنا است که هر ب
	ى	ب) انتشار - رمز - کلید	رمز	لف) گمراه کنندگی - آشکار - متن
	تن رمز	د) انتشار - آشکار - م		ج) گمراه کنند <i>گی</i> - رمز - کلید

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

». كدام قسمت الگوريتم DES باعث غير خطي شدن سامانه مي شود (به طور دقيق).

P (د) $S(\tau)$ $E(\tau)$ F(t)

ياسخ: گزينهي "S" صحيح ميباشد.

١.

- 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 راه حل نمره ندارد.
 - ۵. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

6 (د) 2 (ج) 4 (ب) 8 الف)

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) هيچ كدام 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. كدام گزينه صحيح است؟ (شايد چند گزينه ياسخ 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 این که Alice پیامی را برای Bob رمز کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد محرمانه Bob ب) كليد محرمانه Alice ج) كليد عمومي Bob د) كليد عمومي

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

- ۹. کدام گزینه در مورد PGP صحیح است؟
- الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا

- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور 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، آن گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

 $4 \ (چ \ 6 \ (ب \ 5 \)$ الف $5 \ (خ)$

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

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

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

- الف) طول كليد مى بايست برابر با طول متن اصلى باشد.
 - ب) کلید باید به صورت کاملا تصادفی تولید شود.
- ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۲. اثبات کنید که اگر p=pq باشد، آن گاه (p-1)(q-1) (سوال تشریحی) پاسخ: این مورد در کلاس توضیح داده شد.

۱۳. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.

 3^{90} وقم آخر عدد 3^{90} چند است?

8 (د) 9 (ج) 9 (الف) 7

پاسخ: 🗖 دقت کنید که در واقع ما به دنبال پاسخ (10 3^{90} هستم. میدانیم که:

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

🗀 آنگاه براحتی میتوانیم بنویسیم که:

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

	ونهای که	کلید عمومی در نظر می گیریم، به گر	پاسخ: پارامتر e را به عنوان
	$1 < e < \phi(n), (e, \phi(n))$	n)) = 1.	
	کن است چند گزینه صحیح باشد)	اولیه (Primitive Root) دارند؟ (مم	۱۸. کدام یک از اعداد زیر ریشه
2 (ა	ج) 6	ب) 27	الف) 25
عاسباتی دشمن، نتواند بر اساس متن رمز شده عملا از نظر محاسباتی پیچیده و طولانی باشد. بم. حملهگر در صورت مشاهده متن رمز، نباید	ن عبارت صحیح /غلط را بنویسید. در صورتی که علی رغم توان زیاد مح ی توسط متن رمز درز نمی کند. در صورتی که شکستن سیستم رمز در صورتی که شکستن سیستم رمز به متن اصلی اضافه کنب سبت به حمله نوع سوم کاملا شکن میک نویز به متن اصلی اضافه ک	نیح است و کدام غلط؟ لطفا جلوی آ لا (UnconditionalSecurity) یعنی ا که هیچگونه اطلاعاتی از متن اصلر (Computational Security) یعنی سرط امن شناخته شده، سامانه nam داری، ما بهصورت غیرعمد میخواهد در مورد متن اصلی پی ببرد. ببت به حمله نوع اول و دوم مقاوم و و بیات سامانه رمزگذاری آگاهی دارد. ذاری، ما بهصورت عمدی میخواهد	۱۹. کدام یک از جملات زیر صح الف امنیت بدون شرط سیستم را بشکند، چر ب امنیت محاسباتی (ج تنها سامانه بدون ش د در یک سامانه رمزگذ به هیچگونه اطلاعاتی و دشمن از تمامی جز پاسخ: در یک سامانه رمزگ ایمنی دارد. مابقی گزینهها
د) حمله نوع دوم	ج) حمله نوع سوم	ب) هیچکدام	الف) حمله نوع اول
رمزشکنی ماشین (Known Plaintext Atta)، رمزشکنی ماشین بوده است. $a^{\phi(n)}=1 \mod n$ (سوال تشریحی) پاسخ: ضرب عدد a در مجموعه کاهش یافته ماندهها	و، بخشی از متن متن اصلی معلوم ل باشند، آنگاه خواهیم داشت:	یای نسل دو (GSM) است. در هر در a دو عدد a و a نسبت به همدیگر او	Enigma و A5/2 در شبکهه ۲۱. این قضیه را اثبات کنید: اگ

۱۵. برای این که Alice پیامی را برای Bob امضا کند، می بایست آن را با رمز کند و برای Bob ارسال کند.

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

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

د) کلید محرمانه Alice

ج) کلید عمومی Alice

الف) كليد عمومي Bob ب) كليد محرمانه

۱۷. کدام شرط در مورد RSA الزامی است؟

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

ج) کلید عمومی باید نسبت به n اول باشد.

یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ 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 علی بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

ب) یک مساله از نوع اثبات دانایی صفر است.

الف) همه گزینهها صحیح است.

د) یک مساله از نوع روشهای غیرتعاملی است.

ج) یک مساله تسهیم راز است.

یاسخ: 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 می شود؟ در تمام مراحل یکپارچگی پیامها حفظ می شود در تمام مراحل پیامها با کلید نامتقارن رمز می شود در مراحل انتهایی، کل پیامهای مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می شود. هیچکدام

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

۲۴. طول واقعی کلید DES برابر است با

الف) ۵۶ ج) ۴۸ ب

ياسخ: گزينهي "۵۶" صحيح ميباشد.

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)

17 (د) 7 (ج على على الله) 10 الف) 17 (د) 7 (على الله) 17 (د) 17 (د) 17 (د) 19 (

پاسخ: اگر $\{r_1, r_2, \dots, r_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1, ar_2, \dots, ar_{\phi(n)}$ باشد. پس پاسخ اعداد 10 و 7 است.

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

- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با (تباط، برابر با رقراری ارتباط، برابر با با تعداد کلید در الگوریتمهای نامتقارن بین n نفر برای برقراری ارتباط، برابر با
 - 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

- ۲۷. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- 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 اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمني دارد.
- ببله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری بر مخفی ماندن کلید باشد، حتی اگر حمله گر 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 صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه اطلاعاتی در مورد متن اصلی پی ببرد.

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

PGP .۲۹ امنیت را در کدام لایه برای ما به ارمغان می آورد؟

الف) لايه شبكه ب) لايه كاربرد ج) لايه انتقال داده

ياسخ: گزينه صحيح لايه كاربرد (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.

ب) گمراه کنندگی - متن رمز شده - متن آشکار

د) انتشار - متن آشکار - متن رمز شده

الف) گمراه کنندگی - متن آشکار - متن رمز شده

ج) انتشار - متن رمز شده - متن آشکار

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

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
79	14.4/.4/11	امنیت سیستمهای کامپیوتری		

 3^{90} چند است 3^{90}

7 (ع ج) 8 (ج ب) 9 الف)

پاسخ: 🗖 دقت کنید که در واقع ما به دنبال پاسخ (10 3^{90} هستم. میدانیم که:

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

🗖 آنگاه براحتی میتوانیم بنویسیم که:

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

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 - متن آشکار 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، آن گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

6 (د) 3 (ج) 5 (ب) 4 (لف)

یاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

پس ابتدا $\phi(n)$ را محاسبه می کنیم که برابر با $\phi(35)=24$ خواهد شد. سپس باید معکوس عدد e=5 در پیمانه $\phi(n)=24$ را محاسبه کنیم که برابر با $\phi(n)=0$ 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)

		و راه حل نمره ندارد.	نوشته باشد قابل قبول است
		حیح است؟	۸. کدام گزینه در مورد PGP ص
	سازی و بعد امضا	ِمزنگاری انجام میشود بعد فشرده	
		نشردهسازی انجام میشود بعد رمز	
		مضا انجام میشود بعد فشردهسازی	
		مضا انجام میشود بعد رمزکردن و ب	
مريد فشري ما المريد من المريد التريد فالمريد			
ِد، بعد فشردهسازی و بعد عملیات رمز <i>گ</i> ذاری.	اهضای دیجینال بر روی پیام می حور	ی نیر مطرح سد، در ۱۵۱ اول یک	پسی. همان طور که در کاره
(یدها است.	حی) پاسخ: پاسخ این سوال در اسا	لمن را توضيح دهيد؟ (سوال تشريه	۹. پروتکل توافق کلید دیفی-ھ
		ام گزینه است؟	۱۰. تعداد ریشه اولیه عدد 60 کد
8 (১	ع) 4	2 (ب	الف) 6
0 (3	± (¿	2 (ب	0 (32)
		دارد.	پاسخ: این عدد ریشه اولیه ن
		است با	۱۱. طول واقعی کلید DES برابر
۶۴ (۵	ج) ۵۶	ب) ۴۸	الف) ۳۲
/ 1 (3	ج/ (ج	ب ۱۸	11 (3)
		مىباشد.	پاسخ: گزینهی "۵۶" صحیح
	لهای صورت پذیرفت؟	توسط Turing، توسط چه نوع حما	۱۲. رمزشکنی ماشین Enigma:
د) حمله نوع دوم	ج) حمله نوع اول	ب) هیچکدام	الف) حمله نوع سوم
Known Plaintext Atta)، رمزشکنی ماشین			
وده است.	و، بخشی از متن متن اصلی معلوم ب		
		ثاید چند گزینه پاسخ باشد)	 کدام گزینه صحیح است؟ (نا
ی دارند.	رن با طول کلید کمتر امنیت بیشتر _؟	نارن نسبت به الگوريتم كليد نامتقا	الف) الگوريتمهاي كليد متق
ری احتیاج دارند.	تم کلید نامتقارن به تعداد کلید کمت	مهای کلید متقارن نسبت به الگوری	ب) در یک شبکه، الگوریتر
	ریه اعداد است.	ریتمهای کلید متقارن مبتنی بر نظ	ج) امنیت بسیاری از الگو
ل امن نداريم.	ِی به مانند گواهینامه، نیازی به کانا	نامتقارن در صورت داشتن سازوکار	د) در الگوریتمهای کلید
مه گزینهها درست است.	ِن مبتنی بر نظریه اعداد است.)، ه	بسیاری از الگوریتمهای کلید متقار	پاسخ: به جز گزینه (امنیت
ست، هر کس پاسخ درستی نوشته باشد قابل	ِ با ۳۲ میشود. جواب آخر ملاک ا	د؟ (سوال تشریحی) پاسخ: برابر	را محاسبه کنیا $\phi(80)$ را محاسبه کنیا
			1.0
		رد.	قبول است و راه حل نمره ندا
	۱۷۰		قبول است و راه حل نمره ندا RSA الزا

ج) 34

E (ج

پاسخ: اگر a عدد a عدد a در مجموع کاهشیافته مانده ها باشد، آن گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته

مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ باشد. پس پاسخ اعداد 10 و 7 است.

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

ب) 10

كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مىشود(به طور دقيق).

P (ب

الف) 7

الف) F

پاسخ: گزینهی "S" صحیح میباشد.

د) 17

S (۵

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

الف) 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 می گیریم، به گونهای که

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

۱۶. اثبات کنید که اگر p=pq باشد، آن گاه (p-1)(q-1) ((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.

ب) گمراه کنندگی - رمز - کلید

ج) گمراه کنندگی - آشکار - متن رمز

الف) انتشار - رمز - كليد

د) انتشار - آشکار - متن رمز

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

۳A. PGP امنیت را در کدام لایه برای ما به ارمغان می آورد؟

الف) لايه پيوند داده ب) لايه كاربرد ج) لايه انتقال د) لايه شبكه

ياسخ: گزينه صحيح لايه كاربرد (Application Layer) است.

۱۹. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح/غلط را بنويسيد.

- الف امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.
- دریک سامانه رمزگذاری، ما بهصورت غیرعمد میخواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 <u>بهصورت عمدی می</u>خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینهها صحیح است.

۲۰. برای این که 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 Bob د) کلید عمومی

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

۲۱. كدام گزينه صحيح است؟ (شايد چند مورد صحيح باشد)

- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با رابر برای برقراری ارتباط، برابر با تعداد کلید در الگوریتمهای نامتقارن بین n نفر برای برقراری ارتباط، برابر با
 - 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 می دهد.

• توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

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

- الف) طول كليد مى بايست برابر با طول متن اصلى 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 متن اصلی ندارد. از دیدگاه شانون، چنین سامانهای ویژگی امنیت بدون شرط را دارد. بدین سان می توان 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)

6 (د) 25 (ج) 25 (ج) 27 (الف)

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

۲۴. برای این که Alice پیامی را برای Bob امضا کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد عمومي Alice ب) كليد محرمانه Bob ج) كليد محرمانه Alice د) كليد عمومي

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

۲۵. کدام گزینه در مورد مساله غار علی بابا 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.

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

- ۲۶. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- 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.

یاسخ:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمنى دارد.
- ببله 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 حمله گر 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 صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.

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

باسخ: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a یعنی a یک جایگشت کامل از مجموعه اولیه است. پس داریم:

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

- ۱۹۰. 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: یاسخ 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: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
٣٠	14.47.411	امنیت سیستمهای کامپیوتری		

ل. این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها اگر $\mathbb{Z}_n^* = \{r_1, r_2, \dots, r_{\phi(n)}\}$ 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.

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 راه حل 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: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

۵. كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

$$S$$
 (ه F (ج E (ب P الف)

پاسخ: گزینهی "S" صحیح میباشد.

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

الف) حمله نوع سوم ب) هيچ كدام ج) 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 می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام میخورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

- ۸. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) پاسخ: پاسخ این سوال در اسلایدها است.
 - ۹. برای این که Alice پیامی را برای Bob امضا کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

Bob جرمانه Alice ب) کلید محرمانه Alice ج) کلید عمومی Alice کلید عمومی

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

- ۱۰. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- 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 حمله گر 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 صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.

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

۱۲. برای این که Alice پیامی را برای Bob رمز کند، می ایست آن را با رمز کند و برای Bob ارسال کند.

Alice کلید محرمانه Bob برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می کند.

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

4 (ه 5 (ج 3 (ب 6 (الف)

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

پس ابتدا $\phi(n)$ را محاسبه می کنیم که برابر با $\phi(35)=24$ خواهد شد. سپس باید معکوس عدد e=5 در پیمانه $\phi(n)=24$ را محاسبه کنیم که برابر با $\phi(n)=0$ خواهد شد.

- باسخ: وند 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 كليد مي بايست برابر با طول متن اصلى 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان 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)

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

۱۷. طول واقعی کلید DES برابر است با

ياسخ: گزينهي "۵۶" صحيح ميباشد.

- ۱۸. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.
- در یک سامانه رمزگذاری، ما بهصورت غیرعمد می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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)

34 (د) 10 (ج) 17 (الف) 7

پاسخ: اگر $\{r_1,r_2,\dots,r_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1,ar_2,\dots,ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1,ar_2,\dots,ar_{\phi(n)}\}$ باشد. پس پاسخ اعداد 10 و 7 است.

- ۲۰. كدام گزينه صحيح است؟ (شايد چند گزينه 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؟

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

الف) متن اصلی باید نسبت به n اول باشد.

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

ج) کلید عمومی باید نسبت به n اول باشد.

پارمتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

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

ب) یک مساله از نوع اثبات دانایی صفر است.

الف) یک مساله از نوع روشهای غیرتعاملی است.

د) همه گزینهها صحیح است.

ج) یک مساله تسهیم راز است.

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

۲۳. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.

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

- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با روتباط، برابر با نفر برای برقراری ارتباط، برابر با روتباط، برابر با روتباط، برابر با
 - 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، 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.

ج) انتشار - متن آشکار - متن ره	ز شده	د) انتشار - متن رمز شده - متن آه	شكار
پاسخ: گزینهی "انتشار - متن آشک رقم آخر عدد 3 ⁹⁰ چند است؟	ر - متن رمز شده" صحیح میباشد.		
الف) 6	ب) 8	ج) 9	7 (১
	$3^4 = 1 \pmod{10}$:	و نسبت به آن اول هست.	
اثبات کنید که اگر $n=pq$ باشد، آ PGP امنیت را در کدام لایه برای ما	گاه $\phi(n)=(p-1)(q-1)$ ؟ (سواا) به ارمغان می آورد؟	ل تشریحی) پاسخ: این مورد در کلا	س توضیح داده شد.
الف) لايه كاربرد	ب) لايه پيوند داده	ج) لايه انتقال	د) لايه شبكه
پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است. 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

ج) 8

Enigma و A5/2 در شبکههای نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

ب) 4

الف) گمراه کنندگی - متن آشکار - متن رمز شده

.٢۶

.۲۷

۸۲.

.۲۹

الف) 2

۳۰. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

یاسخ: این عدد ریشه اولیه ندارد.

ب) گمراه کنندگی - متن رمز شده - متن آشکار

د) 6

شماره برگه	تاریخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
٣١	14.4/.4/11	امنیت سیستمهای کامپیوتری		
		عی) پاسخ: پاسخ این سوال در اسا <i>ر</i>		
	ال کند.	ا با رمز کند و برای Bob ارس	ی Bob امضا کند، میبایست آن ر	ی این که Alice پیامی را برای

یاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می کند.

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)

پاسخ: اگر $\{r_1, r_2, \dots, r_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1, ar_2, \dots, ar_{\phi(n)}\}$ باشد. پس پاسخ اعداد 10 و 7 است.

۴. کدام گزینه در مورد مساله غار علی بابا 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 راه حل نمره ندارد.
 - رمزشكنى ماشين Enigma توسط Turing، توسط چه نوع حملهاى صورت پذيرفت؟

الف) حمله نوع سوم ب) حمله نوع دوم ج) هيچ كدام 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 a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها اگر $\mathbb{Z}_n^* = \{r_1, r_2, \dots, r_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

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

٨. تعداد ريشه اوليه عدد 60 كدام گزينه است؟

8 (ه ج ع الف) 2

پاسخ: این عدد ریشه اولیه ندارد.

۹. رقم آخر عدد 3^{90} چند است؟

١.

۲.

9 (ه ج ع الف) 7 الف) 7

پاسخ: 🕰 دقت کنید که در واقع ما به دنبال پاسخ (10 3^{90} هستم. میدانیم که:

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

🛍 آنگاه براحتی میتوانیم بنویسیم که:

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

- ١٠. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح/غلط را بنويسيد.
- الف امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 كليد مي بايست برابر با طول متن اصلى 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۲. طول واقعی کلید DES برابر است با

الف) ۳۲ (ب که ۲۸ د) ۴۸ د) ۴۸ د)

پاسخ: گزینهی "۵۶" صحیح میباشد.

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

الف) لايه پيوند داده ب) لايه شبكه ج) لايه كاربرد د) لايه انتقال

ياسخ: گزينه صحيح لايه كاربرد (Application Layer) است.

14. كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مىشود(به طور دقيق).

ياسخ: گزينهي "S" صحيح مي باشد.

۱۵. اثبات کنید که اگر p=pq باشد، آنگاه (p-1)(q-1) ((p-1)(q-1) ؛ (سوال تشریحی) پاسخ: این مورد در کلاس توضیح داده شد.

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

د) کلید محرمانه Alice

ج) کلید عمومی Bob

ب) کلید محرمانه Bob

الف) کلید عمومی Alice

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

۱۷. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.

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

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

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

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

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

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

ب) انتشار - آشکار - متن رمز د) گمراه کنندگی - رمز - کلید الف) گمراه کنندگی - آشکار - متن رمز ج) انتشار - 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 صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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.

یاسخ

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمنى دارد.
- ببله 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 حمله گر 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 می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

۲۴. کدام شرط در مورد RSA الزامی است؟

n اول باشد. باید نسبت به n اول باشد.

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

د) کلید عمومی باید نسبت به n اول باشد.

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

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای 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)

 پاسخ: اثبات می شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1,2,4,p^k,2 imes p^k\}$. 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: یاسخ این سوال در اسلایدها است.
 - ۲۷. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حملهای صورت پذیرفت؟

الف) هيچ كدام 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. كدام گزينه صحيح است؟ (شايد چند گزينه 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 كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با روتباط، برابر با تعداد کلید در الگوریتمهای نامتقارن بین n نفر برای برقراری ارتباط، برابر با
 - د) هیچکدام از گزینهها صحیح نیست

پاسخ: هیچ کدام 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
٣٢	14.4/.4/11	امنیت سیستمهای کامپیوتری		

- ١. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى أن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 گزینه ها صحیح است.

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

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

- ۳. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) یاسخ: پاسخ این سوال در اسلایدها است.
 - PGP امنیت را در کدام لایه برای ما به ارمغان می آورد؟

الف) لايه انتقال ب) لايه پيوند داده ج) لايه كاربرد د) لايه شبكه

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

۵. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

6 (ء ع الف) 2 ج) 8 (ج

یاسخ: این عدد ریشه اولیه ندارد.

 \mathbb{Z}_{17}^* 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)

10 (د) 34 (ج) 71 الف) 7

پاسخ: اگر $\{ar_1,ar_2,\ldots,r_{\phi(n)}\}$ عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1,ar_2,\ldots,ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر a الست، اگر a 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.
 - Λ . رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حملهای صورت پذیرفت؟

الف) هيچكدام 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 ج) ۳۲ ج

پاسخ: گزینهی "۵۶" صحیح میباشد.

- ١٠. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- 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.

ياسخ:

- الف این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- ببله 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 حمله گر 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 راه حل نمره ندارد.
 - ۱۲. کدام شرط در مورد RSA الزامی است؟

الف) کلید عمومی باید نسبت به n اول باشد. γ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

١٣. كدام گزينه صحيح است؟ (شايد چند گزينه پاسخ باشد)

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

- ب) دریک 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.

متن اَشکار - متن رمز شده	د) گمراه کنندگی -	متن رمز شده - متن آشکار	ج) گمراه کنندگی -
، است، هر کس پاسخ درستی نوشته باشد قابل		ر - متن آشکار - متن رمز شده " صحیح ه ه کنید؟ (سوال تشریحی) باسخ : برای	
ا است بر حس پسی فرستی توست بست فین	ر به ۲۰ سی سوده جورب و در در		قبول است و راه حل نم
	شود(به طور دقیق).	ر DES باعث غیر خطی شدن سامانه می	
F (
F (۵	Р (ج	S (ب	الف) E
			پاسخ: گزینهی "S" ص
		است؟	۱۷. رقم آخر عدد 3^{90} چند
د) 9	ج) 7	6 (ب	الف) 8
	n 3 ⁹⁰ (مستم. میدانیم که:	ید که در واقع ما به دنبال پاسخ (mod 10	پاسخ: 🕮 دقت کنی
ى.	ز 10 است و نسبت به آن اول هست	ی چهار عدد مثبت وجود دارد که کمتر ا	يعنب. $\phi(10)=4$ •
	(6	(3,10)=1 بت به هم اول هستند، یعنی	🔸 عدد سه و ده نس
		$3^4 = 1 \pmod{10}$ لر-فرما داريم:	
		ىتوانيم بنويسيم كه:	🕰 آنگاه براحتی م
3.90	$(3^4)^2 = 3^{4 \times 22 + 2} = (3^4)^{22} \times (3^2) = 3^4 \times 22 + 2 = 3^4 \times 22 + 2 = 3^4 \times 22 = 3^4 \times 22$	= 9 (mod 10).	
	(0) // (0)	(1104 10).	
کدام گزینه خواهد شد؟	اه d یا همان کلید محرمانه برابر با d	مقدار 35 $n=3$ و مقدار 5 $e=5$ باشد، آن گا	۱۸. اگر در الگوریتم RSA ه
د) 6	3 (₇	ب) 5	الف) 4
ر نظر میگیریم، بهگونهای که	ارامتر e را به عنوان کلید عمومی د	ىدد پنج است. همانطور كه مىدانيد، پا	پاسخ: گزینه صحیح ع
	$1 < e < \phi(n), (e, \phi(n))$	(x)) = 1.	
) که:	ید محرمانه در نظر می گیریم، به گونهای	پارامتر d را به عنوان کل
	$ed \equiv 1 \pmod{\phi(n)}$)),	
5 در پیمانه 24 را محاسبه کنیم که برابر با $e=5$	اهد شد. سپس باید معکوس عدد	سبه می کنیم که برابر با $\phi(35)=24$ خو	
ن در پیمانه 24 را محاسبه کنیم که برابر با ز $e=5$	اهد شد. سپس باید معکوس عدد	سبه میکنیم که برابر با $\phi(35)=24$ خو	پس ابتدا $\phi(n)$ را محاد خواهد شد.

