

نام و نام خانوادگی	شماره دانشجویی	نام درس	تاریخ	شماره برگه
		امنیت سیستم‌های کامپیوتری	۱۴۰۱/۰۹/۲۷	۱

نکات



الف) این امتحان نمره منفی دارد.

ب) دقت کنید که نام و نام خانوادگی خود را بر روی تمامی برگه‌ها بنویسید.

۱. در SSH چگونه از حمله تغییر قابلیت‌های مشتری نظیر الگوریتم‌های رمزنگاری مورد پشتیبانی جلوگیری می‌شود؟
پاسخ: خدمت‌گزار از همان تابع استفاده می‌کند، و با استفاده از ورودی‌های زیر مقدار چکیده پیام را درست می‌کند:

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

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

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

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

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

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

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

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

۴. تفاوت Transport Mode و Tunnel Mode را بیان کنید؟ (سوال تشریحی)

۵. کدام شرط در مورد RSA الزامی است؟

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

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

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



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

پاسخ: اثبات می‌شود که فقط اعداد این مجموعه ریشه اولیه دارند. $\{1, 2, 4, p^k, 2 \times p^k\}$. بنابراین همه گزینه‌های فوق ریشه اولیه دارند.
۷. تعداد ریشه اولیه عدد 30 کدام گزینه است؟

پاسخ: تعداد ریشه‌های اولیه عدد n برابر با $\phi(\phi(n))$ است. پس خواهیم داشت:

$$\phi(\phi(30)) = \phi(8) = 4$$

۸. رقم آخر عدد 3^{90} چند است؟

پاسخ:  دقت کنید که در واقع ما به دنبال پاسخ $3^{90} \pmod{10}$ هستیم. می‌دانیم که:
 • $\phi(10) = 4$. یعنی چهار عدد مثبت وجود دارد که کمتر از 10 است و نسبت به آن اول هست.
 • عدد سه و ده نسبت به هم اول هستند، یعنی $(3, 10) = 1$
 • برطبق قضیه اویلر-فرما داریم: $3^4 = 1 \pmod{10}$
 آن‌گاه براحتی می‌توانیم بنویسیم که:

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

۹. کدام گزینه در مورد PGP صحیح است؟

الف) در PGP اول عملیات رمزنگاری انجام می‌شود بعد فشرده‌سازی و بعد امضا
 ب) در PGP اول عملیات فشرده‌سازی انجام می‌شود بعد رمزنگاری و بعد امضا
 ج) در PGP اول عملیات امضا انجام می‌شود بعد فشرده‌سازی و بعد رمزکردن
 د) در PGP اول عملیات امضا انجام می‌شود بعد رمزکردن و بعد فشرده‌سازی
 پاسخ: همان‌طور که در کلاس نیز مطرح شد، در PGP اول یک امضای دیجیتال بر روی پیام می‌خورد، بعد فشرده‌سازی و بعد عملیات رمزگذاری.

۱۰. جای خالی را پر کنید:

الف) ثبت‌نام، تایید هویت و تخصیص شناسه به کاربر در PKI، برعهده است.
 ب) وظیفه تولید کلید عمومی و خصوصی و تولید گواهینامه در PKI، برعهده است.
 ج) مسوولیت اعتبارسنجی گواهینامه‌ها در PKI، برعهده است.
 د) کاربران انسانی، ماشین و هر شی‌ای که بتواند از گواهینامه (Certificate) بهره‌برد، نام دارد.

۱۱. اثبات کنید که اگر $n = pq$ باشد که p و q دو عدد اول باشند، در این صورت داریم: $\phi(n) = (p-1)(q-1)$ (سوال تشریحی)

۱۲. مرورگرها برای مدیریت ابطال گواهینامه از چه روش‌هایی استفاده می‌کنند؟ برای Chrome و Firefox توضیح دهید؟ (سوال تشریحی)

۱۳. ایده شامیر برای تسهیم راز (Secret Sharing) را بیان کنید؟ (سوال تشریحی)

۱۴. تفاوت AH (Authentication Header) و ESP (Encapsulating Security Payload) در IPSec را بیان کنید (سوال تشریحی)

۱۵. کدام گزینه در مورد محرمانگی پیش‌رو و محرمانگی پس‌رو صحیح نیست؟ (دو گزینه را باید انتخاب کنید)

الف) محرمانگی پیش‌رو یعنی اگر کاربر به سامانه وارد شد، داده‌های گذشته لو نرود.

ب) محرمانگی پیش‌رو زمانی کاربر سامانه را ترک کرد، داده‌های در آینده لو نرود.

ج) محرمانگی پس‌رو یعنی اگر کاربر به سامانه وارد شد، داده‌های گذشته لو نرود.

د) محرمانگی پس‌رو زمانی کاربر سامانه را ترک کرد، داده‌های در آینده لو نرود.

پاسخ: محرمانگی پس‌رو: اگر کاربر به سامانه وارد شد، داده‌های گذشته لو نرود. محرمانگی پیش‌رو: زمانی کاربر سامانه را ترک کرد، داده‌های در آینده لو نرود.

۱۶. 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) 4

ج) 3

د) 5

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

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

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

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

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

۱۷. کدام گزینه در مورد مساله غار علی‌بابا که در کلاس مطرح شد، صحیح است؟

الف) یک مساله از نوع روش‌های غیرتعاملی است.