الف) انتشار - متن آشكار - متن رمز شده

ب) انتشار - متن رمز شده - متن آشکار

د) کلید محرمانه Alice

۱۹. برای این که Alice پیامی را برای Bob رمز کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد عمومي Bob ب) كليد عمومي Bob ج) كليد محرمانه

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

- ۲۰. کدام گزینه صحیح نیست؟ (میتوانید چند گزینه را انتخاب کنید).
- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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)

25 (ع 27 (ج 2 (ب 6 (الف) 2

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

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

- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با روتباط، برابر با نفر برای برقراری ارتباط، برابر با روتباط، برابر با روتباط، برابر با
 - د) هیچکدام از گزینهها صحیح نیست

پاسخ: هیچ کدام 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، 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 بالف) گمراه کنندگی - آشکار - متن رمز

ج) انتشار - آشکار - متن رمز دار کلید کلید کاید کلید دار - کلید دار

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

۲۴. برای این که Alice پیامی را برای Bob امضا کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد محرمانه Alice ب) كليد عمومي Bob ج) كليد محرمانه Bob

یاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می کند.

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

الف) هيچكدام 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 می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن

د) در PGP اول عملیات امضا انجام می شود بعد رمز کردن و بعد فشرده سازی

یاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

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

ب) یک مساله تسهیم راز است.

الف) یک مساله از نوع اثبات دانایی صفر است.

د) یک مساله از نوع روشهای غیرتعاملی است.

ج) همه گزینهها صحیح 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 a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها اگر $\mathbb{Z}_n^* = \{r_1, r_2, \dots, r_{\phi(n)}\}$ یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ 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 می بایست برابر با طول متن اصلی باشد.

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد است.

د) شکستن این رمز عملانیاز 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۳۰. اثبات کنید که اگر p=pq باشد، آن گاه (p-1)(q-1) (سوال تشریحی) پاسخ: این مورد در کلاس توضیح داده شد.

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
٣٣	14.4/.4/11	امنیت سیستمهای کامپیوتری		

۱. طول واقعی کلید DES برابر است با

94 (ع ج) 48 (ج با 48 ما با 48

پاسخ: گزینهی "۵۶" صحیح میباشد.

- ۲. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.
 - ۳. کدام گزینه در مورد PGP صحیح است؟
 - الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا
 - ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
 - ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
 - د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

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

ب) یک مساله تسهیم راز است.

الف) همه گزینهها صحیح است.

د) یک مساله از نوع اثبات دانایی صفر است.

ج) یک مساله از نوع روشهای غیرتعاملی 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 راه حل نمره ندارد.
- این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها اگر $\mathbb{Z}_n^* = \{r_1, r_2, \dots, r_{\phi(n)}\}$ 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)

10 (د) 7 (ج 34 (ب 17

پاسخ: اگر $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1, ar_2, \dots, ar_{\phi(n)}\}$ باشد. پس پاسخ اعداد 10 و 7 است.

٩. كدام گزينه صحيح نيست؟ (مي توانيد چند گزينه را انتخاب كنيد).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.

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 Vernam اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید در یک سامانه رمزگذاری، ما به صورت غیرعمد می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به صورت عمدی می خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه ها صحیح است.

پاسخ: در یک سامانه رمزگذاری، ما به صورت عمدی می خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه ها صحیح است.

الف) گمراه کنندگی - رمز - کلید

چ) انتشار - آشکار - متن رمز

پاسخ: گزینه ی "گمراه کنندگی - رمز - کلید" صحیح می باشد.

در کار تر سید الله الله الله المیت بر الله من سیار باید به می باشد.

۱۱. كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

P (ه S (ج E (ب F (الف)

یاسخ: گزینهی "S" صحیح میباشد.

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

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

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

6 (ه 27 (ب 25 (الف) 25

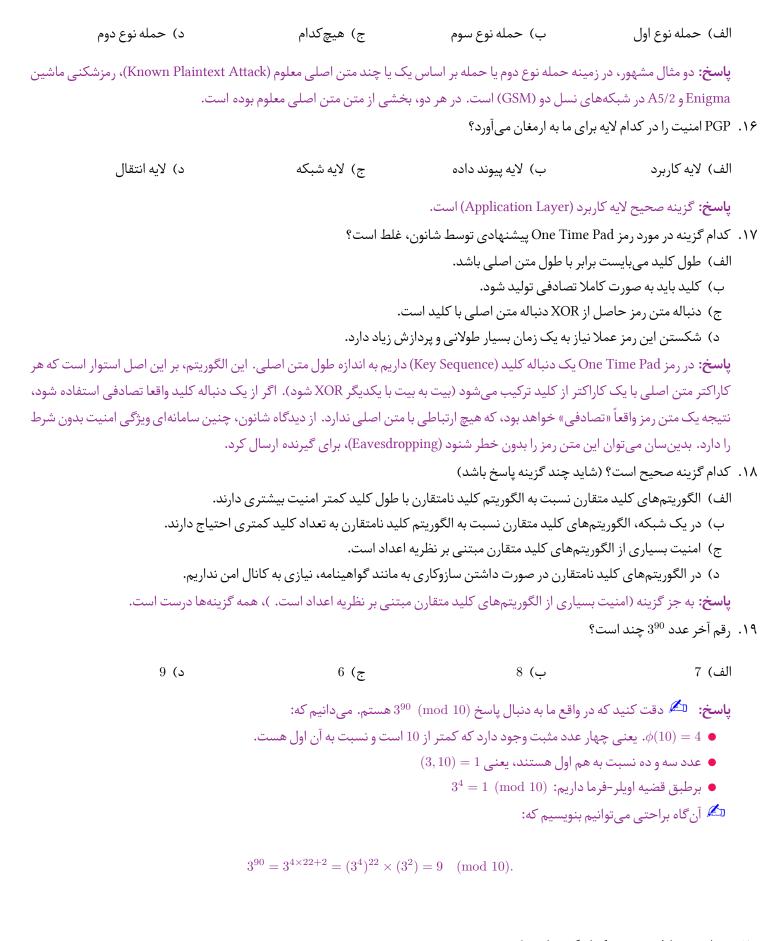
یاسخ: اثبات می شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1,2,4,p^k,2\times p^k\}$. بنابراین همه گزینههای فوق ریشه اولیه دارند.

۱۴. برای این که 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

یاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می کند.

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



۲۰. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

8 (ع ب) 2 (ب) 6 الف)

پاسخ: این عدد ریشه اولیه ندارد.

- ۲۱. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- 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.

یاسخ

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمنى دارد.
- ببله 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.
 - ٢٢. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.
- دوریک سامانه رمزگذاری، ما بهصورت غیرعمد می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 <u>بهصورت عمدی می</u>خواهیم 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 p=pq باشد، آن گاه (p-1)(q-1) ((p-1)(q-1) هد. اثبات کنید که اگر و باشد، آن گاه ((p-1)(q-1) باز گاه ((p-1)(q-1) باز
 - ۲۴. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)
 - الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با رتباط، برابر با نفر برای برقراری ارتباط، برابر با روبا تعداد کلید در الگوریتمهای نامتقارن بین n
 - 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوى ديگر، تعداد كليد براي الگوريتمهاي متقارن است نه نامتقارن

- که. 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 آشكار
 - ج) گمراه کنندگی متن رمز شده متن آشکار
 - ب) گمراه کنندگی متن آشکار متن رمز شده
 - د) انتشار متن آشکار متن رمز شده

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

۲۷. كدام شرط در مورد RSA الزامي است؟

ب) متن اصلی باید نسبت به $\phi(n)$ اول باشد. الف) کلید عمومی باید نسبت به n اول باشد. د) کلید عمومی باید نسبت به $\phi(n)$ اول باشد. ج) متن اصلی باید نسبت به n اول باشد. **پاسخ:** پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای 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؟ د) 5 ₃ (ج الف) 6 پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که $1 < e < \phi(n), \quad (e, \phi(n)) = 1.$ پارامتر d را به عنوان کلید محرمانه در نظر می گیریم، به گونهای که: $ed \equiv 1 \pmod{\phi(n)}$, پس ابتدا $\phi(n)$ را محاسبه می کنیم که برابر با $\phi(35)=24$ خواهد شد. سپس باید معکوس عدد e=5 در پیمانه $\phi(n)=24$ را محاسبه کنیم که برابر با $\phi(n)=0$ خواهد شد. ۲۹. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حملهای صورت پذیرفت؟ ب) حمله نوع دوم د) حمله نوع اول ج) حمله نوع سوم الف) هيچكدام **یاسخ:** دو مثال مشهور، در زمینه حمله نوع دوم یا حمله بر اساس یک یا چند متن اصلی معلوم (Known Plaintext Attack)، رمزشکنی ماشین

الف) کلید عمومی Bob

Enigma و A5/2 در شبکههای نسل دو (GSM) است. در هر دو، بخشی از متن متن اصلی معلوم بوده است.

۳۰. برای این که Alice پیامی را برای Bob رمز کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

ب) کلید عمومی Alice

ج) كليد محرمانه Bob

د) کلید محرمانه Alice

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
44	14.4/.1/1	امنیت سیستمهای کامپیوتری		

۱. کدام شرط در مورد RSA الزامی است؟

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

د) متن اصلی باید نسبت به n اول باشد.

الف) کلید عمومی باید نسبت به n اول باشد.

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

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

- ۲. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)
- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با روزاری ارتباط، برابر با نفر برای برقراری ارتباط، برابر با روزاری ارتباط، برابر با
 - د) هیچکدام از گزینهها صحیح نیست

پاسخ: هیچ کدام 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

- ۳. اثبات کنید که اگر p=pq باشد، آنگاه (p-1)(q-1) ((p-1)(q-1) ؛ (سوال تشریحی) پاسخ: این مورد در کلاس توضیح داده شد.
 - ۴. طول واقعی کلید DES برابر است با

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) هيچكدام 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.

- پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) پاسخ: پاسخ این سوال در اسلایدها است.
- ۷. کدام گزینه در مورد مساله غار علی بابا 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.

ياسخ: فقط اين گزينه صحيح است: يک مساله از نوع اثبات دانايي صفر است.

٨. كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).



۱۴. کدام گزینه در مورد PGP صحیح است؟

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

- الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمزکردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام میخورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

۱۵. 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: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

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 ج) 70 ج) 10 الف

پاسخ: اگر $\{r_1,r_2,\ldots,r_{\phi(n)}\}$ 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 $ar_1,ar_2,\ldots,ar_{\phi(n)}$ باشد. پس پاسخ اعداد 10 و 7 است.

١٧. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح/غلط را بنويسيد.

- الف امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه اطلاعاتی در مورد متن اصلی یی 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 <u>بهصورت عمدی</u> میخواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینهها صحیح است.

۱۸. برای این که Alice پیامی را برای Bob رمز کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد عمومي Bob ب) كليد عمومي Alice ج) كليد محرمانه Bob عمومي Bob عمومي

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

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 ج) گمراه کنندگی - متن آشکار - متن رمز شده دارمز شد دارمز شد دارمز شد دارمز شد دارمز شد دارمز شد دارمز شده دارمز شد دارمز شد دارمز ش

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

۲۰. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.

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

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

5 پس ابتدا $\phi(n)$ را محاسبه می کنیم که برابر با $\phi(35)=\phi(35)=\phi(35)=0$ خواهد شد. سپس باید معکوس عدد e=5 در پیمانه 24 را محاسبه کنیم که برابر با خواهد شد.

۲۲. برای این که Alice پیامی را برای Bob امضا کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

Alice ب) كليد محرمانه Alice ب) كليد عمومي Bob ب عمومي Bob ب) كليد عمومي الف)

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

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

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 راه حل 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 بالف) گمراه کنندگی - رمز - کلید د) انتشار - 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)

6 (ه 27 (ج 25 (الف) 25

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

PGP . ۲۷ امنیت را در کدام لایه برای ما به ارمغان می آورد؟

الف) لايه انتقال ب) لايه پيوند داده ج) لايه شبکه د) لايه 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 می بایست 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 متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانهای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

- ۲۹. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح/غلط را بنويسيد.
- 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.

ىاسخ

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمنى دارد.
- ببله 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 حمله گر 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.



شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
۳۵	14.4/.4/11	امنیت سیستمهای کامپیوتری		

١. تعداد ريشه اوليه عدد 60 كدام گزينه است؟

4 (ع ع الف) 2 (ج) 8 (ج

یاسخ: این عدد ریشه اولیه ندارد.

ج) انتشار - رمز - کلید

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

الف) گمراه کنندگی - آشکار - متن رمز بالف) گمراه کنندگی - رمز - کلید

د) انتشار - آشکار - متن رمز

یاسخ: 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 راه حل نمره ندارد.

۴. کدام شرط در مورد RSA الزامی است؟

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

الف) متن اصلی باید نسبت به n اول باشد.

د) کلید عمومی باید نسبت به n اول باشد.

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

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای 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)

25 (ع ج) 6 (ج ب) 25

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

- ۶. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى أن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 گزینه ها صحیح است.

- ٧. پروتكل توافق كليد ديفي-هلمن را توضيح دهيد؟ (سوال تشريحي) پاسخ: پاسخ اين سوال در اسلايدها است.
 - ۸. طول واقعی کلید DES برابر است با

الف) ۵۶ (ج با ۸۸ بر الف) ۵۶ الف

پاسخ: گزینهی "۵۶" صحیح میباشد.

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

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.

- 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.

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)

34 (ع ب ت ع ب 17 ج ب 17 الف) 10 الف

پاسخ: اگر $\{r_1,r_2,\ldots,r_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آن گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1,ar_2,\ldots,ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1,ar_2,\ldots,ar_{\phi(n)}\}$ باشد. پس پاسخ اعداد 10 و 7 است.

۱۱. کدام گزینه در مورد PGP صحیح است؟

- الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

۱۲. برای این که Alice پیامی را برای Bob امضا کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد محرمانه Alice ب) كليد محرمانه Bob ج) كليد عمومي Bob د) كليد عمومي

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

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

الف) هيچكدام 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؟

7 (ع ج 9 (ج ج الف)

پاسخ: 🕰 دقت کنید که در واقع ما به دنبال پاسخ (10 mod) 3^{90} هستم. میدانیم که:

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

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

10. كدام قسمت الكوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

S (د) F (ج P (ب E

پاسخ: گزینهی "S" صحیح میباشد.

PGP . ۱۶ امنیت را در کدام لایه برای ما به ارمغان می آورد؟

الف) لايه پيوند داده ب) لايه كاربرد ج) لايه انتقال د) لايه شبكه

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

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

- الف) طول كليد مى بايست برابر با طول متن اصلى 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۸. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.

- 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.

یاسخ:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمني دارد.
- ببله 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۱۹. برای این که Alice پیامی را برای Bob رمز کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد عمومي Alice ب) كليد محرمانه Abice ج) كليد محرمانه Bob د) كليد عمومي

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

- ۲۰. كدام گزينه صحيح است؟ (شايد چند گزينه 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) هيچ كدام ج) حمله نوع اول 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.

باسخ: a (سوال تشریحی) $a^{\phi(n)} = 1 \mod n$ این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: a عدد a در مجموعه کاهش یافته مانده ها اگر a عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a یعنی a 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 (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل 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.

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

ج) گمراه کنندگی - متن رمز شده - متن آشکار

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

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: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

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

ب) یک مساله تسهیم راز است.

الف) یک مساله از نوع روشهای غیرتعاملی است.

د) همه گزینهها صحیح است.

ج) یک مساله از نوع اثبات دانایی صفر است.

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

- ۲۷. اثبات کنید که اگر p=pq باشد، آنگاه (p-1)(q-1) ((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: یاسخ این سوال در اسلایدها است.
 - ۴۹. اگر در الگوریتم RSA مقدار n=35 و مقدار e=5 باشد، آن گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

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

- ۳۰. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)
- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با روزاری ارتباط، برابر با نفر برای برقراری ارتباط، برابر با روزاری ارتباط، برابر با
 - د) هیچکدام از گزینهها صحیح نیست

یاسخ: 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
٣۶	14.4/.4/11	امنیت سیستمهای کامپیوتری		

- ١. كدام گزينه صحيح است؟ (شايد چند گزينه 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 p=pq باشد، آنگاه (p-1)(q-1) ((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 راه حل نمره ندارد.
 - ۴. کدام گزینه در مورد مساله غار علی بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

ب) همه گزینهها صحیح است.

الف) یک مساله تسهیم راز است.

د) یک مساله از نوع روشهای غیرتعاملی است.

ج) یک مساله از نوع اثبات دانایی صفر 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 كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با روزاری ارتباط، برابر با نفر برای برقراری ارتباط، برابر با روزاری ارتباط، برابر با
 - 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

- 9. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.
- ۷. این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها اگر $\mathbb{Z}_n^* = \{r_1, r_2, \dots, r_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

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

٨. تعداد ريشه اوليه عدد 60 كدام گزينه است؟

پاسخ: این عدد ریشه اولیه ندارد.

۹. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا

ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن

د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

۱۰. در SSH چگونه از حمله تغییر قابلیتهای مشتری نظیر الگوریتههای 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: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

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؟

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

یارامتر d را به عنوان کلید محرمانه در نظر می گیریم، به گونهای که:

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

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

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

الف) انتشار - آشکار - متن رمز بالف) انتشار - آشکار - متن رمز جالید بالف) انتشار - رمز - کلید بالکتار بالکتار بالکتار - رمز - کلید بالکتار بالک

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

۱۳. برای این که Alice پیامی را برای Bob امضا کند، می بایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد محرمانه Alice ب) كليد محرمانه Bob ج) كليد عمومي Alice د) كليد عمومي

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

۱۴. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.

- الف امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.
- دوریک سامانه رمزگذاری، ما بهصورت غیرعمد می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 كليد مي بايست برابر با طول متن اصلى 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان 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) هيچ كدام

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.

 3^{90} رقم آخر عدد 3^{90} چند است?

8 (ه ب) 7 ج) 9 (اف)

پاسخ: 🛍 دقت کنید که در واقع ما به دنبال پاسخ (10 3^{90} هستم. میدانیم که:

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

: 25	بنويسيم	توانيم		احتـ	، ب	آن گاه	
٠.	بنويسيم	بوابيم	سی	استني	، بر	اں ت	,

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

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.

یاسخ:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمنى دارد.
- ببله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری بر مخفی ماندن کلید باشد، حتی اگر حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

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

17 (د) 70 ج) 7 الف) 10 الف)

پاسخ: اگر $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1, ar_2, \dots, ar_{\phi(n)}\}$ باشد. پس پاسخ اعداد 10 و 7 است.

· ٢. كدام قسمت الكوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

P (ه S (ج F (ب E (الف)

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)

25 (د) 6 (ج 2 (ب 27

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

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

الف) لايه شبكه ب) لايه انتقال ج) لايه كاربرد داده

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

۲۵. برای این که Alice پیامی را برای Bob رمز کند، می بایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد محرمانه Alice ب) كليد محرمانه Bob ج) كليد عمومي Alice د) كليد عمومي

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

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

ب) گمراه کنندگی - متن رمز شده - متن آشکار الف) انتشار - متن آشكار - متن رمز شده د) گمراه کنندگی - متن آشکار - متن رمز شده ج) انتشار - متن رمز شده - متن آشکار پاسخ: گزینهی "انتشار - متن آشکار - متن رمز شده" صحیح میباشد. ۲۷. کدام گزینه صحیح نیست؟ (می توانید چند گزینه را انتخاب کنید). الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچگونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.

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. حمله گر 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؟

ب) متن اصلی باید نسبت به n اول باشد.

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

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

ج) کلید عمومی باید نسبت به n اول باشد.

یاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

۲۹. طول واقعی کلید DES برابر است با

۵۶ (۵ **ک**۴ (ت الف) ۳۲ ج) ۴۸

ياسخ: گزينهي "۵۶" صحيح ميباشد.

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

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

ام و نام خانوادگی	شماره دانشجویی	نام درس	تاريخ	شماره برگه
		امنیت سیستمهای کامپیوتری	14.4/.7/11	٣٧

- ارن نسبت به الكوريتم كليد
- ب) دریک 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.

طول واقعی کلید DES برابر است با

ج) ۴۸ ۶۴ (۵ ب) ۳۲ الف) ۵۶

پاسخ: گزینهی "۵۶" صحیح میباشد.

- ۳. کدام گزینه در مورد PGP صحیح است؟
- الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

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

۴. برای این که Alice پیامی را برای Bob امضا کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

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

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

ه. این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: $a^{\phi(n)}=1 \mod n$ (سوال تشریحی) پاسخ: اگر $(r_0, r_0, \dots, r_{\phi(n)})$ مجموعه کاهش یافته مانده ها باشد، آن گاه مجموعه حاصل شده از ضرب عدد $(r_0, r_0, \dots, r_{\phi(n)})$ مجموعه کاهش یافته مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ 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 راه حل نمره ندارد.
 - ٧. كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

F (ب الف) P د) E s (ج

یاسخ: 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)

10 (د) 17 ج) 17 د) 34 الف)

پاسخ: اگر $\{r_1,r_2,\dots,r_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1,ar_2,\dots,ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1,ar_2,\dots,ar_{\phi(n)}\}$ باشد. پس پاسخ اعداد 10 و 7 است.

90 وقم آخر عدد 3^{90} چند است

پاسخ: 🕰 دقت کنید که در واقع ما به دنبال پاسخ (10 mod 10) هستم. می دانیم که:

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

🗀 آنگاه براحتی می توانیم 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 علی بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

ب) یک مساله از نوع روشهای غیرتعاملی است.

الف) همه گزینهها صحیح است.

د) یک مساله از نوع اثبات دانایی صفر است.

ج) یک مساله تسهیم راز 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 كليد مي بايست برابر با طول متن اصلى 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 متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانهای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۱۲. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل 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) هيچ كدام

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 كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با (تباط، برابر با نفر برای برقراری ارتباط، برابر با با رعداد کلید در الگوریتمهای نامتقارن بین n
 - 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، 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.

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

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

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

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

- ۱۸. کدام گزینه صحیح نیست؟ (میتوانید چند گزینه را انتخاب کنید).
- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچگونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 می شود؟ در تمام مراحل یکپارچگی پیامها حفظ می شود در تمام مراحل پیامها با کلید نامتقارن رمز می شود در مراحل انتهایی، کل پیامهای مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می شود. هیچکدام

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

• 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

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

6 (د) 25 (ج) 25 (ج) 25 (ع)

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

۲۱. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.

- الف امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.
- در یک سامانه رمزگذاری، ما بهصورت غیرعمد می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 <u>بهصورت عمدی می</u>خواهیم 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.

ب) انتشار - متن آشکار - متن رمز شده

د) گمراه کنندگی - متن آشکار - متن رمز شده

الف) انتشار - متن رمز شده - متن آشکار

ج) گمراه کنندگی - متن رمز شده - متن آشکار

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

۲۳. کدام شرط در مورد RSA الزامی است؟

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

د) متن اصلی باید نسبت به n اول باشد.

الف) کلید عمومی باید نسبت به n اول باشد.

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

یاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

۲۴. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى أن عبارت صحيح /غلط را بنويسيد.

- 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.

یاسخ:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمني دارد.
- ببله 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۲۵. برای این که 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 Bob الف

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

۲۶. اثبات کنید که اگر p=pq باشد، آن گاه (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 می آورد؟

الف) لايه كاربرد ب) لايه انتقال ج) لايه پيوند داده د) لايه شبكه

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

۲۸. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

8 (ه ج) 6 (ج ب) 4 الف) 2

یاسخ: این عدد ریشه اولیه ندارد.

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

الف) هيچكدام ب) حمله نوع سوم ج) حمله نوع اول 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.



شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
٣٨	14.47.411	امنیت سیستمهای کامپیوتری		

است؟	PGP صحيح	در مورد	گزىنە د	كدام	٠.١

الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا

- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام میخورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

۲. برای این که Alice پیامی را برای Bob رمز کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد محرمانه Alice ب) كليد عمومي Alice ج) كليد محرمانه Bob د) كليد عمومي

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

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

الف) هيچكدام 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 (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.
 - كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

E (د) P (ج F الف) F

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 می دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با (رمی ارتباط، برابر با نفر برای برقراری ارتباط، برابر با n
 - 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، 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)

پاسخ: اثبات می شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1,2,4,p^k,2 imes p^k\}$. 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 آشكار

ج) گمراه کنندگی - متن آشکار - متن رمز شده

ب) انتشار - 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 می آورد؟

ج) لايه پيوند داده داده کاربرد

ب) لايه شبكه

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

۱۱. برای این که Alice پیامی را برای Bob امضا کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

د) کلید محرمانه Alice

ج) كليد محرمانه Bob

ب) کلید عمومی Alice

الف) كليد عمومي Bob

الف) لايه انتقال

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

۱۲. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.

- 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 اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمنى دارد.
- ببله 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

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

ب) یک مساله از نوع روشهای غیرتعاملی است.

الف) یک مساله از نوع اثبات دانایی صفر است.

د) یک مساله تسهیم راز است.

ج) همه گزینهها صحیح است.

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

این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a یعنی a بیک جایگشت کامل از مجموعه اولیه است. پس داریم:

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

10. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

2 (ع ج) 4 ج) 8 الف) 8

پاسخ: این عدد ریشه اولیه ندارد.

1۶. 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 راه حل 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)

7 (د) 34 (ج) 10 (الف) 17 الف

پاسخ: اگر $\{r_1, r_2, \dots, r_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1, ar_2, \dots, ar_{\phi(n)}$ باشد. پس پاسخ اعداد 10 و 7 است.

 3^{90} چند است 3^{90} چند است

9 (د) 9 (ج) 8 (الف)

پاسخ: 🕰 دقت کنید که در واقع ما به دنبال پاسخ (10 mod 10) هستم. می دانیم که:

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

🛍 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 باکشار - 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. كدام گزينه صحيح است؟ (شايد چند گزينه 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.

یاسخ: 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. γ اول باشد.

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

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

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

الف) حمله نوع دوم ب) حمله نوع اول ج) هيچ كدام 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 كليد مى بايست برابر با طول متن اصلى باشد.
 - ب) کلید باید به صورت کاملا تصادفی تولید شود.
 - ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

- ۲۵. اثبات کنید که اگر p=pq باشد، آن گاه (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 می شود؟ در تمام مراحل یکپارچگی پیامها حفظ می شود در تمام مراحل پیامها با کلید نامتقارن رمز می شود در مراحل انتهایی، کل پیامهای مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می شود. هیچکدام

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

۲۷. طول واقعی کلید DES برابر است با

الف) ۳۲ ج) ۶۴ ج

ياسخ: گزينهي "۵۶" صحيح مي باشد.

۲۸. کدام گزینه صحیح نیست؟ (می توانید چند گزینه را انتخاب کنید).

- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 گزینه ها 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؟

 \mathbf{y} یاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر \mathbf{e} را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

یارامتر d را به عنوان کلید محرمانه در نظر می گیریم، به گونهای که:

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

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



شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
٣٩	14.4/.4/11	امنیت سیستمهای کامپیوتری		

۱. کدام شرط در مورد RSA الزامی است؟

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

الف) متن اصلی باید نسبت به n اول باشد.

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

ج) کلید عمومی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می eیریم، به eونهای که

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

كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

F (ب

E (ه S (ج

الف) P

یاسخ: گزینهی "S" صحیح میباشد.

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

ب) گمراه کنندگی - رمز - کلید

الف) انتشار - آشكار - متن رمز

د) انتشار - رمز - کلید

ج) گمراه کنندگی - آشکار - متن رمز

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

۴. برای این که Alice پیامی را برای Bob امضا کند، می بایست آن را با رمز کند و برای Bob ارسال کند.

د) کلید محرمانه Bob

ج) کلید عمومی Bob

ب) کلید محرمانه Alice

الف) كليد عمومي Alice

یاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می کند.

- ۵. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه اطلاعاتی در مورد متن اصلی یی 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 <u>بهصورت عمدی می</u>خواهیم 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 علی بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

4 (د	ج) 6	ب) 5	الف) 3
در نظر می گیریم، به گونهای که	پارامتر e را به عنوان کلید عمومی د	۰ پنج است. همان طور که می دانید،	پاسخ: گزینه صحیح عد
	$1 < e < \phi(n), (e, \phi(n))$) = 1.	
	ى كە:	د محرمانه در نظر می گیریم، به گونها:	پارامتر d را به عنوان کلی
	$ed \equiv 1 \pmod{\phi(n)}$),	
5 در پیمانه 24 را محاسبه کنیم که برابر با و $e=5$	واهد شد. سپس باید معکوس عدد	به می کنیم که برابر با $\phi(35)=24$ خ	پس ابتدا $\phi(n)$ را محاس خواهد شد.
	وم و نسبت به حمله نوع سوم کاملا	صحیح است و کدام غلط؟ لطفا جلوی Ver نسبت به حمله نوع اول و دوم مقا ی جزئیات سامانه رمزگذاری آگاهی د	num الف سامانه •
برطبق این اصل، امنیت یک الگوریتم رمزگذاری رمزگذاری و رمزگشایی داشته باشد.	شانون از اصل Kerckhoffs است.	ملا غلط است. Vernum فقط نسبت و صحیح است. در واقع این جمله بیان و فی ماندن کلید باشد، حتی اگر حمله	• الف اين جمله كاه • ب بله اين جمله <i>-</i>
رو حجم وسیعی از پراکنده است.	ن معنا است ساختاری آماری	مانه قوی ویژ <i>گی</i> را دارد که به ای	۹. طبق گفته شانون یک س
ز شده - متن آشکار کار - متن رمز شده	ب) انتشار - متن رم د) انتشار - متن آش	متن رمز شده - متن آشکار متن آشکار - متن رمز شده	
ر باشد؟ (ممكن است چند گزينه صحيح باشد)		- متن آشکار - متن رمز شده" صحیح در کدام عدد ضرب کنیم تا مجموعه ج	
د) 34	ج) 17	ب) 7	الف) 10
ىل شده از ضرب عدد a در مجموعه كاهش يافته a باشد. پس پاسخ اعداد a 0 و a 7 است.		یک جایگشت کامل ا $\{ar_1, ar_2, \dots,$	
۳۲ (۵	ج) ۶۴	ب) ۵۶	الف) ۴۸
ِسال کند.	را با رمز کند و برای Bob ار ۲۳۰	حیح میباشد. برا برای Bob رمز کند، میبایست آن	پاسخ: گزینهی ۵۶″ ص ۱. برای این که Alice پیامی

الف) یک مساله تسهیم راز است.

ج) یک مساله از نوع اثبات دانایی صفر 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، آن گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

ب) یک مساله از نوع روشهای غیرتعاملی است.

د) همه گزینهها صحیح است.

الف) كليد عمومي Bob ب) كليد محرمانه Alice ج) كليد محرمانه Bob الف) كليد عمومي

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

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

الف) لايه كاربرد ب) لايه انتقال ج) لايه پيوند داده د) لايه شبكه

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

۱۴. رقم آخر عدد 3^{90} چند است؟

7 (د) 8 (ج) 9 (الف) 9

پاسخ: 🕰 دقت کنید که در واقع ما به دنبال پاسخ (10 3^{90} هستم. میدانیم که:

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

🔼 آن گاه 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 می بایست 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 متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانهای ویژگی امنیت بدون شرط را دارد. بدین سان می توان 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 می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

١٧. كدام گزينه صحيح است؟ (شايد چند مورد صحيح باشد)

- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با روتباط، برابر با نفر برای برقراری ارتباط، برابر با روتباط، برابر با روتباط، برابر با
 - 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها اگر a عدد a در مجموعه کاهش یافته مانده ها اگر a عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a یعنی a 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 راه حل نمره ندارد.
 - ۲۰. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حملهای صورت پذیرفت؟

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؟

یاسخ: این عدد ریشه اولیه ندارد.

- ک۲۲. 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 می شود؟ در تمام مراحل یکپارچگی پیامها حفظ می شود در تمام مراحل پیامها با کلید نامتقارن رمز می شود در مراحل انتهایی، کل پیامهای مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می شود. هیچکدام

یاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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. كدام گزينه صحيح است؟ (شايد چند گزينه پاسخ باشد)
 - الف) الگوریتمهای کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.
- ب) دریک 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)

2 (د) 25 (ج) 25 (ف)

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

- ۲۸. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.
 - ۲۹. اثبات کنید که اگر p=pq باشد، آن گاه (p-1)(q-1) ((p-1)(q-1) باشد، آن گاه (p-1)(q-1) باشد، آن گاه روز در کلاس توضیح داده شد.
 - ۳۰. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حملهای صورت پذیرفت؟

الف) حمله نوع دوم ب) هيچ كدام 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.



شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
4.	14.4/.4/11	امنیت سیستمهای کامپیوتری		

كدام قسمت الگوریتم DES باعث غیر خطی شدن سامانه می شود (به طور دقیق).

E (ج P (ب S (۵ الف) F

یاسخ: 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 می شود در تمام مراحل پیامها با کلید نامتقارن رمز می شود در مراحل انتهایی، کل پیامهای مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می شود. هیچ کدام

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

- ٣. كدام گزينه صحيح نيست؟ (مي توانيد چند گزينه را انتخاب كنيد).
- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچگونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه اطلاعاتی در مورد متن اصلی پی ببرد.

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

- ۴. كدام گزينه صحيح است؟ (شايد چند مورد صحيح باشد)
- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت مے ،کنند.
 - (م) تعداد کلید در الگوریتمهای نامتقارن بین n نفر برای برقراری ارتباط، برابر با (م) تعداد کلید در الگوریتمهای نامتقارن بین n
 - د) هیچکدام از گزینهها صحیح نیست

یاسخ: 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

۵. کدام گزینه در مورد مساله غار علی بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد) 8

ب) یک مساله از نوع اثبات دانایی صفر است.		الف) همه گزینهها صحیح است.	
روشهای غیرتعاملی است.	د) یک مساله از نوع	Ü.	ج) یک مساله تسهیم راز است
	صفر است.	ست: یک مساله از نوع اثبات دانایی ه	پاسخ: فقط این گزینه صحیح ا
ِسال کند.	رمز کند و برای Bob ار	ی Bob امضا کند، میبایست آن را با	۶. برای این که Alice پیامی را برای
Alice د) کلید محرمانه	ج) کلید عمومی 30b	ب) كليد محرمانه Bob	الف) كليد عمومي Alice
	ه و برای Bob ارسال می کند	را با کلید خصوصی خودش رمز کرد $\it m$	n برای امضا، پیام Alice پاسخ:
		است؟	۷. کدام شرط در مورد RSA الزامی
نسبت به $\phi(n)$ اول باشد.	ب) کلید عمومی باید	به n اول باشد.	الف) کلید عمومی باید نسبت ب
سبت به $\phi(n)$ اول باشد.	د) متن اصلی باید نی	اول باشد. n	ج) متن اصلی باید نسبت به
) که	د عمومی در نظر می گیریم، به گونهای	پاسخ: پارامتر e را به عنوان کلید
	$1 < e < \phi(n), (e$	$e, \phi(n)) = 1.$	
	صورت بذبرفت؟	بط Turing، توسط چه نوع حملهای ه	۸. رمزشکنی ماشین Enigma توس
د) حمله نوع اول	ج) حمله نوع سوم	ب) حمله نوع دوم	الف) هیچکدام
Known Plaintext Attacl)، رمزشکنی ماشین			
		نسل دو (GSM) است. در هر دو، بخر	
ندام تزینه خواهد شد؛	همان کلید محرمانه برابر با	و مقدار $e=5$ باشد، آن گاه d یا $n=$	۱۰. آگر در الحوریتم KSA مقدار 35
د) 3	ج) 4	6 (ب	الف) 5
ر نظر می گیریم، به گونهای که	را به عنوان کلید عمومی در e	ست. همانطور که میدانید، پارامتر	پاسخ: گزینه صحیح عدد پنج ا
	$1 < e < \phi(n), (e$	$e, \phi(n)) = 1.$	
		انه در نظر می گیریم، به گونهای که:	پارامتر d را به عنوان کلید محرم
	$ed \equiv 1 \pmod{8}$	$d \phi(n)$,	
5 در پیمانه 24 را محاسبه کنیم که برابر با و $e=5$	د. سپس باید معکوس عدد	نیم که برابر با $\phi(35)=24$ خواهد ش	پس ابتدا $\phi(n)$ را محاسبه می ک
		One Tim پیشنهادی توسط شانون، غ	خواهد شد. ۱۰ کداه گذینه در مورد روز pe Pad

ب) کلید باید به صورت کاملا تصادفی تولید شود.

ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد است.

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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان 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.

PGP .۱۲ امنیت را در کدام لایه برای ما به ارمغان می آورد؟

الف) لايه كاربرد ب) لايه شبكه ج) لايه انتقال داده

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

- ١٣. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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. كدام گزينه صحيح است؟ (شايد چند گزينه پاسخ باشد)

- الف) الگوریتمهای کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.
- ب) دریک 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 \mathbb{Z}_{17}^* (ممکن است چند گزینه صحیح باشد)

7 (د) 10 (ج) 11 (الف) 17

پاسخ: اگر $\{r_1, r_2, \dots, r_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1, ar_2, \dots, ar_{\phi(n)}$ 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) هيچ كدام 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.

 3^{90} وقم آخر عدد 3^{90} چند است?

6 (ع ج) 7 ج الف) 9

پاسخ: 🕰 دقت کنید که در واقع ما به دنبال پاسخ (10 mod 10) هستم. می دانیم که:

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

🔼 آنگاه براحتی میتوانیم بنویسیم که:

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

این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها اگر a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a یعنی a 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

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 می شود بعد فشرده سازی و بعد امضا
 - ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
 - ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
 - د) در PGP اول عملیات امضا انجام می شود بعد رمز کردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام میخورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

۲۲. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.

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

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

۲۴. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

2 (ع ع الف) 6 الف) 6 جا

پاسخ: این عدد ریشه اولیه ندارد.

۲۵. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى أن عبارت صحيح /غلط را بنويسيد.

- 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 اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمنى دارد.
- ببله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری بر مخفی ماندن کلید باشد، حتی اگر حمله گر 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 - متن آشکار جاندگی - متن آشکار - متن رمز شده - متن آشکار - متن رمز شده جا) گمراه کنندگی - متن آشکار - متن رمز شده

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

۲۷. اثبات کنید که اگر p=pq باشد، آن گاه (p-1)(q-1) ((p-1)(q-1) هدر کلاس توضیح داده شد.

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

Alice کلید محرمانه Bob ج) کلید محرمانه Bob بالک کلید عمومی Bob ج) کلید محرمانه ها Bob برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می کند.

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

27 (ه 25 (ج 2 (ب 6 (الف)

پاسخ: اثبات می شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1,2,4,p^k,2 imes p^k\}$. 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 راه حل نمره ندارد.

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
41	14.47.411	امنیت سیستمهای کامپیوتری		

- ۱. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.
 - ٢. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
 - 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.
- ببله 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.
 - ۳. PGP امنیت را در کدام لایه برای ما به ارمغان می آورد؟

الف) لايه انتقال ب) لايه پيوند داده ج) لايه كاربرد د) لايه شبكه

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

- 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، آن گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 6 (ح) لا عند الف 6 (عند الف) 5 (عند الف) 5 (عند الف) 8 (عند الف) 8 (عند الف) 9 (عند ا

 \mathbf{y} سخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

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

- ۶. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.

- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه اطلاعاتی در مورد متن اصلی یی 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 <u>بهصورت عمدی می</u>خواهیم 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 كليد مي بايست برابر با طول متن اصلى باشد.
 - ب) کلید باید به صورت کاملا تصادفی تولید شود.
 - ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان 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: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

- 9. 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 راه حل نمره ندارد.
 - ۱۰. کدام گزینه در مورد مساله غار علی بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

ب) یک مساله از نوع روشهای غیرتعاملی است.

الف) یک مساله تسهیم راز است.

د) یک مساله از نوع اثبات دانایی صفر است.

ج) همه گزینهها صحیح است.

یاسخ: 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.

ل الگوریتمهای متقارن است نه نامتقارن	از سوی دیگر، تعداد کلید برای		
ند.	رمز کند و برای Bob ارسال ک	Bob امضا کند، میبایست آن را با	۱۳. برای این که Alice پیامی را برای
د) کلید محرمانه Bob	ج) كليد محرمانه Alice	ب) کلید عمومی Bob	الف) كليد عمومي Alice
	گرده و برای Bob ارسال می کند.	را با کلید خصوصی خودش رمز ک $\it r$	پاسخ: Alice برای امضا، پیام <i>n</i>
سوال تشریحی) پاسخ $a^{\phi(n)}=1 \mod$			
عدد a در مجموعه کاهش یافته مانده ه	، آنگاه مجموعه حاصل شده از ضرب	مجموع كاهشيافته ماندهها باشد.	$\mathbb{Z}_n^* = \{r_1, r_2, \dots, r_{\phi(n)}\}$ اگر
	به است. پس داریم:	بک جایگشت کامل از مجموعه اولی	یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ ی
$\prod_{i=1}^{\phi(n)} (ar_i \mod n)$	$= \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right) \left(\prod_{i=1}^{\phi(n)} r_i\right)$	$= \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1$	\pmod{n}
	(به طور دقیق).	ث غیر خطی شدن سامانه میشود	۱۵. كدام قسمت الگوريتم DES باعد
E (s	ج) S	F (ب	الف) P
		اشد.	پاسخ: گزینهی "S" صحیح می
ر توضیح دهید؟ (سوال تشریحی) پاسخ	د تولید کلید عمومی و خصوصی را نیز		
			پاسخ این سوال در اسلایدها اس
		_ح است؟	۱۷. کدام گزینه در مورد PGP صحیح
	ی و بعد امضا	گاری انجام میشود بعد فشردهساز	الف) در PGP اول عملیات رمزناً
		دهسازی انجام میشود بعد رمزنگار	
		ا انجام می شود بعد فشرده سازی و	
		ا انجام می شود بعد رمزکردن و بعد	
ند فشردهسازی و بعد عملیات رمز <i>گ</i> ذاری	مای دیجیتال بر روی پیام میخورد، بع	بز مطرح شد، در PGP اول یک امض	پاسخ: همانطور که در کلاس ن
		ئزينه است؟	۱۸. تعداد ریشه اولیه عدد 60 کدام گ
2 (ა	4 (ج	6 (ب	الف) 8
		د.	پاسخ: این عدد ریشه اولیه نداره
(ممكن است چند گزينه صحيح باشد)	ک جایگشت از مجموعه اصلی باشد؟	عدد ضرب کنیم تا مجموعه جدید یک	۱۹. اعضای مجموعه \mathbb{Z}_{17}^* را در کدام :
	747		

۱۲. كدام گزينه صحيح است؟ (شايد چند مورد صحيح باشد)

د) هیچکدام از گزینهها صحیح نیست

الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.

• تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می دهد.

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

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

• توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

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

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

ج) متن اصلی باید نسبت به n اول باشد.

یاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

 3^{90} رقم آخر عدد 3^{90} چند است?

ج) 7 د) 8 6 (ب الف) 9

پاسخ: 🕰 دقت کنید که در واقع ما به دنبال پاسخ (10 3^{90} هستم. میدانیم که:

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

(3,10) = 1 عدد سه و ده نسبت به هم اول هستند، یعنی •

 $3^4=1\pmod{10}$ برطبق قضیه اویلر-فرما داریم: •

🛍 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.

ب) گمراه کنندگی - آشکار - متن رمز الف) انتشار - آشكار - متن رمز د) انتشار - رمز - کلید ج) گمراه کنندگی - رمز - کلید **ياسخ:** گزينهي "گمراه كنندگي - رمز - كليد" صحيح ميباشد. ۲۷. طول واقعی کلید DES برابر است با د) ۶۴ ج) ۳۲ ے) ۵۶ الف) ۴۸ **ياسخ:** گزينهي "۵۶" صحيح مي باشد.

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

ج) 6 د) 27 2 (ب الف) 25

 $m{y}$ پاسخ: اثبات می شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1,2,4,p^k,2 imes p^k\}$. بنابراین همه گزینههای فوق ریشه اولیه دارند.

۲۹. کدام گزینه صحیح نیست؟ (می توانید چند گزینه را انتخاب کنید).

- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچگونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچگونه اطلاعاتی در مورد متن اصلی یی 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؟

د) حمله نوع دوم ج) هيچكدام ب) حمله نوع اول الف) 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.

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
47	14.4/.4/11	امنیت سیستمهای کامپیوتری		

رمزشكنى ماشين Enigma توسط Turing، توسط چه نوع حملهاى صورت پذيرفت؟

الف) حمله نوع سوم ب) حمله نوع دوم ج) حمله نوع اول د) هيچ كدام

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 ب) گمراه کنندگی - رمز - کلید د) گمراه کنندگی - رمز - کلید

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

۳. 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: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمتگزار آن را با کلید عمومی خودش امضا می کند.

- ۴. کدام گزینه در مورد PGP صحیح است؟
- الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

یاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

- ۵. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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.
 - <mark>و</mark> 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 گزینه ها صحیح است.

- کدام گزینه صحیح نیست؟ (میتوانید چند گزینه را انتخاب کنید).
- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.