ب) همه گزینه‌ها صحیح است.

ج) یک مساله از نوع اثبات دانایی صفر است.

د) یک مساله تسهیم راز است.

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

۱۸. اعضای مجموعه \mathbb{Z}_{13}^* را در کدام عدد ضرب کنیم تا مجموعه جدید یک جایگشت از مجموعه اصلی باشد؟ (ممکن است چند گزینه صحیح باشد)

الف) 26

ب) 7

ج) 13

د) 10

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 a در مجموعه کاهش‌یافته

مانده‌ها یعنی $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ یک جایگشت کامل از مجموعه اولیه است، اگر $(a, n) = 1$ باشد. پس پاسخ اعداد 10 و 7 است.

۱۹. 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 Alice

د) کلید عمومی Bob

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

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

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

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

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

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

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

۲۱. کدام یک از گزینه‌های زیر جزو شروط داشتن یک شبکه امن نمی‌باشد؟

Encryption (الف) Integrity (ب) Authentication (ج) Freshness (د)

پاسخ: گزینه‌ی "Authentication" صحیح می‌باشد.

۲۲. مسئولیت اعتبارسنجی گواهینامه بر عهده کیست؟

RA (الف) VA (ب) End-Entity (ج) CA (د)

پاسخ: گزینه‌ی "VA" صحیح می‌باشد.

۲۳. برای امضای دیجیتال هنوز از استفاده می‌شود.

RSA (الف) AES (ب) SSL (ج) DES (د)

پاسخ: گزینه‌ی "RSA" صحیح می‌باشد.

۲۴. در صورتی که Bob از مرجع صدور گواهی نامه Z و Alice از مرجع صدور گواهی نامه W گواهی نامه‌های خود را اخذ کرده باشند. Bob می‌تواند از زنجیره‌ای از گواهی نامه‌ها برای بدست آوردن کلید عمومی Alice استفاده کند. کدام گزینه زنجیره‌ی صحیح را به ترتیب نشان می‌دهد.

W Z Z Aice (الف) Z Z W Bob (ب) Z W W Bob (ج) Z W W Alice (د)

پاسخ: گزینه‌ی "Z W W Alice" صحیح می‌باشد.

۲۵. کدام عنصر زیر در گواهینامه X.۵۰۹ اختیاری است؟

Certificate Signature (الف) Validity (ب) Version (ج) Extensions (د)

پاسخ: گزینه‌ی "Extensions" صحیح می‌باشد.

۲۶. در الگوریتم‌های کلید نامتقارن، کلید عمومی و خصوصی به ترتیب در اختیار چه کسانی است؟

الف) فرستنده و گیرنده - گیرنده
ب) فرستنده - فرستنده و گیرنده
ج) اعلان عمومی - گیرنده
د) گیرنده - اعلان عمومی

پاسخ: گزینه‌ی "اعلان عمومی - گیرنده" صحیح می‌باشد.

۲۷. کدام گزینه بیانگر یک چارچوب متشکل از سخت افزارها، نرم افزارها، سیاست‌ها، استانداردها و دستورالعمل‌هایی برای مدیریت کلید عمومی، مدیریت شناسه، تولید، توزیع، ذخیره سازی، ابطال و مدیریت گواهینامه می‌باشد؟

Rest Framework (الف) World Wide Web (ب)
Public-Key Infrastructure (ج) Web of Trust (د)

پاسخ: گزینه‌ی "Public-Key Infrastructure" صحیح می‌باشد.

۲۸. پروتوکل توافقی دیفی هلمن بر اساس کدام گزینه طراحی شده است؟

الف) مساله لگاریتم پیوسته
ب) مساله لگاریتم گسسته
ج) مساله تجزیه اعداد اول
د) مساله ریشه اولیه

پاسخ: گزینه‌ی "مساله لگاریتم گسسته" صحیح می‌باشد.

۲۹. کدام گزینه‌ی زیر صحیح نمی‌باشد؟

الف) امنیت الگوریتم‌های کلید متقارن و نامتقارن، مبتنی بر مسائل نظریه اعداد است.

ب) در الگوریتم کلید متقارن نیاز به کانال امن نداریم اما در الگوریتم کلید نامتقارن وجود یک کانال امن واجب است.

ج) از نظر سرعت عمل، الگوریتم کلید متقارن بهتر از الگوریتم کلید نامتقارن عمل می‌کند.

د) الگوریتم کلید نامتقارن نقش مکمل برای الگوریتم کلید متقارن در توزیع کلید را دارد.

پاسخ: گزینه‌ی "در الگوریتم کلید متقارن نیاز به کانال امن نداریم اما در الگوریتم کلید نامتقارن وجود یک کانال امن واجب است." صحیح می‌باشد.

۳۰. Bob قصد دارد توسط الگوریتم لید، RSA عمومی و خصوصی خودش را تولید کند. در صورتی که مقدار متن رمز شده (Ciphertext) برابر ۲۰، مقدار n برابر ۱۶۱ و کلید عمومی برابر ۹۷ باشد، مقدار کلید خصوصی را بدست آورید

۳۵ (د)

۴۲ (ج)

۴۹ (ب)

۳۷ (الف)

پاسخ: گزینه‌ی "۴۹" صحیح می‌باشد.