پاسخ: در یک سامانه رمزگذاری، ما به صورت عمدی می خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه ها صحیح است.

- ۷. اثبات کنید که اگر p=pq باشد، آنگاه (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) هيچ كدام 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.

9. كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

E (ع E (ج E (ج P الف)

پاسخ: گزینهی "S" صحیح میباشد.

۱۰. طول واقعی کلید DES برابر است با

الف) ۴۸ (ب ۳۲ ج) ۶۴ (د

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 راه حل نمره ندارد.
 - ۱۲. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟
 - الف) طول كليد مى بايست برابر با طول متن اصلى 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 عملانیاز 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

الف) یک مساله تسهیم راز است. ب) یک مساله از نوع روشهای غیرتعاملی است. د) یک مساله از نوع اثبات دانایی صفر است. ج) همه گزینهها صحیح است. پاسخ: فقط این گزینه صحیح است: یک مساله از نوع اثبات دانایی صفر است. ١٥. كدام گزينه صحيح است؟ (شايد چند گزينه 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 كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد. ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند. $\binom{n}{2}$ برابر با (تباط، برابر با رقراری ارتباط، برابر با با تعداد کلید در الگوریتمهای نامتقارن بین n نفر برای برقراری ارتباط، برابر با د) هیچکدام از گزینهها صحیح نیست یاسخ: 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 می دهد. • توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند. از سوی دیگر، 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. ب) انتشار - متن رمز شده - متن آشکار الف) گمراه کنندگی - متن آشکار - متن رمز شده د) انتشار - متن آشکار - متن رمز شده ج) گمراه کنندگی - متن رمز شده - متن آشکار **یاسخ:** گزینهی "انتشار - متن آشکار - متن رمز شده" صحیح می باشد. ۱۸. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد. ۱۹. برای این که Alice پیامی را برای Bob رمز کند، می بایست آن را با رمز کند و برای Bob ارسال کند. د) کلید عمومی Alice ج) كليد محرمانه Bob ب) کلید عمومی Bob الف) كليد محرمانه Alice پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می کند. ۲۰. اگر در الگوریتم RSA مقدار n=35 و مقدار e=5 باشد، آن گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟ ج) 5 د) 6 4 (ب الف) 3 پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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 علی بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

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

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

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

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

(سوال تشریحی) پاسخ: $a^{\phi(n)} = 1 \mod n$ این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ در مجموعه کاهش یافته مانده ها اگر $a^{\phi(n)} = a$ عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $a^{\phi(n)} = a$ 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؟

پاسخ: این عدد ریشه اولیه ندارد.

۲۳. برای این که Alice پیامی را برای Bob امضا کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد محرمانه Alice ب) كليد عمومي Bob ج) كليد محرمانه Bob

یاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می کند.

- ۲۴. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- 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.
- بب 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

 3^{90} حدد است؟ رقم آخر عدد 3^{90} چند است

7 (د) 8 (ج) 8 (الف) 6

پاسخ: 🛍 دقت کنید که در واقع ما به دنبال پاسخ (10 3^{90} هستم. میدانیم که:

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

🛍 آنگاه براحتی میتوانیم بنویسیم که:

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

انیز توضیح دهید؟ (سوال تشریحی) پاسخ:	وند تولید کلید عمومی و خصوصی را		
			پاسخ این سوال در اسلایدها PGP .۲۷
		رای ما به ارمعان می اورد:	۱۱۷ املیک را در ندام دیه ج
د) لايه انتقال	ج) لايه كاربرد	ب) لايه شبكه	الف) لايه پيوند داده
		برد (Application Layer) است.	پاسخ: گزینه صحیح لایه کار
		می است؟	۲۸. کدام شرط در مورد RSA الزا
بت به $\phi(n)$ اول باشد.	ب) کلید عمومی باید نس	به n اول باشد.	الف) متن اصلى بايد نسبت
بت به n اول باشد.	د) کلید عمومی باید نس		ج) متن اصلی باید نسبت
	های که	کلید عمومی در نظر م <i>ی گیر</i> یم، به <i>گ</i> ون	پاسخ: پارامتر <i>e</i> را به عنوان ک
	$1 < e < \phi(n), (e, \phi)$	(n)) = 1.	
	کن است چند گزینه صحیح باشد)	ولیه (Primitive Root) دارند؟ (ممک	۲۹. کدام یک از اعداد زیر ریشه ا
6 (s	2 (_Z	ب) 25	الف) 27
همه گزینههای فوق ریشه اولیه دارند.	د. $\{1,2,4,p^k,2 imes p^k\}$. بنابراین ه	ط اعداد این مجموعه ریشه اولیه دارن	پاسخ: اثبات میشود که فقص
د؟ (ممكن است چند گزينه صحيح باشد)			
34 (د	10 (ح	ب) 7	الف) 17
ده از ضرب عدد a در مجموعه کاهش یافته	هها باشد، آنگاه مجموعه حاصل ش	مجموع کاهشیافته ماند $\mathbb{Z}_n^* = \{r_1$	$\{r,r_2,\ldots,r_{\phi(n)}\}$ پاسخ: اگر
		یک جایگشت کامل از مع $\{ar_1, ar_2,$	

گە	شماره برگ	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
	۴٣	14.4/.4/11	امنیت سیستمهای کامپیوتری		

۱. برای این که Alice پیامی را برای Bob رمز کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

د) کلید محرمانه Bob

ج) كليد محرمانه Alice

ب) کلید عمومی Bob

الف) كليد عمومي Alice

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

- ۲. کدام گزینه صحیح نیست؟ (می توانید چند گزینه را انتخاب کنید).
- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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، آن گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

4 (ه 5 (ج 6 (ب 3 الف)

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

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

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

الف) حمله نوع دوم ب) هيچ كدام ج) 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 اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمني 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

تعداد ریشه اولیه عدد 60 کدام گزینه است؟

پاسخ: این عدد ریشه اولیه ندارد.

- ۷. كدام گزينه صحيح است؟ (شايد چند مورد صحيح باشد)
- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با رتباط، برابر با نفر برای برقراری ارتباط، برابر با روبا تعداد کلید در الگوریتمهای نامتقارن بین n
 - 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

۸. برای این که Alice پیامی را برای Bob امضا کند، می بایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد عمومي Alice ب) كليد عمومي Bob ج) كليد محرمانه Bob

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

9. این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها اگر $\mathbb{Z}_n^* = \{r_1, r_2, \dots, r_{\phi(n)}\}$ 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 می شود بعد فشرده سازی و بعد امضا

- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

۱۱. کدام گزینه در مورد مساله غار علی بابا 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.

ب) یک مسانه از نوع روسهای غیرتعاملی 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 می بایست 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 می شود (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. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

- ۱۳. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.
- ۱۴. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۸ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.
 - ۱۵. اعضای مجموعه $_{17}^*\mathbb{Z}$ را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

7 (ه 34 (ب 10 (ف) 17

پاسخ: اگر $\{r_1,r_2,\dots,r_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1,ar_2,\dots,ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1,ar_2,\dots,ar_{\phi(n)}$ 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 با انتشار - متن رمز شده - متن آشکار

ج) گمراه کنندگی - متن رمز شده - متن آشکار دمن 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 با نتشار - 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) هيچ كدام 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. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه اطلاعاتی در مورد متن اصلی یی 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 <u>بهصورت عمدی می</u>خواهیم 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؟

8 (د) 8 (ج) 7 (الف) 7

یاسخ: هم در واقع ما به دنبال پاسخ (10 mod 10) هستم. می دانیم که:

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

🖒 آنگاه براحتی می توانیم 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)

یاسخ: اثبات می شود 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

٣٢ (٥ ج) ۶۴ ج سرم (۵۶ با ۲۸ الف)

ياسخ: گزينهي "۵۶" صحيح مي باشد.

۲۵. اثبات کنید که اگر p=pq باشد، آن گاه (p-1)(q-1) ((p-1)(q-1) وسوال تشریحی) پاسخ: این مورد در کلاس توضیح داده شد.

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

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

۲۷. کدام شرط در مورد RSA الزامی است؟

ب) متن اصلی باید نسبت به n اول باشد.

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

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

ج) کلید عمومی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

- ۲۸. كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).
- S (د) F (ج E (ب P الف)

پاسخ: گزینهی "S" صحیح میباشد.

- ٢٩. كدام گزينه صحيح است؟ (شايد چند گزينه پاسخ باشد)
- الف) الگوریتمهای کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.
- ب) دریک 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.

یاسخ: 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 می آورد؟

د) لايه شبكه

ج) لايه انتقال

ب) لايه كاربرد

الف) لايه پيوند داده

ياسخ: گزينه صحيح لايه كاربرد (Application Layer) است.

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
44	14.4/.4/11	امنیت سیستمهای کامپیوتری		

 3^{90} چند است? الم آخر عدد 3^{90}

9 (ه ج) 7 (ج 8 (ب 6 الف)

پاسخ: 🖾 دقت کنید که در واقع ما به دنبال پاسخ (10 3^{90} هستم. میدانیم که:

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

🗀 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؟

 $6 \ (چ \ 5 \ (ب)$ 3 (ع

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

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

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

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

- ٣. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.
- دریک سامانه رمزگذاری، ما بهصورت غیرعمد میخواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 گزینه ها صحیح است.

- ۴. كدام گزينه صحيح است؟ (شايد چند گزينه 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 این که Alice پیامی را برای Bob رمز کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد عمومي Alice ب) كليد محرمانه Alice ج) كليد عمومي Alice

پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob مند.

- ۶. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟
 - الف) طول کلید می بایست 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۷. طول واقعی کلید DES برابر است با

الف) ۳۲ (ج) ۶۴ (ج) ۳۲ (لف)

پاسخ: گزینهی "۵۶" صحیح میباشد.

- ٨. كدام گزينه صحيح نيست؟ (ميتوانيد چند گزينه را انتخاب كنيد).
- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 این که Alice پیامی را برای Bob امضا کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد عمومي Alice ب) كليد عمومي Bob ج) كليد محرمانه Bob

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

- 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 علی بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

د) حمله نوع اول	ج) ھيچکدام	ب) حمله نوع دوم	الف) حمله نوع سوم
Known Plaintext At)، رمزشکنی ماشی	یک یا چند متن اصلی معلوم (tack	مینه حمله نوع دوم یا حمله بر اساس	پاسخ: دو مثال مشهور، در ز
ده است.	بخشی از متن متن اصلی معلوم بو	ای نسل دو (GSM) است. در هر دو،	Enigma و A5/2 در شبکهها
عجم وسیعی از پراکنده است.	عنا است ساختاری آماری رو ح	، قوی ویژ <i>گی</i> را دارد که به این م ه	۱۴. طبق گفته شانون یک سامانه
ن رمز شده - متن آشکار	ب) گمراه کنند <i>گی</i> - متر	متن رمز شده	الف) انتشار - متن آشکار - ،
_ه آشکار - متن رمز شده	د) گمراه کنندگی - متر·	- متن آشکار	ج) انتشار - متن رمز شده
	باشد.	ن آشکار - متن رمز شده" صحیح می	پاسخ: گزینهی "انتشار - مت
اب آخر ملاک است، هر کس پاسخ درست) پاسخ: برابر با ۸ میشود. جو		
			نوشته باشد قابل قبول است
		رای ما به ارمغان میاورد؟	PGP .1۶ امنیت را در کدام لایه ب
د) لايه انتقال	ج) لايه پيوند داده	ب) لايه كاربرد	الف) لايه شبكه
		برد (Application Layer) است.	پاسخ: گزینه صحیح لایه کار
وگیری میشود؟ در تمام مراحل یکپارچگ	_ا های رمزنگاری مورد پشتیبانی جل	بر قابلیتهای مشتری نظیر الگوریتم	۱۷. در SSH چگونه از حمله تغیب
مای مبادله شده به صورت امضا شده از سر _ا	ی شود در مراحل انتهایی، کل پیامه	مراحل پیامها با کلید نامتقارن رمز م	پیامها حفظ میشود در تمام
		ل مىشود. ھيچكدام	خدمتگزار برای مشتری ارسا
ا درست می کند:	ورودیهای زیر مقدار چکیده پیام ر	نابع استفاده می کند، و با استفاده از	پاسخ: خدمت گزار از همان ا
• Client Identification Id: SSH-2.0	-libssh_0.9.3		
• Server Identification Id: SSH-2.0	-OpenSSH_8.2p1 Ubuntu-4uh	ountu0.5	
• 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			
آن را با کلید عمومی خودش امضا می کند	این چکیده تولید شد، خدمتگزار	بعد از این که	
	د(به طور دقیق).	باعث غیر خطی شدن سامانه میشوه	۱۸. كدام قسمت الگوريتم DES
P (3	Е (ج	F (ب	الف) S
		ىياشد.	پاسخ: گزینهی "S" صحیح ه
	ن است چند گزینه صحیح باشد) ۲۶۱	ولیه (Primitive Root) دارند؟ (ممک	۱۹. کدام یک از اعداد زیر ریشه ا

ب) یک مساله از نوع روشهای غیرتعاملی است.

د) همه گزینهها صحیح است.

الف) یک مساله تسهیم راز است.

ج) یک مساله از نوع اثبات دانایی صفر است.

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

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

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

25 (ع 6 (ج 27 (ب 2 الف) 2

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

- ۲۰. اثبات کنید که اگر p=pq باشد، آن گاه (p-1)(q-1) ((p-1)(q-1) هد. اثبات کنید که اگر (p-1)(q-1) باشد، آن گاه ((p-1)(q-1) باشد، آن گاه ((p-1)(q-1)
 - ۲۱. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
 - 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 اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمنى دارد.
- ببله 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 حمله گر 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 بالف) گمراه کنندگی آشکار متن رمز بالنشار رمز کلید بالنشار رمز رمز
 - 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) هيچ كدام 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 می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشردهسازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

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

- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - ${n \choose 2}$ برابر با رتباط، برابر با نفر برای برقراری ارتباط، برابر با جو اتعداد کلید در الگوریتم های نامتقارن بین n
 - 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

۲۶. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.

رسوال تشریحی) پاسخ: a این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a یعنی a بایگشت 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؟

ب) متن اصلی باید نسبت به n اول باشد.

 $\frac{1}{2} \frac{1}{2} \frac{1}$

الف) کلید عمومی باید نسبت به n اول باشد. σ کلید عمومی باید نسبت به σ اول باشد.

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

یاسخ: یارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

۲۹. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

4 (۵ ج) 6 (ج ع) 8 الف)

یاسخ: 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)

34 (ع ب ا 10 ج ع ب 17 الف) 7

پاسخ: اگر $\{a,n\}$ عدد a در مجموعه کاهش یافته مانده ها باشد، آن گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1,ar_2,\ldots,ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر a باشد. پس یاسخ اعداد 10 و 7 است.

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
40	14.4/.4/1	امنیت سیستمهای کامپیوتری		

- ۱. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟
 - الف) طول كليد مي بايست برابر با طول متن اصلى باشد.
 - ب) کلید باید به صورت کاملا تصادفی تولید شود.
 - ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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 متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانهای ویژگی امنیت بدون شرط را دارد. بدین سان می توان 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؟

5 (د) 5 (ج) 4 (ب) 3 الف) 3

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

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

۳. این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: a سوال تشریحی) **پاسخ:** a این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها اگر a یعنی a عدی a عدی 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. كدام گزينه صحيح است؟ (شايد چند مورد صحيح باشد)
- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - (م) تعداد کلید در الگوریتمهای نامتقارن بین n نفر برای برقراری ارتباط، برابر با (م) تعداد کلید در الگوریتمهای نامتقارن بین n
 - 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 می دهد.

• توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتم های متقارن است نه نامتقارن

در می توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده

سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.

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 یا است.

د) در یک سامانه بدون شرط امن شناخته شده، سامانه عنده می نوین به متن اصلی اضافه کنیم. حمله گرد، صورت مشاهده متن به من ناید

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. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- 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.

ياسخ:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمنى 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.
 - ۷. طول واقعی کلید DES برابر است با

الف) ۶۴ (ج سر) ۳۲ ج) ۴۸

ياسخ: گزينهي "۵۶" صحيح ميباشد.

۸. برای این که 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

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

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 بانتشار - متن آشکار - متن رمز شده

ج) انتشار - متن رمز شده - 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 این که Alice پیامی را برای Bob امضا کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد عمومي Alice ب) كليد محرمانه Alice ج) كليد عمومي Bob

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

۱۲. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.

- الف امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.

 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.

 در یک سامانه رمزگذاری، ما به صورت غیرعمد می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 \mathbb{Z}_{17}^* (ممکن است چند گزینه صحیح باشد)

17 (ح ج الف) 7 الف 7 را 34 (ح ج الف ع الف

پاسخ: اگر $\{r_1,r_2,\dots,r_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آن گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1,ar_2,\dots,ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1,ar_2,\dots,ar_{\phi(n)}$ 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 باکتار - رمز - کلید باکتار - متن رمز باکتار - مت

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

١۵. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

4 (ع ع الف) 8 (ج ع الف) 6 (الف)

پاسخ: این عدد ریشه اولیه ندارد.

16. كدام قسمت الكوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

E (ه F (ج S (ب P الف)

پاسخ: گزینهی "S" صحیح میباشد.

۱۷. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا

- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمز کردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام میخورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

۱۸. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.

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

ب) یک مساله تسهیم راز است. الف) یک مساله از نوع اثبات دانایی صفر است. د) همه گزینهها صحیح است. ج) یک مساله از نوع روشهای غیرتعاملی 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 راه حل نمره ندارد. ٢١. كدام گزينه صحيح است؟ (شايد چند گزينه 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. **یاسخ:** 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. 3^{90} عدد است? رقم آخر عدد د) 8 الف) 6 ج) 9 ب) 7 پاسخ: 🕰 دقت کنید که در واقع ما به دنبال پاسخ (10 3^{90} هستم. میدانیم که: • بعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست. $\phi(10) = 4$ (3,10) = 1 عدد سه و ده نسبت به هم اول هستند، یعنی • $3^4 = 1 \pmod{10}$ برطبق قضیه اویلر-فرما داریم: •

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

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

2 (د) 27 (ج) 25 (ب) 6 (الف)

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

۲۵. PGP امنیت را در کدام لایه برای ما به ارمغان می آورد؟

🕰 آن گاه براحتی می توانیم بنویسیم که:

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: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

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

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

یاسخ: 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؟

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

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

یاسخ: یارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

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

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

یاسخ: 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 p=pq باشد، آن گاه (p-1)(q-1) ((p-1)(q-1) وسوال تشریحی) پاسخ: این مورد در کلاس توضیح داده شد.

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
45	14.4/.4/11	امنیت سیستمهای کامپیوتری		

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

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

- 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؟

یاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

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

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

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

- ۴. کدام گزینه صحیح نیست؟ (میتوانید چند گزینه را انتخاب کنید).
- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حملهگر در صورت مشاهده متن رمز، نباید به هیچگونه اطلاعاتی در مورد متن اصلی یی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به صورت عمدی می خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه ها صحیح است.

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

6 (ء 25 (ج 25 (ح 25 الف) 27 (ع 25 (ح 25 (- 25 (+))))))))))))))))

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

- ۶. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- 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.

یاسخ:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمنى دارد.
- ببله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری بر مخفی ماندن کلید باشد، حتی اگر حمله گر 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 با کیار - متن رمز

ج) گمراه کنندگی - رمز - کلید دار مین رمز علید دار کلید دار مین رمز دار مین رمز دار کلید دار مین رمز دار کلید دا

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

۸. PGP امنیت را در کدام لایه برای ما به ارمغان می آورد؟

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

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

ج) انتشار - متن آشکار - متن رمز شده

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

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

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

- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مىدهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با روتباط، برابر با تعداد کلید در الگوریتمهای نامتقارن بین n نفر برای برقراری ارتباط، برابر با
 - 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 می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

۱۱. كدام قسمت الكوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

S (ه P (ج F (ب E الف)

ياسخ: گزينهي "S" صحيح ميباشد.

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)

پاسخ: اگر $\{r_1,r_2,\dots,r_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1,ar_2,\dots,ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر a الشد. پس پاسخ اعداد 10 و 7 است.

١٣. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى أن عبارت صحيح /غلط را بنويسيد.

- الف امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.
- <mark>د</mark> 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 گزینه ها صحیح است.

۱۴. كدام گزينه صحيح است؟ (شايد چند گزينه 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 علی بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

ب) یک مساله از نوع روشهای غیرتعاملی است.

الف) همه گزینهها صحیح است.

د) یک مساله تسهیم راز است.

ج) یک مساله از نوع اثبات دانایی صفر 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) هيچ كدام

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 راه حل نمره ندارد.

۱۸. برای این که Alice پیامی را برای Bob رمز کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد محرمانه Bob ب) كليد عمومي Bob ج) كليد محرمانه Bob د) كليد عمومي

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

 3^{90} وقم آخر عدد 3^{90} چند است

پاسخ: 🕰 دقت کنید که در واقع ما به دنبال پاسخ (10 mod 10) هستم. می دانیم که:

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

🔼 آن گاه 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 می شود بعد فشرده سازی و بعد امضا

- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام میخورد، بعد فشرده سازی 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) هيچ كدام 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 p=pq باشد، آن گاه (p-1)(q-1)=(p-1) ؟ (سوال تشریحی) پاسخ: این مورد در کلاس توضیح داده شد.

۲۳. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

8 (ه 2 (ب 6 (الف) 6

یاسخ: این عدد ریشه اولیه ندارد.

.۲۴. این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a در a در مجموعه کاهش یافته مانده ها باشد، آنگاه 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 (ج) ۳۲ (ج) ۴۸ (الف

یاسخ: گزینهی "۵۶" صحیح می باشد.

۲۶. كدام شرط در مورد RSA الزامي است؟

ب) کلید عمومی باید نسبت به n اول باشد.

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

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

ج) متن اصلی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای 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 كليد مي بايست برابر با طول متن اصلى باشد.
 - ب) کلید باید به صورت کاملا تصادفی تولید شود.
 - ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۲۸. برای این که Alice پیامی را برای Bob امضا کند، می بایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد محرمانه Bob ب) كليد عمومي Alice ب) كليد عمومي Alice الف

یاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می کند.

- 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 (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
41	14.4/.4/11	امنیت سیستمهای کامپیوتری		

- 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: μ یاسخ این سوال در اسلایدها است.
 - ٣. كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

S (هE (جP (ب

پاسخ: گزینهی "S" صحیح میباشد.

- ۴. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.
 - ۵. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.
- دوریک سامانه رمزگذاری، ما بهصورت غیرعمد می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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.

- کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)
- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با روتباط، برابر با نفر برای برقراری ارتباط، برابر با روتباط، برابر با روتباط، برابر با
 - 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

۷. کدام گزینه در مورد PGP صحیح است؟

- الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمز کردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

الف) حمله نوع سوم	ب) حمله نوع اول	ج) هیچکدام	ام	د) حمله نوع دوم
پاسخ: دو مثال مشهور، در زمین	حمله نوع دوم یا حمله بر اسار	ں یک یا چند متن اصلی معل	intext Attack) معلوم	Known Pla)، رمزشکنی ماشین
مر شرکه و A5/2 م Enigma	سا ده (GSM) است. در ه. د	برخش ادمتن متن اصل	با معلمه بمده است.	

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

ب) همه گزینهها صحیح است.

الف) یک مساله از نوع روشهای غیرتعاملی است.

د) یک مساله تسهیم راز است.

ج) یک مساله از نوع اثبات دانایی صفر 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 صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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.

١١. تعداد ريشه اوليه عدد 60 كدام گزينه است؟

4 (ه ک الف) 2 ج الف) 2 جا

پاسخ: این عدد ریشه اولیه ندارد.

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

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

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

ب) گمراه کنندگی - آشکار - متن رمز

الف) انتشار - آشكار - متن رمز

د) انتشار - رمز - کلید

ج) گمراه کنندگی - رمز - کلید

ياسخ: گزينهي "گمراه کنندگي - رمز - کليد" صحيح مي باشد.

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

د) 6	ج) 27	ب) 25	2 (الف
	د. $\{1,2,4,p^k,2 imes p^k\}$. بنابراین همه گ $1,2,4,p^k$ ارسال کند و برای Bob ارسال کند		
د) کلید محرمانه Alice	ج) کلید عمومی Alice	ب) کلید عمومی Bob	الف) كليد محرمانه Bob
نه خواهد شد؟	کرده و برای Bob ارسال می کند. ۵ یا همان کلید محرمانه برابر با کدام گزیا	م m را با کلید خصوصی خودش رمز $n=35$ و مقدار $e=5$ باشد، آنگاه n	
د) 5	ج) 6	ب) 3	الف) 4

 \mathbf{y} سخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

یارامتر d را به عنوان کلید محرمانه در نظر می گیریم، به گونهای که:

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

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

۱۷. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.

- 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.

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمني 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.
- ۱۸. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) **یاسخ:** برابر با ۸ میشود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.
 - PGP . ۱۹ امنیت را در کدام لایه برای ما به ارمغان می آورد؟

الف) لابه شبكه د) لايه پيوند داده ج) لايه كاربرد ب) لايه انتقال

ياسخ: گزينه صحيح لايه كاربرد (Application Layer) است.

 3^{90} وقم آخر عدد 3^{90} چند است?

د) 9 ج) 7 6 (<u></u> الف) 8

پاسخ: 🛍 دقت کنید که در واقع ما به دنبال پاسخ (10 3^{90} هستم. می دانیم که:

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

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

🔼 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) هيچكدام 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 كليد مي بايست برابر با طول متن اصلى 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

- ٢٣. كدام گزينه صحيح است؟ (شايد چند گزينه 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 p=pq باشد، آن گاه (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 بانتشار - متن آشکار - متن رمز شده

ج) انتشار - متن رمز شده - متن آشکار در شده - متن آشکار - متن رمز شده

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

رسوال تشریحی) پاسخ: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: اگر دو عدد a (سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a یعنی a یک جایگشت کامل از مجموعه اولیه است. پس داریم:

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

7 (ه	34 (-	ب) 17	الف) 10
. پس پاسخ اعداد 10 و 7 است.	موعه اولیه است، اگر $(a,n)=1$ باشد	مجموع کاهشیافته مانده ه $\mathbb{Z}_n^* = \{r_1, r_2 \}$ مجموع کاهشیافته مانده و $\{ar_1, ar_2, \dots \}$ را برای Bob رمز کند، میبایست آن را با .	$,ar_{\phi(n)}\}$ ماندهها یعنی
د) کلید محرمانه Bob	ج) کلید عمومی Alice	ب) كليد محرمانه Alice	الف) كليد عمومي Bob
	ِده و برای او ارسال م <i>ی کند</i> .	دن، پیام m را با کلید عمومی Bob رمز کررابر است با	پاسخ: Alice برای رمزکر ۲۹. طول واقعی کلید DES ب
۵۶ (۵	ج) ۶۴	۴۸ (ب	الف) ۳۲
			پاسخ: گزینهی ۵۶″ صه ۳۵۸ میرد RSA
به $\phi(n)$ اول باشد.	ب) کلید عمومی باید نسبت	بت به n اول باشد.	الف) متن اصلى بايد نس
به n اول باشد.	د) کلید عمومی باید نسبت	بت به $\phi(n)$ اول باشد.	ج) متن اصلی باید نس
	ای که	ان کلید عمومی در نظر می گیریم، به گونه	پاسخ: پارامتر e را به عنو
	$1 < e < \phi(n), (e,$	$\phi(n)) = 1.$	

 * ۲۷. اعضای مجموعه * را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد * (ممکن است چند گزینه صحیح باشد)

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
47	14.4/.4/11	امنیت سیستمهای کامپیوتری		

است؟	صحيح	PGP	مورد	در	گزینه	كدام	٠.	١
------	------	------------	------	----	-------	------	----	---

الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا

- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور 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 علی بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

ب) یک مساله از نوع روشهای غیرتعاملی است.

الف) یک مساله از نوع اثبات دانایی صفر است.

ج) یک مساله تسهیم راز است.

د) همه گزینهها صحیح است.

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

7. این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: $a^{\phi(n)}=1 \mod n$ (سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها اگر $\mathbb{Z}_n^*=\{r_1,r_2,\ldots,r_{\phi(n)}\}$ 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. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- 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.

ياسخ:

- الف این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- ببله 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.

۵. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

2 (ء (ج 8 (ب 4 الف)

پاسخ: این عدد ریشه اولیه ندارد.

باشد، آن گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؛ e=5 باشد، آن گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؛

6 (ه 3 (ب 5 الف) 5

 $oldsymbol{\psi}$ پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

5 پس ابتدا $\phi(n)$ را محاسبه می کنیم که برابر با $\phi(35)=\phi(35)=\phi(35)$ خواهد شد. سپس باید معکوس عدد e=5 در پیمانه $\phi(n)$ را محاسبه کنیم که برابر با 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 بانتشار - رمز - کلید د) انتشار - آشکار - متن رمز بانتشار - رمز - کلید

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)

10 (د) 17 (ج) 34 (ب) 7 (الف) 7

پاسخ: اگر $\{r_1, r_2, \dots, r_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1, ar_2, \dots, ar_{\phi(n)}$ باشد. پس پاسخ اعداد 10 و 7 است.

طول واقعی کلید DES برابر است با

الف) ۳۲ (ب کا ۲۸ ج) ۶۴ (۵

پاسخ: گزینهی "۵۶" صحیح میباشد.

- ۱۰. کدام گزینه صحیح نیست؟ (میتوانید چند گزینه را انتخاب کنید).
- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 الگوریتههای 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: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

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 راه حل نمره ندارد.

١٣. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.

- الف امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.
- در یک سامانه رمزگذاری، ما بهصورت غیرعمد می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 <u>بهصورت عمدی می</u>خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینهها صحیح است.

 3^{90} وقم آخر عدد 3^{90} چند است?

الف) 6 ج) 9 ج) 9 طف) 6

پاسخ: 🕰 دقت کنید که در واقع ما به دنبال پاسخ (mod 10) 3^{90} هستم. میدانیم که:

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

🔼 آنگاه براحتی می توانیم 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 كليد مي بايست برابر با طول متن اصلى باشد.
 - ب) کلید باید به صورت کاملا تصادفی تولید شود.
- ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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،

بن سامانه ای ویژگی امنیت بدون شرط	ین اصلی ندارد. از دیدگاه شانون، چنی	ئی» خواهد بود، که هیچ ارتباطی با مت	نتیجه یک متن رمز واقعاً «تصادف
	Eavesdı)، برای گیرنده ارسال کرد.	لتن رمز را بدون خطر شنود (ropping	را دارد. بدینسان میتوان این ه
		، چند گزینه پاسخ باشد)	۱۶. كدام گزينه صحيح است؟ (شايد
	طول کلید کمتر امنیت بیشتری دارند.	ل نسبت به الگوريتم كليد نامتقارن با م	الف) الگوريتمهاي كليد متقارن
	بد نامتقارن به تعداد کلید کمتری احت		
		مهای کلید متقارن مبتنی بر نظریه اع	
داريم.	مانند گواهینامه، نیازی به کانال امن ن	قارن در صورت داشتن سازوکاری به ه	د) در الگوریتمهای کلید نامت
هها درست است.	نی بر نظریه اعداد است.)، همه گزین	اری از الگوریتمهای کلید متقارن مبت	پاسخ: به جز گزینه (امنیت بسی
	، طور دقیق).	ث غیر خطی شدن سامانه میشود(به	۱۷. كدام قسمت الگوريتم DES باع
S (2	P (ج	F (ب	الف) E
		باشد.	پاسخ: گزینهی "S" صحیح می
ست.	باسخ: پاسخ این سوال در اسلایدها ا	ر ا توضیح دهید؟ (سوال تشریحی) ب	۱۸. پروتکل توافق کلید دیفی-هلمن
	سورت پذیرفت؟	ط Turing، توسط چه نوع حملهای <i>م</i>	۱۹. رمزشکنی ماشین Enigma توس
د) حمله نوع دوم	ج) حمله نوع اول	ب) هیچکدام	الف) حمله نوع سوم
Known Plainte)، رمزشکنی ماشین	یا چند متن اصلی معلوم (xt Attack	ه حمله نوع دوم یا حمله بر اساس یک	یاسخ: دو مثال مشهور، در زمین
	شی از متن متن اصلی معلوم بوده اس		
ِ کس پاسخ درستی نوشته باشد قابل			
			قبول است و راه حل نمره ندارد.
	رمز کند و برای Bob ارسال کند.		
د) كليد محرمانه Alice	ج) كليد محرمانه Bob	ب) کلید عمومی Bob	الف) كليد عمومي Alice
	ه و برای Bob ارسال می کند.	را با کلید خصوصی خودش رمز کرد n	پاسخ: Alice برای امضا، پیام <i>n</i>
		است؟	۲۲. کدام شرط در مورد RSA الزامی
اول باشد. n	ب) کلید عمومی باید نسبت به	ه $\phi(n)$ اول باشد،	الف) کلید عمومی باید نسبت ب
	n د) متن اصلی باید نسبت به n		ج) متن اصلی باید نسبت به (
. 67			_
	که	. عمومی در نظر م <i>ی گ</i> یریم، به <i>گ</i> ونهای	پاسخ: پارامتر e را به عنوان کلید
	$1 < e < \phi(n), ($	$(e,\phi(n)) = 1.$	
	رمز کند و برای Bob ارسال کند.	، Bob رمز کند، میبایست آن را با	۲۳. برای این که Alice پیامی را برای
د) کلید محرمانه Bob	ج) کلید محرمانه Alice	ب) کلید عمومی Bob	الف) كليد عمومي Alice

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 می دهد.

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

ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند. $\binom{n}{2}$ برابر با روتباط، برابر با نفر برای برقراری ارتباط، برابر با روتباط، برابر با روتباط، برابر با د) هیچکدام از گزینهها صحیح نیست پاسخ: هیچ کدام 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 می دهد. • توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند. از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

۲۵. اثبات کنید که اگر p=pq باشد، آنگاه (p-1)(q-1) = (p-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)

2 (د ج) 25 6 (ب الف) 27

پاسخ: اثبات می شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1,2,4,p^k,2 imes p^k\}$. 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: یاسخ این سوال در اسلایدها است.

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

د) لايه شبكه ج) لايه انتقال ب) لايه پيوند داده الف) لايه كاربرد

ياسخ: گزينه صحيح لايه كاربرد (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.

ب) انتشار - متن آشکار - متن رمز شده الف) 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.

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

د) حمله نوع دوم ج) هيچكدام ب) حمله نوع سوم الف) 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.

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
49	14.4/.1/1	امنیت سیستمهای کامپیوتری		

- ۱. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.
- ۲. این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ 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)

10 (د) 7 (ج) 34 (ب) 17

پاسخ: اگر $\{ar_1, ar_2, \dots, r_{\phi(n)}\}$ عدد $ar_n = \{r_1, r_2, \dots, r_{\phi(n)}\}$ باشد، آن گاه مجموعه حاصل شده از ضرب عدد $ar_n = \{r_1, r_2, \dots, r_{\phi(n)}\}$ مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_n = \{r_1, r_2, \dots, ar_{\phi(n)}\}$ باشد. پس پاسخ اعداد 10 و 7 است.

ب رقم آخر عدد 3^{90} چند است؟ *

پاسخ: 🛍 دقت کنید که در واقع ما به دنبال پاسخ (10 $100 \mod 10)$ هستم. میدانیم که:

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

🛍 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 كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با (رتباط، برابر با نفر برای برقراری ارتباط، برابر با (رتباط، برابر با ایم تعداد کلید در الگوریتم های نامتقارن بین n
 - د) هیچکدام از گزینهها صحیح نیست

پاسخ: هیچ کدام 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، 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.
 - ٧. كدام قسمت الكوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

E (ه F (ج P (ب S

پاسخ: گزینهی "S" صحیح میباشد.

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

25 (ع 27 \rightarrow 6 (الف) 25

پاسخ: اثبات می شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1,2,4,p^k,2 imes p^k\}$. 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 راه حل نمره ندارد.
 - ۱۰. کدام گزینه در مورد مساله غار علی بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

ب) یک مساله از نوع روشهای غیرتعاملی است.

الف) یک مساله تسهیم راز است.

د) یک مساله از نوع اثبات دانایی صفر است.

ج) همه گزینهها صحیح است.

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

- ۱۱. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 مشتری نظیر الگوریتمهای رمزنگاری مورد پشتیبانی جلوگیری می شود؟ در تمام مراحل یکپارچگی پیامها حفظ می شود در تمام مراحل پیامها با کلید نامتقارن رمز می شود در مراحل انتهایی، کل پیامهای مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می شود. هیچکدام

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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

د) کلید محرمانه Bob

بعد از این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

2 (د) 8 (ج) 8 (ب) 8 (ف) 8 (د) 2 (د) 8 (د) 8 (د) 9 (د)

پاسخ: این عدد ریشه اولیه ندارد.

۱۴. کدام گزینه در مورد PGP صحیح است؟

الف) انتشار - آشكار - متن رمز

- الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمزکردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

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

ب) انتشار - رمز - کلید

ج) گمراه کنندگی - رمز - کلید دار متن رمز 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 با انتشار - متن رمز شده - متن آشکار

ج) گمراه کنندگی - متن رمز شده - متن آشکار دمن آشکار - متن رمز شده

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

۱۷. طول واقعی کلید DES برابر است با

الف) ۴۸ (ح (ح (ک الف) ۴۸ (ک الف) ۵۶ (ک الف) ۵۶ (ک الف) ۱۹۵ (ک ا

پاسخ: گزینهی "۵۶" صحیح میباشد.

الف) كليد عمومي Alice

۱۸. کدام گزینه صحیح نیست؟ (می توانید چند گزینه را انتخاب کنید).

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.

- 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.

ج) کلید عمومی Bob

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

۱۹. برای این که Alice پیامی را برای Bob رمز کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

ب) كليد محرمانه Alice

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

۲۰. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟ الف) طول كليد مي بايست برابر با طول متن اصلى باشد. ب) کلید باید به صورت کاملا تصادفی تولید شود. ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد. ۲۱. برای این که Alice پیامی را برای Bob امضا کند، می بایست آن را با رمز کند و برای Bob ارسال کند. د) کلید عمومی Alice ب) کلید عمومی Bob ج) كليد محرمانه Alice الف) كليد محرمانه Bob یاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می کند. ۲۲. PGP امنیت را در کدام لایه برای ما به ارمغان می آورد؟ ج) لايه پيوند داده الف) لايه انتقال د) لايه شبكه ب) لايه كاربرد پاسخ: گزینه صحیح لایه کاربرد (Application Layer) است. ۲۳. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حملهای صورت پذیرفت؟ الف) حمله نوع اول د) حمله نوع سوم ج) حمله نوع دوم ب) 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. ۲۴. اگر در الگوریتم RSA مقدار n=35 و مقدار e=5 باشد، آن گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟ د) 3 ج) 4 و (ب الف) 5 پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که $1 < e < \phi(n), \quad (e, \phi(n)) = 1.$ پارامتر d را به عنوان کلید محرمانه در نظر می گیریم، به گونهای که:

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

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

۲۵. اثبات کنید که اگر pq باشد، آنگاه (p-1)(q-1) ((p-1)(q-1) ؛ (سوال تشریحی) پاسخ: این مورد در کلاس توضیح داده شد.

۲۶. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.

- 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.

•	

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمني دارد.
- ببله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری بر مخفی ماندن کلید باشد، حتی اگر حمله گر 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.

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

۲۹. كدام شرط در مورد RSA الزامي است؟

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

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

د) متن اصلی باید نسبت به n اول باشد.

ج) کلید عمومی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

- . ٣٠. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حملهای صورت پذیرفت؟
- الف) حمله نوع دوم ب) حمله نوع سوم ج) هيچ کدام 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.

شماره دانشجویی	نام درس	تاریخ	ا شماره برگ
	امنیت سیستمهای کامپیوتری	14.4/.4/11	۵٠
	امىيت سىستمھاى كامپيونرى	11 *1 / * 1 / 1 1	
		امنیت سیستمهای کامپیوتری	امنیت سیستمهای کامپیوتری ۱۴۰۳/۰۲/۱۱

- الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

یاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشردهسازی و بعد عملیات رمزگذاری.

- ۲. مقدار $\phi(80)$ را محاسبه کنید؟ (سوال تشریحی) **یاسخ:** برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.
 - ۳. كدام يك از اعداد زير ريشه اوليه (Primitive Root) دارند؟ (ممكن است چند گزينه صحيح باشد)

د) 6 ج) 25 27 (ت الف) 2

یاسخ: اثبات می شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1,2,4,p^k,2 imes p^k\}$. بنابراین همه گزینههای فوق ریشه اولیه دارند.

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

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

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)

ت) 10 د) 17 34 (ج الف) 7

یاسخ: اگر $\{r_1, r_2, \dots, r_{\phi(n)}\}$ مجموع کاهشیافته ماندهها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ باشد.

- کدام گزینه صحیح نیست؟ (می توانید چند گزینه را انتخاب کنید).
- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- ب) امنیت محاسباتی (Computational Security) یعنی در صورتی که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد.

		ىباشد.	پاسخ: گزینهی "۵۶" صحیح مے	
	رمز کند و برای Bob ارسال کند	، Bob امضا کند، میبایست آن را با	۱. برای این که Alice پیامی را برای	٨
د) کلید عمومی Bob	ج) کلید عمومی Alice	ب) كليد محرمانه Alice	الف) كليد محرمانه Bob	
	ه و برای Bob ارسال م <i>ی ک</i> ند.	را با کلید خصوصی خودش رمز کرد n	پاسخ: Alice برای امضا، پیام <i>n</i>	
نىد)	ح است؟ (این مورد امروز درس داده ش	لیبابا که در کلاس مطرح شد، صحیح	'. کدام گزینه در مورد مساله غار ع	1
ایی صفر است.	ب) یک مساله از نوع اثبات دانا		الف) یک مساله تسهیم راز است	
، غیرتعاملی است.	د) یک مساله از نوع روشهای	. (ج) همه گزینهها صحیح است	
		ست: یک مساله از نوع اثبات دانایی ص		
ِ کلاس توضیح داده شد.) برای کاه $\phi(n)=(p-1)(q-1)$ و برای کاه $\phi(n)=(p-1)(q-1)$		
	صورت پدیرفت؟	ط Turing، توسط چه نوع حملهای <i>م</i>	ٔ . رمزشکنی ماشین Enigma توس	١.
د) حمله نوع سوم	ج) حمله نوع دوم	ب) هیچکدام	الف) حمله نوع اول	
Known Plainte!)، رمزشکنی ماشین ت.		ه حمله نوع دوم یا حمله بر اساس یک نسل دو (GSM) است. در هر دو، بخنا		
		ئزينه اس <i>ت</i> ؟	ٔ. تعداد ریشه اولیه عدد 60 کدام گ	١,
د) 6	2 (ج	4 (ب	الف) 8	
		د.	پاسخ: این عدد ریشه اولیه ندار	
ضیح دهید؟ (سوال تشریحی) پاسخ:	ولید کلید عمومی و خصوصی را نیز تو		m روند امضای یک پیام به مانند $$	١١
سیعی از پراکنده است.	ست ساختاری آماری رو حجم و	ی ویژگی را دارد که به این معنا ا		١,
شده - متن آشکار	ب) گمراه کنندگی - متن رمز نا	ئار - متن رمز شده	الف) گمراه کنندگی - متن آشک	
رمز شده	د) انتشار - متن آشکار - متن	ىتن آشكار	ج) انتشار - متن رمز شده - ه	
		شکار - متن رمز شده" صحیح میباش 		
ست.		را توضیح دهید؟ (سوال تشریحی) ب		
	رمز کند و برای ۵۵b ارسال کند.	, Bob رمز کند، میبایست آن را با	ٔ . برای این نه Alice پیامی را برای	١,

د) در یک سامانه رمزگذاری، ما بهصورت غیرعمد میخواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید

ج) ۳۲

د) ۴۸

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

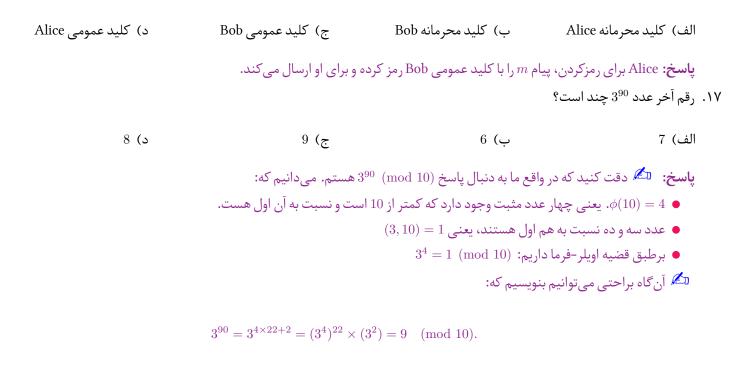
ج) تنها سامانه بدون شرط امن شناخته شده، سامانه Vernam یا One Time Pad است.

ب) ۵۶

به هیچ گونه اطلاعاتی در مورد متن اصلی پی ببرد.

۷. طول واقعی کلید DES برابر است با

الف) ۶۴



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

الف) حمله نوع اول ب) حمله نوع سوم ج) هيچ کدام 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.

١٩. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.

- 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.

ياسخ:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمني دارد.
- ببله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری بر مخفی ماندن کلید باشد، حتی اگر حمله گر 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. $\phi(n)$ اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای 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 می بایست برابر با طول متن اصلی باشد.

- ب) کلید باید به صورت کاملا تصادفی تولید شود.
- ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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 متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانهای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۲۲. PGP امنیت را در کدام لایه برای ما به ارمغان می آورد؟

الف) لايه پيوند داده ب) لايه شبكه ج) لايه كاربرد د

ياسخ: گزينه صحيح لايه كاربرد (Application Layer) است.

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

الف) انتشار - رمز - کلید با نتشار - آشکار - متن رمز با کنندگی - رمز - کلید با گمراه کنندگی - رمز - کلید با 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، آن گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

6 (د) 3 (ج) 5 (ب) 4 (الف)

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

5 پس ابتدا $\phi(n)$ را محاسبه می کنیم که برابر با $\phi(35)=24$ خواهد شد. سپس باید معکوس عدد e=5 در پیمانه $\phi(n)=24$ را محاسبه کنیم که برابر با 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 راه حل نمره ندارد.
 - ۲۶. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)
 - الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با (تباط، برابر با رقراری ارتباط، برابر با با تعداد کلید در الگوریتمهای نامتقارن بین n نفر برای برقراری ارتباط، برابر با
 - 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوى ديگر، تعداد كليد براي الگوريتمهاي متقارن است نه نامتقارن

- ٢٧. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- **الف** امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 گزینه ها صحیح است.

.۲۸. این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a یعنی a در مجموعه کامل از مجموعه اولیه است. پس داریم:

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

٢٩. كدام گزينه صحيح است؟ (شايد چند گزينه 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.

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

٣٠. كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

P (د) $S(\tau)$ $F(\tau)$ E(t)

ياسخ: گزينهي "S" صحيح ميباشد.



اره برگه	شم	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
۵۱		14.4/.1/1	امنیت سیستمهای کامپیوتری		

۱. كدام گزينه صحيح است؟ (شايد چند مورد صحيح باشد)

- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با (تباط، برابر با نفر برای برقراری ارتباط، برابر با با رعداد کلید در الگوریتمهای نامتقارن بین n
 - 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

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

ب) یک مساله از نوع روشهای غیرتعاملی است.

الف) همه گزینهها صحیح است.

د) یک مساله تسهیم راز است.

ج) یک مساله از نوع اثبات دانایی صفر است.

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

۳. كدام يك از اعداد زير ريشه اوليه (Primitive Root) دارند؟ (ممكن است چند گزينه صحيح باشد)

2 (د) 25 (ج) 25 (طف)

یاسخ: اثبات می شود 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. كدام گزينه صحيح است؟ (شايد چند گزينه 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. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.
- ۔ دریک سامانه رمزگذاری، ما بهصورت غیرعمد می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 <u>بهصورت عمدی می</u>خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینهها صحیح است.

PGP امنیت را در کدام لایه برای ما به ارمغان می آورد؟

الف) لايه پيوند داده ب) لايه كاربرد ج) لايه شبكه د) لايه 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 كليد مي بايست برابر با طول متن اصلى باشد.
 - ب) کلید باید به صورت کاملا تصادفی تولید شود.
- ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

۸. برای این که Alice پیامی را برای Bob رمز کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد محرمانه Bob ب) كليد عمومي Alice ج) كليد عمومي Bob عند عمومي الف

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

۹. كدام شرط در مورد RSA الزامي است؟

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

الف) کلید عمومی باید نسبت به n اول باشد.

د) متن اصلی باید نسبت به n اول باشد.

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

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

۱۰. اثبات کنید که اگر p=pq باشد، آن گاه (p-1)(q-1) ((p-1)(q-1) هد. اثبات کنید که اگر و باشد، آن گاه ((p-1)(q-1) باز گاه ((p-

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

ب) گمراه کنند*گی* - آشکار - متن رمز

الف) گمراه کنندگی - رمز - کلید

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 این که Alice پیامی را برای Bob امضا کند، می بایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد عمومي Bob ب) كليد محرمانه Bob ج) كليد عمومي Bob د) كليد محرمانه

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

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

الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.

- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 راه حل نمره ندارد.
 - ۱۶. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى أن عبارت صحيح /غلط را بنويسيد.
 - 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.

یاسخ:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمني دارد.
- ب بله این جمله صحیح است. در واقع این جمله بیان شانون از اصل Kerckhoffs است. برطبق این اصل، امنیت یک الگوریتم رمزگذاری بر مخفی ماندن کلید باشد، حتی اگر حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.
- ۱۷. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.
- .۱۸. این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a یعنی a بعنی a بعنی a بعنی 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: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

3 (الف	4 (ب	ج) 5	6 (s
پاسخ: گزینه صحیح عدد پنج است.	همان طور که می دانید، پارامتر e را بد	ه عنوان کلید عمومی در نظر می گیر	ریم، بهگونهای که
	$(e,\phi(n))=1.$	$1 < e < \phi(n),$	
پارامتر d را به عنوان کلید محرمانه در	ِ نظر می گیریم، به گونهای که:		

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

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

۲۱. طول واقعی کلید DES برابر است با

الف) ۵۶ (ج) ۴۸ (ب ۵۶

پاسخ: گزینهی "۵۶" صحیح میباشد.

۲۲. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا

ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا

ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن

د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

یاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

S (۵

۲۳. كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مىشود(به طور دقيق).

ياسخ: گزينهي "S" صحيح ميباشد.

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 بالف) انتشار - متن رمز شده الف) انتشار - متن رمز شده بالف) انتشار - متن رمز شده

ج) گمراه کنندگی - متن رمز شده - متن آشکار دمن آشکار - متن آشکار - متن رمز شده

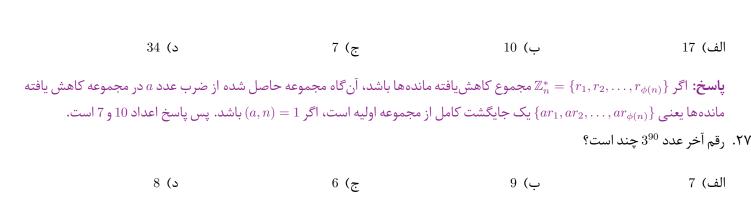
پاسخ: گزینهی "انتشار - متن آشکار - متن رمز شده" صحیح میباشد.

۲۵. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

6 (ه ج ع الف) 2 الف) 2

یاسخ: 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)



یاسخ: (mod 10) دقت کنید که در واقع ما به دنبال یاسخ (mod 10) 3⁹⁰ هستم. می دانیم که:

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

🗀 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) هيچكدام ب) حمله نوع سوم ج) حمله نوع اول 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.

- 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) هيچكدام 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.



شماره برگه	تاريخ	نام درس امنیت سیستمهای کامپیوتری	شماره دانشجویی	نام و نام خانوادگی
۵۲	14.4/.4/11	امنیت سیستمهای کامپیوتری		
تصادفی استفاده شود،	ال کند. د) کلید این الگوریتم، بر این ا زیک دنباله کلید واقعا	ا با رمز کند و برای Bob ارس ج) کلید عمومی Bob ز کرده و برای Bob ارسال می کند. بن، غلط است؟ ست. ازش زیاد دارد. ۱) داریم به اندازه طول متن اصلی. بیت با یکدیگر XOR شود). اگر از	امضا کند، می بایست آن ر ب) کلید محرمانه Alice با کلید خصوصی خودش رم One پیشنهادی توسط شانو طول متن اصلی باشد. دفی تولید شود. لا دنباله متن اصلی با کلید ار یک زمان بسیار طولانی و پرد دنباله کلید (Sey Sequence	بروتکل توافق کلید دیفی-هلمن را نادی میلید دیفی-هلمن را نادی میلید دیفی-هلمن را نادی میلید عمومی Alice پیامی را برای الف) کلید عمومی Alice پیام شراه پیام شرای امضا، پیام شراه کدام گزینه در مورد رمز Time Pad کلید میبایست برابر با میلید باید به صورت کاملا تصاه بی کلید باید به صورت کاملا تصاه بی کلید باید به صورت کاملا تصاه بی کلید باید مین رمز حاصل از OR کی پاسخ: در رمز One Time Pad یک کاراکتر متن اصلی با یک کاراکتر از کاراکتر متن رمز واقعاً «تصادفی»
				را دارد. بدینسان میتوان این متن
				. کدام یک از اعداد زیر ریشه اولیه (tc
	د) 6	2 (₇	ب) 25	. كدام يك از اعداد زير ريشه اوليه (ot الف) 27
یشه اولیه دارند.	6 (s			الف) 27
	د) 6 همه گزینههای فوق ر	ند. $\{1,2,4,p^k,2 imes p^k\}$. بنابراین سازی و بعد امضا گاری و بعد امضا رو بعد رمزکردن بد فشردهسازی	، این مجموعه ریشه اولیه دار ت؟ بی انجام میشود بعد فشرده، بازی انجام میشود بعد رمزنگ عام میشود بعد فشردهسازی عام میشود بعد رمزکردن و ب	
	د) 6 همه گزینههای فوق ر	ند. $\{1,2,4,p^k,2 imes p^k\}$. بنابراین سازی و بعد امضا گاری و بعد امضا رو بعد رمزکردن بد فشردهسازی	، این مجموعه ریشه اولیه دار بت؟ بی انجام میشود بعد فشرده، بازی انجام میشود بعد رمزن ^د عام میشود بعد فشردهسازی عام میشود بعد رمزکردن و بع طرح شد، در PGP اول یک ا	الف) 27 پاسخ: اثبات می شود که فقط اعداد کدام گزینه در مورد PGP صحیح اس الف) در PGP اول عملیات رمزنگاری ب) در PGP اول عملیات فشرده س ج) در PGP اول عملیات امضا انج د) در PGP اول عملیات امضا انج

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 p=pq باشد، آنگاه (p-1)(q-1) (سوال تشریحی) پاسخ: این مورد در کلاس توضیح داده شد.

سی را نیز توضیح دهید؟ (سوال تشریحی) پاسخ	ما روند تولید کلید عمومی و خصوص	ه مانند m را در RSA توضیح دهید؟ حت	۹. روند امضای یک پیام ب
		لايدها است.	پاسخ این سوال در اس
رس داده شد)	ه، صحیح است؟ (این مورد امروز در	ساله غار علیبابا که در کلاس مطرح شد	۱۰. کدام گزینه در مورد می
حيح است.	ب) همه گزینهها صح	ـم راز است.	الف) یک مساله تسهی
روشهای غیرتعاملی است.	د) یک مساله از نوع	ع اثبات دانایی صفر است.	ج) یک مساله از نوع
	دانایی صفر است.	، صحیح است: یک مساله از نوع اثبات	پاسخ: فقط این گزینه
		ت؟ (شاید چند مورد صحیح باشد)	۱۱. كدام گزينه صحيح اس
ز قرار میدهد.	ید کرده و در اختیار طرف مقابل نی	Key Agreeme): یک سمت کلید را توا	الف) توافق كليد (ent
ﻪ.	ر فرایند تولید کلید مشارکت می کنن	Key Establishmen): هر دو سمت، د	ب) برقراری کلید (t
	$\binom{n}{2}$ قراری ارتباط، برابر با	گوریتمهای نامتقارن بین n نفر برای بر	ج) تعداد کلید در ال
		نهها صحيح نيست	د) هیچکدام از گزی
اری کلید (Key Establishment):	تیم که استفاده از سازوکارهای برقر	ینهها صحیح نیست. در اسلایدها داش	پاسخ: هیچکدام از گز
قرار مىدهد.	ک کرده و در اختیار طرف مقابل نیز	Key Transp): یک سمت کلید را تولیا	ort) تبادل کلید
	ند تولید کلید مشارکت می کنند.	Key Agreeme): هر دو سمت، در فراین	• توافق کلید (ent
لید برای الگوریتمهای متقارن است نه نامتقارن	از سویدیگر، تعداد ک		
	یشود(به طور دقیق).	DES باعث غير خطى شدن سامانه مح	۱۲. كدام قسمت الگوريتم
Е (ъ	F (ج	S (ب	الف) P
		حیح میباشد.	پاسخ: گزینهی "S" ص
		ت؟ (شاید چند گزینه پاسخ باشد)	۱۳. كدام گزينه صحيح اس
تری دارند.	قارن با طول کلید کمتر امنیت بیشن	يد متقارن نسبت به الگوريتم كليد نامت	الف) الگوريتمهاي كل
متری احتیاج دارند.	ریتم کلید نامتقارن به تعداد کلید ک	گوریتمهای کلید متقارن نسبت به الگو	ب) در یک شبکه، ال
	ظریه اعداد است.	از الگوریتمهای کلید متقارن مبتنی بر ن	ج) امنیت بسیاری ا
كانال امن نداريم.	^ی اری به مانند گواهینامه، نیازی به ک	_، کلید نامتقارن در صورت داشتن سازوک	د) در الگوریتمهای
، همه گزینهها درست است.	نارن مبتنی بر نظریه اعداد است.).	منیت بسیاری از الگوریتمهای کلید متن	پاسخ: به جز گزینه (اه
		RS الزامي است؟	۱۴. کدام شرط در مورد A
سبت به n اول باشد.	ب) متن اصلی باید ن	نسبت به $\phi(n)$ اول باشد.	الف) متن اصلى بايد
$\phi(n)$ اول باشد.	د) کلید عمومی باید	n د نسبت به n اول باشد.	ج) کلید عمومی بای
	،گونهای که	منوان کلید عمومی در نظر میگیریم، با	پاسخ: پارامتر e را به ع
	$1 < e < \phi(n), (e, \phi(n))$) = 1.	
(\alpha = \alpha \cdot \	- -		7*
باشد؟ (ممكن است چند گزينه صحيح باشد)	دید یک جایدشت از م <i>ج</i> موعه اصنی		
د) 10	34 (z	ا 17 (ت	الف) 7

پاسخ: اگر a عدد a عدد a مجموع کاهشیافته مانده ها باشد، آن گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ باشد. پس پاسخ اعداد 10 و 7 است. رسوال تشریحی) پاسخ: a این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها اگر a عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a یعنی a 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، آن گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

الف) 5 (ج) 5 (الف) 5

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

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

۱۸. برای این که Alice پیامی را برای Bob رمز کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد محرمانه Alice ب) كليد محرمانه Bob ج) كليد عمومي Alice د) كليد عمومي

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

١٩. تعداد ريشه اوليه عدد 60 كدام گزينه است؟

2 (ع ع الف) 4 (الف) 4 (ع الف) 4 (ع ا

یاسخ: 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 بالف) گمراه کنندگی - آشکار - متن رمز

ج) انتشار - رمز - کلید داری -

یاسخ: گزینهی "گمراه کنندگی - رمز - کلید" صحیح می باشد.

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 مین آشکار الله کنندگی - متن رمز شده - متن آشکار

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

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

- ۲۲. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.
 - ٢٣. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى أن عبارت صحيح /غلط را بنويسيد.
 - 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.

یاسخ:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمني دارد.
- بب 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.
 - ۲۴. PGP امنیت را در کدام لایه برای ما به ارمغان می آورد؟

الف) لايه كاربرد ب) لايه پيوند داده ج) لايه شبكه د) لايه انتقال

ياسخ: گزينه صحيح لايه كاربرد (Application Layer) است.

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

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

- ۲۶. کدام گزینه صحیح نیست؟ (میتوانید چند گزینه را انتخاب کنید).
- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 راه حل نمره ندارد.
 - ۲۸. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حملهای صورت پذیرفت؟

الف) حمله نوع اول ب) هيچكدام 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.

3^{90} وقم آخر عدد 3^{90} چند است?

پاسخ: 🗖 دقت کنید که در واقع ما به دنبال پاسخ (10 3^{90} هستم. میدانیم که:

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

🗀 آنگاه براحتی می توانیم بنویسیم که:

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

- ۳۰. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.
- در یک سامانه رمزگذاری، ما بهصورت غیرعمد میخواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 <u>بهصورت عمدی می</u>خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینهها صحیح است.

شماره بر	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
۵۳	14.4/.7/11	امنیت سیستمهای کامپیوتری		<u> </u>
	17.1/.1/11	امنیت سیستمهای کامپیوتری		

د) F

S (ج P (ب E الف)

پاسخ: گزینهی "S" صحیح میباشد.

- ۲. اثبات کنید که اگر p=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)

10 (د) 34 (ج بر 17 بر 17 بر 13 بر 17 بر 19 بر 19

پاسخ: اگر $\{x_1,x_2,\dots,x_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد x_n در مجموعه کاهش یافته مانده ها یعنی $\{ar_1,ar_2,\dots,ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $x_n=1$ 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 باکش الف) گمراه کنندگی - آشکار - متن رمز

ج) انتشار - آشکار - متن رمز دانتشار - رمز - کلید

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

 δ . تعداد ریشه اولیه عدد 60 کدام گزینه است $^{\circ}$

2 (د) 2 (ح) 8 (الف) 8

پاسخ: این عدد ریشه اولیه ندارد.

کدام شرط در مورد RSA الزامی است؟

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

ج) کلید عمومی باید نسبت به p(n) اول باشد. p(n) اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

- ٧. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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.

		سامانه رمزگذاری آگاهی دارد.	- و دشمن از تمامی جزئیات
Vern فقط نسبت به حمله نوع اول،	ک نویز به متن اصلی اضافه کنیم. um	، ما بهصورت عمدی میخواهیم یک	پاسخ: در یک سامانه رمزگذاری
			ایمنی دارد. مابقی گزینهها صح
یعی از پراکنده است.	است ساختاری آماری رو حجم وس	ی ویژگی را دارد که به این معنا	۸. طبق گفته شانون یک سامانه قو
. آشکار	ب) انتشار - متن رمز شده - متر	، من شده	الف) انتشار - متن آشکار - متن
	ب) المسار المس رمز ساده المحار د) گمراه کنندگی - متن آشکار		ج) گمراه کنندگی - متن رمز
776			
	ئىد.	مکار - متن رمز شده" صحیح میباش	
		ى با	۹. طول واقعی کلید DES برابر است
۳۲ (۵	ج) ۶۴	ب) ۵۶	الف) ۴۸
		باشد.	پاسخ: گزیندی "۵۶" صحیح می
	است چند گزینه صحیح باشد)		۱۰. کدام یک از اعداد زیر ریشه اولیه
د) 6	ج) 27	ب) 25	الف) 2
بنههای فوق ریشه اولیه دارند.	بنابراین همه گزی $\{1,2,4,p^k,2 imes p^k\}$	داد این مجموعه ریشه اولیه دارند.	پاسخ: اثبات میشود که فقط اء
			۱۱. کدام یک از جملات زیر صحیح ا
ىت.	سبت به حمله نوع سوم کاملا شکننده اس		
		ت سامانه رمزگذاری آگاهی دارد.	
			پاسخ:
	ه نوع اول، ایمنی دارد.	است. Vernum فقط نسبت به حمل	- ,
صل، امنیت یک الگوریتم رمزگذاری	از اصل Kerckhoffs است. برطبق این		
	ش کافی راجع به کل فرایند رمزگذاری و		
ت.	پاسخ: پاسخ این سوال در اسلایدها اس	را توضیح دهید؟ (سوال تشریحی)	۱۲. پروتکل توافق کلید دیفی-هلمن
سیح دهید؟ (سوال تشریحی) پاسخ:	تولید کلید عمومی و خصوصی را نیز توم	را در RSA توضیح دهید؟ حتما روند	m روند امضای یک پیام به مانند. 1
		ت.	پاسخ این سوال در اسلایدها اس
		ما به ارمغان میآورد؟	PGP .۱۴ امنیت را در کدام لایه برای
د) لايه پيوند داده	ج) لايه كاربرد	ب) لايه شبكه	الف) لايه انتقال
		(Application Layer) است.	پاسخ: گزینه صحیح لایه کاربرد
	رمز کند و برای Bob ارسال کند.		۱۵. برای این که Alice پیامی را برای
د) کلید محرمانه Bob	ج) کلید عمومی Bob	ب) کلید عمومی Alice	الف) كليد محرمانه Alice
	ه و برای او ارسال می کند.	م m را با کلید عمومی Bob رمز کرد	پاسخ: Alice برای رمزکردن، پیا
			۱۶. کدام گزینه در مورد رمز me Pad
			الف) طول كليد مىبايست برابر
			ب) کلید باید به صورت کاملا ت
	٣١	۴	

- ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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 می شود (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. بدین سان می توان 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 فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمز کردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

- ۱۸. معکوس عدد پنج در مبنای 13 را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۸ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.
- 19. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.
 - ۲۰. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حملهای صورت پذیرفت؟

الف) حمله نوع دوم ب) هيچ كدام 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.

- ٢١. كدام گزينه صحيح است؟ (شايد چند گزينه پاسخ باشد)
- الف) الگوریتمهای کلید متقارن نسبت به الگوریتم کلید نامتقارن با طول کلید کمتر امنیت بیشتری دارند.
- ب) دریک 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 a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها اگر $a^{\phi(n)} = a$ در مجموعه کاهش یافته مانده ها اگر $a^{\phi(n)} = a$ در مجموعه کاهش یافته مانده ها یعنی a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a یک جایگشت کامل از مجموعه اولیه است. پس داریم:

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

 3^{90} حدد است. رقم آخر عدد 3^{90}

7 (ع ج) 8 (ج ب) 9 الف) 9 (م)

پاسخ: 🕰 دقت کنید که در واقع ما به دنبال پاسخ (mod 10) 3^{90} هستم. میدانیم که:

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

🔼 آن گاه براحتی می توانیم 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 علی بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

ب) یک مساله از نوع اثبات دانایی صفر است.

الف) یک مساله تسهیم راز است.

د) یک مساله از نوع روشهای غیرتعاملی است.

ج) همه گزینهها صحیح 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 صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه اطلاعاتی در مورد متن اصلی پی ببرد.

یاسخ: 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) هيچكدام 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 مشتری نظیر الگوریتمهای رمزنگاری مورد پشتیبانی جلوگیری می شود؟ در تمام مراحل یکپارچگی پیامها حفظ می شود در تمام مراحل پیامها با کلید نامتقارن رمز می شود در مراحل انتهایی، کل پیامهای مبادله شده به صورت امضا شده از سرور خدمتگزار برای مشتری ارسال می شود. هیچکدام

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

۲۸. برای این که Alice پیامی را برای Bob امضا کند، می بایست آن را با رمز کند و برای Bob ارسال کند.

ب) كليد محرمانه Bob ج) كليد محرمانه Alice ب) كليد محرمانه

الف) كليد عمومى Alice

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

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

4 (ع 5 (ج 5 الف) 3

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

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

- ۳۰. كدام گزينه صحيح است؟ (شايد چند مورد صحيح باشد)
- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با (رتباط، برابر با نفر برای برقراری ارتباط، برابر با (رتباط، برابر با ایم تعداد کلید در الگوریتم های نامتقارن بین n
 - د) هیچکدام از گزینهها صحیح نیست

یاسخ: 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
۵۴	14.4/.4/11	امنیت سیستمهای کامپیوتری		

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

الف) حمله نوع اول ب) حمله نوع دوم ج) هيچ كدام 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 راه حل نمره ندارد.
 - ٣. كدام گزينه صحيح است؟ (شايد چند گزينه 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 می شود بعد فشرده سازی و بعد امضا
 - ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
 - ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
 - د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

یاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

- کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)
- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - ج) تعداد کلید در الگوریتمهای نامتقارن بین n نفر برای برقراری ارتباط، برابر با $(\frac{n}{2})$
 - 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، 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)

25 (د) 2 (ح) 2 (ع) 2 (الف) 2 (ع) 2 (ع)

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

کدام شرط در مورد RSA الزامی است؟

ب) متن اصلی باید نسبت به $\phi(n)$ اول باشد. الف) متن اصلی باید نسبت به n اول باشد. د) کلید عمومی باید نسبت به $\phi(n)$ اول باشد. ج) کلید عمومی باید نسبت به n اول باشد. یاسخ: یارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که $1 < e < \phi(n), \quad (e, \phi(n)) = 1.$

٩. ويژگى به اين معنا است كه هر بين از متن بايد به چندين قسمت وابسته باشد.

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

الف) انتشار - رمز - كليد

ج) گمراه کنندگی - رمز - کلید

ياسخ: گزينهي "گمراه كنندگي - رمز - كليد" صحيح ميباشد.

١٠. تعداد ريشه اوليه عدد 60 كدام گزينه است؟

د) 6 2 (ت الف) 4 ₂ (ج

یاسخ: این عدد ریشه اولیه ندارد.

- ۱۱. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى أن عبارت صحيح /غلط را بنويسيد.
- 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.

یاسخ:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمني 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.
 - ۱۲. طول واقعی کلید DES برابر است با

ج) ۶۴ ۲۲ (۵ ے) ۵۶ الف) ۴۸

پاسخ: گزینهی "۵۶" صحیح میباشد.

۱۳. در SSH چگونه از حمله تغییر قابلیتهای مشتری نظیر الگوریتمهای رمزنگاری مورد پشتیبانی جلوگیری می شود؟ 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 می شود. هیچکدام

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

- باسخ: پاسخ: (سوال تشریحی) پاسخ: 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 (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.
 - 3^{90} وقم آخر عدد 3^{90} چند است?

6 (ه 9 (ج 8 (ب 7 8)

پاسخ: 🕰 دقت کنید که در واقع ما به دنبال پاسخ (10 3^{90} هستم. میدانیم که:

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

🔼 آن گاه براحتی میتوانیم بنویسیم که:

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

- ١٧. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 <u>بهصورت عمدی می</u>خواهیم 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 كليد مى بايست برابر با طول متن اصلى باشد.
 - ب) کلید باید به صورت کاملا تصادفی تولید شود.
 - ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

	(به طور دقیق).	ث غیر خطی شدن سامانه میشود(كدام قسمت الگوريتم DES باعد 		
S (2	F (ج	E (ب	الف) P		
		اشد.	پاسخ: گزینهی "S" صحیح میب		
	، صورت پذیرفت؟	ط Turing، توسط چه نوع حملهای	۲. رمزشکنی ماشین Enigma توس		
د) حمله نوع اول	ج) هیچکدام	ب) حمله نوع سوم	الف) حمله نوع دوم		
Known Plaint)، رمزشکنی ماشین	ک یا چند متن اصلی معلوم (ext Attack:	، حمله نوع دوم یا حمله بر اساس یک	پاسخ: دو مثال مشهور، در زمینا		
	خشی از متن متن اصلی معلوم بوده است				
	رمز کند و برای Bob ارسال کند.	Bob رمز کند، میبایست آن را با	۲. برای این که Alice پیامی را برای		
د) کلید عمومی Alice	ج) كليد محرمانه Bob	ب) کلید عمومی Bob	الف) كليد محرمانه Alice		
	ه و برای او ارسال می کند.	م m را با کلید عمومی Bob رمز کرد	پاسخ: Alice برای رمزکردن، پیا		
			۲. کدام گزینه صحیح نیست؟ (می		
من، نتواند بر اساس متن رمز شده	رتی که علی رغم توان زیاد محاسباتی دش	UnconditionalSec) یعنی در صو	الف) امنيت بدون شرط (urity		
	وسط متن رمز درز نمی کند.	هیچگونه اطلاعاتی از متن اصلی تو	سیستم را بشکند، چرا که		
محاسباتی پیچیده و طولانی باشد.	رتی که شکستن سیستم رمز عملا از نظر	Computational Se) یعنی در صو	ب) امنیت محاسباتی (curity		
	است. One Time Pad	ن شناخته شده، سامانه Vernam یا	ج) تنها سامانه بدون شرط امر		
ر در صورت مشاهده متن رمز، نباید	ت نویز به متن اصلی اضافه کنیم. حملهگ	ما بهصورت غيرعمد مىخواهيم يك	د) در یک سامانه رمزگذاری،		
		مورد متن اصلی پی ببرد.	به هیچگونه اطلاعاتی در ه		
گزینهها صحیح است.	ت نویز به متن اصلی اضافه کنیم. مابقی ً	، ما <u>بەصورت عمدى مى</u> خواھيم يك	پاسخ: در یک سامانه رمزگذاری		
پاسخ: (سوال تشریحی) $a^{\phi(n)}=1$	$1 \mod n$ اشند، آنگاه خواهیم داشت	عدد a و n نسبت به همدیگر اول ب	۲. این قضیه را اثبات کنید: اگر دو		
اگر $\{r_1, r_2, \dots, r_{\phi(n)}\}$ مجموع کاهش یافته مانده ها باشد، آن گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها					
	ه است. پس داریم:	ک جایگشت کامل از مجموعه اولید	$\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ يعنى		
$\prod_{i=1}^{\phi(n)} (ar_i \mod$	$d n) = \prod_{i=1}^{\phi(n)} r_i \Longrightarrow \left(a^{\phi(n)}\right) \left(\prod_{i=1}^{\phi(n)} r_i\right)$	$ = \left(\prod_{i=1}^{\phi(n)} r_i\right) \Longrightarrow a^{\phi(n)} \equiv 1 $	\pmod{n}		
خواهد شد؟	با همان کلید محرمانه برابر با کدام گزینه	و مقدار $e=5$ باشد، آن گاه d ی $n=$	۲. اگر در الگوريتم RSA مقدار 35		
4 (د	3 (ج	6 (ب	الف) 5		
بریم، بهگونهای که	را به عنوان کلید عمومی در نظر می گی e	ست. همان طور که میدانید، پارامتر	پاسخ: گزینه صحیح عدد پنج اه		
	$1 < e < \phi(n), (e,$	$\phi(n)) = 1.$			
		نه در نظر می گیریم، به گونهای که:	پارامتر d را به عنوان کلید محرما		
	$ed \equiv 1 \pmod{r}$				

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

کلید عمومی Alice	رى Bob	ج) کلید عمومی	ب) كليد محرمانه Bob	الف) كليد محرمانه Alice	
	کند.	کردہ و برای Bob ارسال مے	را با کلید خصوصی خودش رمز ک	m برای امضا، پیام Alice پاسخ:	
پراکنده است.	رو حجم وسیعی از .	نا است ساختاری آماری	ں ویژ <i>گی</i> را دارد که به این م ع	۲۷. طبق گفته شانون یک سامانه قوی	
ب) انتشار - متن رمز شده - متن آشکار			شده - متن آشکار	الف) گمراه کنندگی - متن رمز ن	
د) انتشار - متن آشکار - متن رمز شده			ج) گمراه کنندگی - متن آشکار - متن رمز شده		
		اشد.	کار - متن رمز شده" صحیح می،	پاسخ: گزینهی "انتشار - متن آش	
	ز درس داده شد)	حیح است؟ (این مورد امرو	یبابا که در کلاس مطرح شد، ص	۲۸. کدام گزینه در مورد مساله غار عل	
ب) همه گزینهها صحیح است.			الف) یک مساله از نوع اثبات دانایی صفر است.		
د) یک مساله از نوع روشهای غیرتعاملی است.				ج) یک مساله تسهیم راز است.	
		ی صفر است.	ت: یک مساله از نوع اثبات دانایر	پاسخ: فقط این گزینه صحیح اس	
			ما به ارم غ ان می آورد؟	PGP. ۲۹ امنیت را در کدام لایه برای ه	
لايه انتقال	ده د)	ج) لايه پيوند داد	ب) لايه كاربرد	الف) لايه شبكه	
			(Application Layer) است.	پاسخ: گزینه صحیح لایه کاربرد (
چند گزینه صحیح باشد)	ىلى باشد؟ (ممكن است	ک جایگشت از مجموعه اص		۳۰. اعضای مجموعه \mathbb{Z}_{17}^* را در کدام ع	
17	(১	ج) 10	ب) 34	الف) 7	
د محموعه کاهش بافته	عاصل شده ا: ضاب عده	ها باشد، آن گاه محموعه ح	محموع کاهش بافته مانده ${\mathbb Z}^*=$	$\{r_1, r_2, \dots, r_{\phi(n)}\}$ پاسخ: اگر	
				$ar_2,\ldots,ar_{\phi(n)}\}$ ماندهها یعنی	

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

۲۶. برای این که Alice پیامی را برای Bob امضا کند، می بایست آن را با رمز کند و برای Bob ارسال کند.

خواهد شد.



شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
۵۵	14.4/.4/11	امنیت سیستمهای کامپیوتری		

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

الف) حمله نوع سوم ب) حمله نوع اول ج) هيچ كدام 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 این که Alice پیامی را برای Bob رمز کند، می بایست 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

یاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می کند.

طول واقعی کلید DES برابر است با

الف) ۳۲ (ب که ۲۸ (ج که ۱۹۵۱) ۴۸ د) ۶۴ (د)

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 متن رمز شده

ج) انتشار - متن آشکار - 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.

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

4 (ه 5 (الف) 5

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

پارامتر d را به عنوان کلید محرمانه در نظر می گیریم، به گونه ای که:

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

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

وسوال تشریحی) پاسخ: a این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a

:يعنى $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ يک جايگشت کامل از مجموعه اوليه است. پس داريم

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

 90 رقم آخر عدد 90 چند است?

6 (ه 9 (الف) 9

پاسخ: 🕰 دقت کنید که در واقع ما به دنبال پاسخ (10 mod 10) هستم. می دانیم که:

- $\phi(10)=4$ یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
 - (3,10)=1 عدد سه و ده نسبت به هم اول هستند، یعنی ullet

🔼 آن گاه براحتی میتوانیم بنویسیم که:

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

- 9. 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.
 - ١٠. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
 - 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.

ياسخ:

- الف این جمله کاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد.
- ببله 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.
 - ۱۱. کدام گزینه در مورد مساله غار علی بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)

ب) یک مساله تسهیم راز است.

الف) یک مساله از نوع اثبات دانایی صفر است.

د) یک مساله از نوع روشهای غیرتعاملی است.

ج) همه گزینهها صحیح 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) هيچ كدام 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؟ (می توانید چند گزینه را انتخاب کنید).

- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 راه حل نمره ندارد.
 - 1۵. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه اطلاعاتی در مورد متن اصلی یی 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 گزینه ها صحیح است.

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

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

- ۱۷. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟
 - الف) طول كليد مي بايست برابر با طول متن اصلي باشد.
 - ب) کلید باید به صورت کاملا تصادفی تولید شود.
 - ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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 می شود (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. بدین سان می توان 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 فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام میخورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

١٩. تعداد ريشه اوليه عدد 60 كدام گزينه است؟

پاسخ: این عدد ریشه اولیه ندارد.

- ۲۰. كدام گزينه صحيح است؟ (شايد چند مورد صحيح باشد)
- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با الگوریتمهای نامتقارن بین n نفر برای برقراری ارتباط، برابر با
 - 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوى ديگر، تعداد كليد براي الگوريتمهاي متقارن است نه نامتقارن

۲۱. اثبات کنید که اگر p=pq باشد، آن گاه (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 می آورد؟

الف) لايه پيوند داده ب) لايه انتقال ج) لايه کاربرد د

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

- ٢٣. كدام گزينه صحيح است؟ (شايد چند گزينه 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 ج) 10 ج) 17 د) 71

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

۲۵. کدام شرط در مورد RSA الزامی است؟

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

الف) کلید عمومی باید نسبت به n اول باشد.

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

ج) متن اصلی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

۲۶. كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

E (ه F (ج

S (ب P (فا

پاسخ: گزینهی "S" صحیح میباشد.

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

25 (s 6 (ج

27 (ب 2 الف)

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

۲۸. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.

۲۹. برای این که Alice پیامی را برای Bob امضا کند، می بایست آن را با رمز کند و برای Bob ارسال کند.

د) کلید محرمانه Alice

ج) کلید عمومی Bob

ب) کلید محرمانه Bob

الف) کلید عمومی Alice

یاسخ: Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می کند.

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

ب) انتشار - آشکار - متن رمز

الف) گمراه کنندگی - رمز - کلید

د) انتشار - رمز - کلید

ج) گمراه کنندگی - آشکار - متن رمز

ياسخ: گزينهي "گمراه كنندگي - رمز - كليد" صحيح مي باشد.



شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
۵۶	14.4/.4/11	امنیت سیستمهای کامپیوتری		

- ١. كدام گزينه صحيح است؟ (شايد چند گزينه 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.

ب) انتشار - متن رمز شده - متن آشکار

الف) گمراه کنندگی - متن آشکار - متن رمز شده

د) انتشار - متن آشکار - متن رمز شده

ج) 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 راه حل 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)

لف) 34 (ف) 17 (ء تا 10 (ب) على الله على

پاسخ: اگر $\{ar_1,ar_2,\ldots,ar_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آن گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1,ar_2,\ldots,ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1,ar_2,\ldots,ar_{\phi(n)}\}$ 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.

ب) انتشار - آشکار - متن رمز

الف) گمراه کنندگی - رمز - کلید

د) گمراه کنندگی - آشکار - متن رمز

ج) انتشار - رمز - کلید

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 (p-1)(q-1) و $\phi(n)=(p-1)(q-1)$ (سوال تشریحی) پاسخ: این مورد در کلاس توضیح داده شد.
 - ۸. کدام شرط در مورد RSA الزامی است؟

ب) کلید عمومی باید نسبت به n اول باشد.

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

د) متن اصلی باید نسبت به n اول باشد.

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

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

٩. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.

- الف امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 <u>بهصورت عمدی می</u>خواهیم 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، آن گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

4 (د) 5 (ج) 5 (الف) 3

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

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

- ۱۱. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟
 - الف) طول كليد مي بايست برابر با طول متن اصلى 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 می شود (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. بدین سان می توان 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) هيچكدام 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.

١٣. تعداد ريشه اوليه عدد 60 كدام گزينه است؟

2 (ه ک الف) 6 (الف) 6 (الف) 8 (ب الف) 8 (ب الف

پاسخ: این عدد ریشه اولیه ندارد.

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

پاسخ: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

1۵. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.

- 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.

باسخ:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمنى دارد.
- ببله 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 حمله گر 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 صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

الف) یک مساله تسهیم راز اس		ب) همه گزینهها صحیح است.	
ج) یک مساله از نوع اثبات ه	یی صفر است.	د) یک مساله از نوع روشهای غیر	رتعاملی است.
پاسخ: فقط این گزینه صحیح	ت: یک مساله از نوع اثبات دانایی صف	فر است.	
۱۹. رقم آخر عدد 3^{90} چند است؟			
الف) 8	و) 6	ج) 9	7 (د
پاسخ: 🖾 دقت کنید که در	قع ما به دنبال پاسخ $3^{90} \pmod{10}$ ه	مستم. میدانیم که:	
يعنى چهار. $\phi(10)=4$	د مثبت وجود دارد که کمتر از 10 است	ت و نسبت به آن اول هست.	
• عدد سه و ده نسبت به ه	(3,10) = 1 ول هستند، یعنی		
• برطبق قضیه اویلر-فرما	$3^4 = 1 \pmod{10}$ يم:		
🛍 آن گاه براحتی میتوانیم	ويسيم كه:		
	$\times (3^2) = 9 \pmod{10}.$	$3^{90} = 3^{4 \times 22 + 2} = (3^4)^{22} >$	
۲۰. PGP امنیت را در کدام لایه برا	ما به ارمغان می آورد؟		
الف) لايه انتقال	ب) لايه شبكه	ج) لايه كاربرد	د) لايه پيوند داده
پاسخ: گزینه صحیح لایه کاربر	(Application Layer) است.		
د روند امضای یک پیام به مانند \imath	ا در RSA توضیح دهید؟ حتما روند تول	ید کلید عمومی و خصوصی را نیز توضیع	ح دهید؟ (سوال تشریحی) پاسخ
پاسخ این سوال در اسلایدها ا	<i>ن</i> .		
۲۲. کدام یک از اعداد زیر ریشه اوا	(Primitive Root) دارند؟ (ممكن اس	ت چند گزینه صحیح باشد)	
الف) 6	ب) 27	ج) 2	د) 25
		بنابراین همه گزینه $\{1,2,4,p^k,2 imes p\}$	های فوق ریشه اولیه دارند.
۲۳. برای این که Alice پیامی را برا	Bob رمز کند، میبایست آن را با	رمز کند و برای Bob ارسال کند.	
الف) كليد محرمانه Alice	ب) کلید عمومی Alice	ج) كليد محرمانه Bob	د) کلید عمومی Bob
پاسخ: Alice برای رمزکردن،	م m را با کلید عمومی Bob رمز کرده و m	برای او ارسال می کند.	
۲۴. طول واقعی کلید DES برابر ام	، با		
الف) ۵۶	ب) ۳۲	ج) ۶۴	د) ۴۸
پاسخ: گزینهی "۵۶" صحیح ه	باشد.		
	Bob امضا کند، میبایست آن را با	رمز کند و برای Bob ارسال کند.	
الف) کلید عمومی Alice	ب) كليد محرمانه Bob	ج) كليد محرمانه Alice	د) کلید عمومی Bob
پاسخ: Alice برای امضا، پیام	را با کلید خصوصی خودش رمز کرده	و برای Bob ارسال می کند.	
	ل Turing، توسط چه نوع حملهای صو		

الف) حمله نوع اول ب) هيچكدام 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.

٧٧. كدام قسمت الكوريتم DES باعث غير خطى شدن سامانه مي شود (به طور دقيق).

P (ه E (ج F (الف)

پاسخ: گزینهی "S" صحیح میباشد.

۲۸. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.

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

الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.

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

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

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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

و سوال تشریحی) پاسخ: $a^{\phi(n)} = 1 \mod n \mod n$ این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) پاسخ: اگر $a^{\phi(n)} = 1 \mod n$ عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $a^{\phi(n)} = 1 \mod n$ یک جایگشت کامل از مجموعه اولیه است. پس داریم:

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



نام و نام خانوادگی	شماره دانشجویی	نام درس	تاريخ	شماره برگه
	<u> </u>	امنیت سیستمهای کامپیوتری	وتری ۴۰۳/۰۲/۱۱	۵۷
`\.\\"*-dsoozo.cl	دراه عدد ضرب کنید تا محمد محمد	در در کی حارگشت از وجوه وعداد ا	صل داشد؟ (ممكن ار	ور گزیر ام
$^{\prime}$ ای مجموعه \mathbb{Z}_{17}^{*} را در	ئدام عدد ضرب کنیم تا مجموعه ح	دید یک جایگشت از مجموعه اصلی	صلی باشد؟ (ممکن اس	چند گزینه صحی
ىاى مجموعه ₁₇ ″را در َ) 10	ئدام عدد ضرب کنیم تا مجموعه ح ب) 34	دید یک جایگشت از مجموعه اصل _ح ج) 7		چند گزینه صحید 1

پاسخ: اگر $\{r_1, r_2, \dots, r_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آن گاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1, ar_2, \dots, ar_{\phi(n)}\}$ باشد. پس پاسخ اعداد 10 و 7 است.

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

ب) یک مساله تسهیم راز است.

الف) همه گزینهها صحیح است.

٠١

د) یک مساله از نوع اثبات دانایی صفر است.

ج) یک مساله از نوع روشهای غیرتعاملی 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، آن گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

4 (ج) 3 (ه (+) 4 (ه (+) 6 (ه (+) 8 (ه) 8 (ه) 8 (ه) 8 (ه) 8 ((+) 8 (ه (+) 8 (ه) 8 (ه) 8 ((+) 8 (ه) 8 (ه) 8 (ه) 8 ((+) 8 (ه) 8 (ه) 8 ((+) 8 (ه) 8 (ه) 8 (ه) 8 ((+) 8 (ه) 8 (ه) 8 ((+) 8 (ه) 8 (ه) 8 ((+) 8 (ه) 8 (ه) 8 ((+) 8 (ه) 8 (ه) 8 ((+) 8 (ه) 8 (ه) 8 ((+) 8 (ه) 8 (ه) 8 ((+) 8 (ه) 8 (ه) 8 ((+) 8 (ه) 8 (ه) 8 ((+)

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

5 پس ابتدا $\phi(n)$ را محاسبه می کنیم که برابر با $\phi(35)=24$ خواهد شد. سپس باید معکوس عدد e=5 در پیمانه $\phi(n)=0$ را محاسبه کنیم که برابر با خواهد شد.

۴. كدام يك از اعداد زير ريشه اوليه (Primitive Root) دارند؟ (ممكن است چند گزينه صحيح باشد)

27 (ه 25 الف) 25

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

- ۵. كدام گزينه صحيح است؟ (شايد چند گزينه 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.

یاسخ: 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 می آورد؟

	ر دقیق).		پاسخ: گزینه صحیح لایه کاربرد (ayer . کدام قسمت الگوریتم DES باعث غیر
P (3	S (5	E (ب	الف) F
		ست؟	پاسخ: گزینهی "S" صحیح میباشد. . تعداد ریشه اولیه عدد 60 کدام گزینه ا
4 (ه	ج) 8	6 (ب	2 (الف

ج) لايه انتقال

د) لايه شبكه

پاسخ: این عدد ریشه اولیه ندارد.

الف) لايه پيوند داده

- ٩. كدام گزينه صحيح نيست؟ (ميتوانيد چند گزينه را انتخاب كنيد).
- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.

ب) لايه كاربرد

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

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

- ۱۰. کدام گزینه صحیح است؟ (شاید چند مورد صحیح باشد)
- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با (تباط، برابر با رقراری ارتباط، برابر با با تعداد کلید در الگوریتمهای نامتقارن بین n نفر برای برقراری ارتباط، برابر با
 - 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

۱۱. کدام گزینه در مورد PGP صحیح است؟

- الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمز کردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی 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 راه حل نمره ندارد.
 - ۱۳. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حملهای صورت پذیرفت؟

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. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- الف امنیت بدون شرط (Unconditional Security) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 به صورت عمدی می خواهیم یک نویز به متن اصلی اضافه کنیم. Vernum فقط نسبت به حمله نوع اول، ایمنی دارد. مابقی گزینه ها صحیح است.

۱۵. کدام شرط در مورد RSA الزامی است؟

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

د) کلید عمومی باید نسبت به n اول باشد.

الف) متن اصلی باید نسبت به n اول باشد.

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

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

- 16. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- 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.

یاسخ:

- 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 بر مخفی ماندن کلید باشد، حتی اگر حمله گر 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 بالف) گمراه کنندگی - آشکار - متن رمز

ج) انتشار - رمز - کلید دارت کلید دار

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

 3^{90} چند است 3^{90} چند است

6 (د) 7 (ج) 8 (د) 9

پاسخ: 🕰 دقت کنید که در واقع ما به دنبال پاسخ (mod 10) 3^{90} هستم. میدانیم که:

- $\phi(10)=4$ یعنی چهار عدد مثبت وجود دارد که کمتر از $\phi(10)=4$ است و نسبت به آن اول هست.
 - (3,10) = 1 عدد سه و ده نسبت به هم اول هستند، یعنی
 - $3^4 = 1 \pmod{10}$ برطبق قضیه اویلر-فرما داریم:
 - 🔼 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 كليد مي بايست برابر با طول متن اصلى باشد.
 - ب) کلید باید به صورت کاملا تصادفی تولید شود.
 - ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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 متن رمز واقعاً «تصادفی» خواهد بود، که هیچ ارتباطی با متن اصلی ندارد. از دیدگاه شانون، چنین سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

- ۲۰. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.
 - ۲۱. برای این که Alice پیامی را برای Bob امضا کند، می بایست آن را با رمز کند و برای Bob ارسال کند.
 - Bob کلید عمومی Alice برای امضا، پیام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می کند.
 - ۲۲. اثبات کنید که اگر p=pq باشد، آن گاه (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 بیان انتشار متن آشکار متن رمز شده متن آشکار جاتن رمز شده متن آشکار جاتن آشکار بیان انتشار کنندگی متن رمز شده متن آشکار جاتن آشکار بیان کنندگی متن رمز شده متن آشکار بیان کنندگی متن آشکار متن رمز شده متن آشکار بیان کنندگی متن آشکار متن رمز شده بیان کنندگی متن آشکار متن آشک
 - **پاسخ:** گزینهی "انتشار متن آشکار متن رمز شده" صحیح میباشد.
 - ۲۵. برای این که Alice پیامی را برای Bob رمز کند، میبایست آن را با رمز کند و برای Bob ارسال کند.
 - Bob کلید محرمانه Bob برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می کند.
 - ۲۶. طول واقعی کلید DES برابر است با

الف) ۵۶ ج) ۴۸ ب

ياسخ: گزينهي "۵۶" صحيح مي باشد.

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

ور سوال تشریحی) پاسخ: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: a سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها اگر a عدد a در مجموعه کاهش یافته مانده ها اگر اگر اور عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a یعنی a 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: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

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

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.

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
۵۸	14.47.411	امنیت سیستمهای کامپیوتری		

۱. اگر در الگوریتم RSA مقدار e=5 و مقدار e=5 باشد، آن گاه d یا همان کلید محرمانه برابر با کدام گزینه خواهد شد؟

4 (ه 5 الف) 5 الف

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

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

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

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

الف) حمله نوع دوم ب) حمله نوع اول ج) هيچ كدام 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.

- ٣. كدام گزينه صحيح است؟ (شايد چند مورد صحيح باشد)
- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با (رتباط، برابر با نفر برای برقراری ارتباط، برابر با (رتباط، برابر با ایم تعداد کلید در الگوریتم های نامتقارن بین n
 - 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، تعداد کلید برای الگوریتمهای متقارن است نه نامتقارن

- ۴. كدام گزينه صحيح نيست؟ (ميتوانيد چند گزينه را انتخاب كنيد).
- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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.

ه. این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها اگر $\mathbb{Z}_n^* = \{r_1, r_2, \dots, r_{\phi(n)}\}$ 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 می آورد؟

الف) لايه شبكه ب) لايه انتقال ج) لايه كاربرد داده

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

۷. کدام شرط در مورد RSA الزامی است؟

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

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

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای 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.

ب) گمراه کنندگی - متن رمز شده - متن آشکار

د) انتشار - متن آشکار - متن رمز شده

الف) گمراه کنندگی - متن آشکار - متن رمز شده

ج) انتشار - متن رمز شده - متن آشکار

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

- ٩. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوي آن عبارت صحيح /غلط را بنويسيد.
- 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.

یاسخ:

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمنى دارد.
- ببله 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 حمله گر 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: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند. ۱۲. برای این که Alice پیامی را برای Bob امضا کند، می بایست آن را با رمز کند و برای Bob ارسال کند. ج) کلید محرمانه Bob ب) کلید عمومی Alice الف) كليد عمومي Bob د) کلید محرمانه Alice پام m را با کلید خصوصی خودش رمز کرده و برای Bob ارسال می کند. m١٣. ويژگى به اين معنا است كه هر بين از متن بايد به چندين قسمت وابسته باشد. ب) گمراه کنندگی - رمز - کلید الف) گمراه كنندگى - آشكار - متن رمز د) انتشار - رمز - کلید ج) انتشار - آشکار - متن رمز ياسخ: گزينهي "گمراه كنندگي - رمز - كليد" صحيح ميباشد. ١٤. كدام گزينه صحيح است؟ (شايد چند گزينه ياسخ 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) د) 7 ب) 34 الف) 17 ج) 10 یاسخ: اگر $\mathbb{Z}_n^* = \{r_1, r_2, \dots, r_{\phi(n)}\}$ مجموع کاهشیافته ماندهها باشد، آن گاه مجموعه حاصل شده از ضرب عدد $\mathbb{Z}_n^* = \{r_1, r_2, \dots, r_{\phi(n)}\}$ مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ باشد. ۱۶. برای این که Alice پیامی را برای Bob رمز کند، می بایست آن را با رمز کند و برای Bob ارسال کند. د) کلید محرمانه Bob ج) كليد محرمانه Alice ب) کلید عمومی Bob الف) كليد عمومي Alice پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می کند. ۱۷. کدام گزینه در مورد PGP صحیح است؟

> ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمزکردن د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی ۳۴۵

الف) در PGP اول عملیات رمزنگاری انجام می شود بعد فشرده سازی و بعد امضا ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

(Primitive Root) دارند؟ (ممکن است چند گزینه صحیح باشد)

(الف) 27 پاسخ: اثبات می شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1,2,4,p^k,2\times p^k\}$. بنابراین همه گزینه های 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 (ج ج) ۴۸ د) ۵۶ د) ۵۶

ياسخ: گزينهي "۵۶" صحيح ميباشد.

۲۱. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.

- الف امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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.
- دوریک سامانه رمزگذاری، ما بهصورت غیرعمد میخواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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 گزینه ها صحیح است.

۲۲. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.

۲۳. اثبات کنید که اگر p = pq باشد، آنگاه (p-1)(q-1) (سوال تشریحی) پاسخ: این مورد در کلاس توضیح داده شد.

۲۴. تعداد ریشه اولیه عدد 60 کدام گزینه است؟

2 (د) 8 (ج) 4 (ب) 6 (الف)

یاسخ: این عدد ریشه اولیه ندارد.

۲۵. کدام گزینه در مورد مساله غار علی بابا 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.

 3^{90} . رقم آخر عدد 3^{90} چند است?

8 (ه ج) 6 (ج ب) 9 الف) 7

پاسخ: شع دقت کنید که در واقع ما به دنبال پاسخ ($10 \mod 10$ هستم. میدانیم که:

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

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

🗀 آنگاه براحتی می توانیم 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 كليد مي بايست برابر با طول متن اصلي باشد.
 - ب) کلید باید به صورت کاملا تصادفی تولید شود.
 - ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

٨٨. كدام قسمت الكوريتم DES باعث غير خطى شدن سامانه مى شود (به طور دقيق).

P (s $S(\tau)$ $F(\tau)$ E(t)

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 راه حل 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) هيچ كدام

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.

شماره برگه	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
۵۹	14.47.411	امنیت سیستمهای کامپیوتری		

کدام شرط در مورد RSA الزامی است؟

ب) متن اصلی باید نسبت به n اول باشد.

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

د) کلید عمومی باید نسبت به n اول باشد.

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

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

- ٢. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- 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.

- الف اين جمله كاملا غلط است. Vernum فقط نسبت به حمله نوع اول، ايمني 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 حمله گر دانش کافی راجع به کل فرایند رمزگذاری و رمزگشایی داشته باشد.
 - ۳. رمزشکنی ماشین Enigma توسط Turing، توسط چه نوع حملهای صورت پذیرفت؟

د) حمله نوع دوم ج) هيچكدام ب) حمله نوع اول الف) 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. طبق گفته شانون یک سامانه قوی ویژگی را دارد که به این معنا است ساختاری آماری رو حجم وسیعی از پراکنده است.

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

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

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 می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمز کردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمز کردن و بعد فشرده سازی

پاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام میخورد، بعد فشرده سازی و بعد عملیات رمزگذاری.

9. 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)

10 (د) 70 ج) 7 ج) 34 الف)

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

٧. تعداد ريشه اوليه عدد 60 كدام گزينه است؟

$$8$$
 (د) 6 (ج) 4 (ب) 2 الف) 2

پاسخ: این عدد ریشه اولیه ندارد.

هنده ها نشریحی) پاسخ: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: a سوال تشریحی) پاسخ: a این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a 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 (80) ϕ را محاسبه کنید؟ (سوال تشریحی) **پاسخ:** برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل نمره ندارد.
- ۱۰. در SSH چگونه از حمله تغییر قابلیتهای مشتری نظیر الگوریتههای 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: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

١١. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.

- الف امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه اطلاعاتی در مورد متن اصلی یی 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 p=pq باشد، آن گاه (p-1)(q-1) ((p-1)(q-1) باشد، آن گاه (p-1)(q-1) باشد، آن گاه روز در کلاس توضیح داده شد.

 3^{90} وقم آخر عدد 3^{90} چند است?

الف) 9 ج) 7 د) 6

پاسخ: 🕰 دقت کنید که در واقع ما به دنبال پاسخ (mod 10) 3^{90} هستم. میدانیم که:

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

🗀 آنگاه براحتی میتوانیم بنویسیم که:

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

۱۴. كدام گزينه صحيح است؟ (شايد چند مورد صحيح باشد)

- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با رتباط، برابر برای برقراری ارتباط، برابر با تعداد کلید در الگوریتمهای نامتقارن بین n
 - د) هیچکدام از گزینهها صحیح نیست

پاسخ: هیچ کدام 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 می دهد.
 - توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.

از سوی دیگر، 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 راه حل نمره ندارد.

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

- الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه اطلاعاتی در مورد متن اصلی پی ببرد.

پاسخ: در یک سامانه رمزگذاری، ما به صورت عمدی می خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینه ها صحیح است.

١٧. كدام گزينه صحيح است؟ (شايد چند گزينه 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.

، گزینههای فوق ریشه اولیه دارند.	بنابراین همه $\{1,2,4,p^k,2 imes p^k\}$	اعداد این مجموعه ریشه اولیه دارند.	پاسخ: اثبات میشود که فقط
			۱۰. طول واقعی کلید DES برابر اس
۳۲ (۵	ج) ۶۴	ب) ۵۶	الف) ۴۸
		راشد.	پاسخ: گزینهی "۵۶" صحیح ه
	. صو، ت بذر فت؟	ییبست. سط Turing، توسط چه نوع حملهای	
	. –		
د) حمله نوع اول	ج) حمله نوع سوم	ب) هیچکدام	الف) حمله نوع دوم
Known Plaintext)، رمزشکنی ماشین	ک یا چند متن اصلی معلوم (Attack	نه حمله نوع دوم یا حمله بر اساس یک	پاسخ: دو مثال مشهور، در زمی
است.	خشی از متن متن اصلی معلوم بوده ا) نسل دو (GSM) است. در هر دو، ب	Enigma و A5/2 در شبکههای
	غلط است؟	One Tim پیشنهادی توسط شانون،	۲. کدام گزینه در مورد رمز e Pad
		بر با طول متن اصلی باشد.	الف) طول کلید میبایست برا
			ب) کلید باید به صورت کاملا
		XOR دنباله متن اصلی با کلید است	
		از به یک زمان بسیار طولانی و پردازن	
الگوریتم، بر این اصل استوار است که هر	داریم به اندازه طول متن اصلی. این) یک دنباله کلید (Key Sequence)	پاسخ: در رمز One Time Pad
دنباله كليد واقعا تصادفي استفاده شود،	ت با یکدیگر XOR شود). اگر از یک	تر از کلید ترکیب میشود (بیت به بی	کاراکتر متن اصلی با یک کاراک
چنین سامانهای ویژگی امنیت بدون شرط	متن اصلی ندارد. از دیدگاه شانون، -	فی» خواهد بود، که هیچ ارتباطی با	نتیجه یک متن رمز واقعاً «تصاد
	Eavesdro)، برای گیرنده ارسال کرد	متن رمز را بدون خطر شنود (pping	را دارد. بدینسان میتوان این
ند.	رمز کند و برای Bob ارسال ک	ی Bob امضا کند، میبایست آن را با	۲۱. برای این که Alice پیامی را برای
د) کلید محرمانه Alice	ج) کلید عمومی Alice	ب) كليد محرمانه Bob	الف) كليد عمومي Bob
	رده و برای Bob ارسال م <i>ی ک</i> ند.	را با کلید خصوصی خودش رمز ک m	پاسخ: Alice برای امضا، پیام
توضيح دهيد؟ (سوال تشريحي) پاسخ:	، تولید کلید عمومی و خصوصی را نیز	را در RSA توضیح دهید؟ حتما روند n	n روند امضای یک پیام به مانند.
			پاسخ این سوال در اسلایدها ا
ن.	رمز کند و برای Bob ارسال کند	ی Bob رمز کند، میبایست آن را با	۲۱. برای این که Alice پیامی را براج
د) کلید محرمانه Alice	ج) کلید عمومی Alice	ب) کلید عمومی Bob	الف) كليد محرمانه Bob
	ه و برای او ارسال می کند.	یام m را با کلید عمومی Bob رمز کرد	پاسخ: Alice برای رمزکردن، پ
ه شد)		علیبابا که در کلاس مطرح شد، صح	
ای غیرتعاملی است.	ب) یک مساله از نوع روشھ	انایی صفر است.	الف) یک مساله از نوع اثبات د
	د) یک مساله تسهیم راز اس		ج) همه گزینهها صحیح اس
	ِ صفر است.	است: یک مساله از نوع اثبات دانای _ح	
		ه هر بین از متن باید به چندین	
			٠٠٠ رير کي ٠٠٠

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

ج) 27

د) 6

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

2 (ب

الف) 25

	ب) انتشار - رمز - کلید د) انتشار - آشکار - متن رمز		الف) گمراه کنندگی - آشکار - ج) گمراه کنندگی - رمز - ک
	المسار السار المسار المسارير	سید ی - رمز - کلید" صحیح میباشد.	
			۲۷. PGP امنیت را در کدام لایه برا
د) لايه انتقال	ج) لايه پيوند داده	ب) لايه شبكه	الف) لايه كاربرد
		د (Application Layer) است.	پاسخ: گزینه صحیح لایه کاربر
.ت.	پاسخ: پاسخ این سوال در اسلایدها اس	ین را توضیح دهید؟ (سوال تشریحی)	۲۸. پروتکل توافق کلید دیفی-هلم
خواهد شد؟	همان کلید محرمانه برابر با کدام گزینه	و مقدار $e=5$ باشد، آن گاه d یا $n=5$	۲۹. اگر در الگوریتم RSA مقدار 35
د) 3	ج) 5	4 (ب	الف) 6
بریم، به گونهای که	را به عنوان کلید عمومی در نظر می گه e	است. همان طور که میدانید، پارامتر	پاسخ: گزینه صحیح عدد پنج
	$1 < e < \phi(n), (\epsilon$	$e, \phi(n)) = 1.$	
		مانه در نظر می گیریم، به گونهای که:	پارامتر d را به عنوان کلید محر
	$ed \equiv 1 \pmod{4}$	$\downarrow \phi(n)),$	
بمانه 24 را محاسبه کنیم که برابر با 5	ىد. سپس بايد معكوس عدد $e=5$ در پ	کنیم که برابر با $\phi(35)=24$ خواهد ش	$\phi(n)$ پس ابتدا $\phi(n)$ را محاسبه می خواهد شد.
	ه طور دقیق).	عث غیر خطی شدن سامانه میشود(ب	 كدام قسمت الگوريتم DES با
F (s	E (ج	S (ب	الف) P
		.باشد.	پاسخ: گزینهی "S" صحیح م _ح

شماره برگ	تاريخ	نام درس	شماره دانشجویی	نام و نام خانوادگی
۶٠	14.4/.7/11	امنیت سیستمهای کامپیوتری		
				اد ریشه اولیه عدد 60 کدام

. for a file and the second field of

پاسخ: این عدد ریشه اولیه ندارد.

- ۲. پروتکل توافق کلید دیفی-هلمن را توضیح دهید؟ (سوال تشریحی) پاسخ: پاسخ این سوال در اسلایدها است.
 - ٣. كدام گزينه صحيح است؟ (شايد چند مورد صحيح باشد)
- الف) توافق كليد (Key Agreement): يك سمت كليد را توليد كرده و در اختيار طرف مقابل نيز قرار مي دهد.
 - ب) برقراری کلید (Key Establishment): هر دو سمت، در فرایند تولید کلید مشارکت می کنند.
 - $\binom{n}{2}$ برابر با روزاری ارتباط، برابر با نفر برای برقراری ارتباط، برابر با روزاری ارتباط، برابر با
 - د) هیچکدام از گزینهها صحیح نیست

پاسخ: هیچ کدام 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 می کنند.

از سوی دیگر، 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 ج) 7 ج) 17

پاسخ: اگر $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ مجموع کاهشیافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $ar_1, ar_2, \dots, ar_{\phi(n)}$

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

الف) هيچكدام 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. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.
- 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.

یاسخ:

- 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 حمله گر 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: خدمت گزار از همان تابع استفاده می کند، و با استفاده از ورودی های زیر مقدار چکیده پیام را درست می کند:

- 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 این که این چکیده تولید شد، خدمت گزار آن را با کلید عمومی خودش امضا می کند.

- ۸. کدام گزینه در مورد رمز One Time Pad پیشنهادی توسط شانون، غلط است؟
 - الف) طول كليد مي بايست برابر با طول متن اصلى باشد.
 - ب) کلید باید به صورت کاملا تصادفی تولید شود.
 - ج) دنباله متن رمز حاصل از XOR دنباله متن اصلى با كليد 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 می شود (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 سامانه ای ویژگی امنیت بدون شرط را دارد. بدین سان می توان این متن رمز را بدون خطر شنود (Eavesdropping)، برای گیرنده ارسال کرد.

- ٩. كدام گزينه صحيح است؟ (شايد چند گزينه 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.
- **یاسخ:** 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 راه حل نمره ندارد.
 - ۱۱. کدام گزینه در مورد مساله غار علی بابا که در کلاس مطرح شد، صحیح است؟ (این مورد امروز درس داده شد)
 - ب) یک مساله از نوع اثبات دانایی صفر است.

الف) همه گزینهها صحیح است.

د) یک مساله از نوع روشهای غیرتعاملی است.

ج) یک مساله تسهیم راز 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 می شود بعد فشرده سازی و بعد امضا
- ب) در PGP اول عملیات فشرده سازی انجام می شود بعد رمزنگاری و بعد امضا
- ج) در PGP اول عملیات امضا انجام می شود بعد فشرده سازی و بعد رمزکردن
- د) در PGP اول عملیات امضا انجام می شود بعد رمزکردن و بعد فشرده سازی

یاسخ: همان طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می خورد، بعد فشرده سازی 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. كدام شرط در مورد RSA الزامي است؟

n متن اصلی باید نسبت به n اول باشد.

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

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

ج) کلید عمومی باید نسبت به n اول باشد.

پاسخ: پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونهای که

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

۱۵. طول واقعی کلید DES برابر است با

الف) ۶۴ (ح ج) ۳۲ (د) ۳۲ (۲ الف) ۳۲ (۱ الف) ۳

پاسخ: گزینهی "۵۶" صحیح میباشد.

۱۶. برای این که Alice پیامی را برای Bob امضا کند، می بایست آن را با رمز کند و برای Bob ارسال کند.

الف) كليد محرمانه Alice ب) كليد محرمانه Bob ج) كليد عمومي Bob د) كليد عمومي

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

۱۷. اثبات کنید که اگر p=pq باشد، آن گاه (p-1)(q-1) ((p-1)(q-1) باشد، آن گاه (p-1)(q-1) باشد، آن گاه و باشد، آن گاه و

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

الف) هيچكدام 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 بالف) گمراه کنندگی - رمز - کلید بالتشار - رمز - رم

ياسخ: گزينهي "گمراه كنندگي - رمز - كليد" صحيح مي باشد.

در این قضیه را اثبات کنید: اگر دو عدد a و a نسبت به همدیگر اول باشند، آنگاه خواهیم داشت: $a^{\phi(n)} = 1 \mod n$ (سوال تشریحی) پاسخ: اگر دو عدد a در مجموعه کاهش یافته مانده ها باشد، آنگاه مجموعه حاصل شده از ضرب عدد a در مجموعه کاهش یافته مانده ها یعنی a در مجموعه کاهش یافته مانده ها باشد، آنگاه 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 این که Alice پیامی را برای Bob رمز کند، میبایست آن را با رمز کند و برای Bob ارسال کند.

د) کلید عمومی Bob ج) كليد محرمانه Bob ب) کلید عمومی Alice الف) كليد محرمانه Alice پاسخ: Alice برای رمزکردن، پیام m را با کلید عمومی Bob رمز کرده و برای او ارسال می کند. ۲۲. کدام گزینه صحیح نیست؟ (می توانید چند گزینه را انتخاب کنید). الف) امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند. 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. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه اطلاعاتی در مورد متن اصلی پی ببرد. پاسخ: در یک سامانه رمزگذاری، ما بهصورت عمدی می خواهیم یک نویز به متن اصلی اضافه کنیم. مابقی گزینهها صحیح است. 3^{90} يرقم آخر عدد 3^{90} چند است? ج) 9 ب) 7 د) 8 الف) 6 پاسخ: 🛍 دقت کنید که در واقع ما به دنبال پاسخ (10 3^{90} هستم. میدانیم که: ullet بعنی چهار عدد مثبت وجود دارد که کمتر از 0 است و نسبت به آن اول هست. $\phi(10)=4$ (3,10) = 1 عدد سه و ده نسبت به هم اول هستند، یعنی $3^4 = 1 \pmod{10}$ برطبق قضیه اویلر-فرما داریم: • 🛍 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 می آورد؟ د) لايه كاربرد ب) لايه شبكه الف) لايه انتقال ج) لايه پيوند داده ياسخ: گزينه صحيح لايه كاربرد (Application Layer) است. ٢٥. كدام قسمت الگوريتم DES باعث غير خطى شدن سامانه مي شود (به طور دقيق). P (ج S (ب د) E الف) F **یاسخ:** گزینهی "S" صحیح میباشد.

۲۶. مقدار (80) ϕ را محاسبه کنید؟ (سوال تشریحی) پاسخ: برابر با ۳۲ می شود. جواب آخر ملاک است، هر کس پاسخ درستی نوشته باشد قابل قبول است و راه حل 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؟

پاسخ: گزینه صحیح عدد پنج است. همان طور که می دانید، پارامتر e را به عنوان کلید عمومی در نظر می گیریم، به گونه ای که

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

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

5 پس ابتدا $\phi(n)$ را محاسبه می کنیم که برابر با $\phi(35)=\phi(35)=\phi(35)=0$ خواهد شد. سپس باید معکوس عدد e=5 در پیمانه $\phi(n)$ محاسبه کنیم که برابر با خواهد شد.

۲۸. كدام يك از جملات زير صحيح است و كدام غلط؟ لطفا جلوى آن عبارت صحيح /غلط را بنويسيد.

- الف امنیت بدون شرط (UnconditionalSecurity) یعنی در صورتی که علی رغم توان زیاد محاسباتی دشمن، نتواند بر اساس متن رمز شده سیستم را بشکند، چرا که هیچ گونه اطلاعاتی از متن اصلی توسط متن رمز درز نمی کند.
- 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 می خواهیم یک نویز به متن اصلی اضافه کنیم. حمله گر در صورت مشاهده متن رمز، نباید به هیچ گونه 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)

2 (د) 25 (ج) 25 (ج) 27 (الف)

یاسخ: اثبات می شود 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 بانتشار - متن آشکار - متن رمز شده

ج) گمراه کنندگی - متن رمز شده - متن آشکار دارنجی است و متن آشکار - متن رمز شده

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