نام و نام خانوادگی	شماره دانشجویی	نام درس	تاریخ	شماره برگه
		امنیت سیستم‌های کامپیوتری	۱۴۰۱/۰۷/۲۴	۱

نکات

الف) این امتحان نمره منفی دارد.

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

ج) در تمام سوالات، فرض کنید که شماره‌گذاری حروف از صفر شروع می‌شود یعنی حرف A شماره صفر و حرف B شماره یک و ...

۱. اگر در یک الگوریتم رمزگذاری رمز جانشینی تک‌الفبایی و تک‌حرفی با نگاشت کلی، بتوانیم با روش‌های تحلیل فرکانسی، پنج حرف را به درستی حدس بزنیم، با یک کامپیوتر 100 petaFLOPS چقدر طول می‌کشد تا به صورت Brute-force این الگوریتم را بشکنیم؟

الف) 0.83 دقیقه ب) 830 دقیقه ج) 83 دقیقه د) 8.3 دقیقه

پاسخ: اگر یک کامپیوتر با قدرت 100 petaFLOPS در اختیار داشته باشیم، انتظار داریم در هر ثانیه این کامپیوتر برای ما 10^{17} حالت را چک کند. از سوی‌دیگر، برای رمز جانشینی از نوع تک‌الفبایی و تک‌حرفی، در صورتی که یک نگاشت کلی را در نظر بگیریم، فضای کلید برابر با $26!$ خواهد شد. به علت این‌که پنج حرف را متوجه شدیم، فضای کلید $26!$ به $21!$ کاهش پیدا می‌کند. پس در نهایت خواهیم داشت:

$$|\mathcal{K}| = 21! \approx 5 \times 10^{19}$$

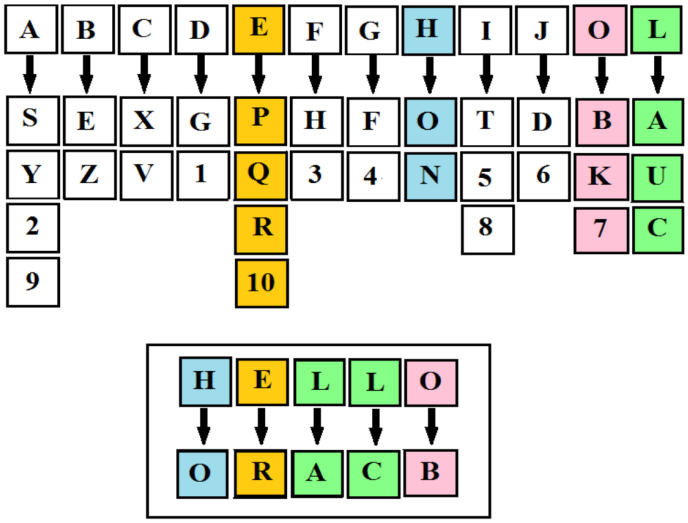
$$\text{Time} = \frac{5 \times 10^{19}}{10^{17}} = 5 \times 10^{2} \text{ [Sec]} \approx 8.3 \text{ [Min]}$$

۲. فرض کنید یک هکر در یک صفحه Login به جای نام کاربری، عبارت Ehsan' ;DROP TABLE users; -- را وارد می‌کند. در صورتی‌که ما در سمت Back-end درست عمل نکرده باشیم، این‌کار موجب پاک شدن کل اطلاعات ورود کاربران خواهد شد؟

الف) حمله Phishing ب) حمله Packet sniffer ج) حمله SQL Injection د) حمله Rootkit

پاسخ: برطبق اسلایدهای فصل اول، مثالی که زده شد، نمونه‌ای از یک حمله SQL Injection است. این حمله، روشی است که به هکرها این اجازه را می‌دهد که از طریق حفره‌های امنیتی موجود در پایگاه داده (Database)، به سامانه نفوذ کند.

۳. شکل زیر نشانگر چه نوع رمزگذاری در بین سامانه‌های رمزگذاری کلاسیک است؟



الف) رمز جایگشتی
ب) رمز جانشینی-چندالفبایی
ج) رمز جانشینی-تک‌الفبایی-تک‌حرفی
د) رمز جانشینی-تک‌الفبایی-چندحرفی

پاسخ: شکل یاد شده بیانگر رمز جانشینی از نوع چند الفبایی است.

۴. کدام گزینه صحیح است؟ (می‌توانید چند گزینه را انتخاب کنید)

الف) یکپارچگی داده یعنی اطمینان از قابل تغییر بودن اطلاعات و برنامه‌ها فقط به صورت مشخص و مجاز
ب) یکپارچگی سامانه یعنی اطمینان از انجام عملیات سامانه به صورت عادی، عاری از دستکاری غیرعمدی و غیرمجاز
ج) دسترس‌پذیری (Availability) یعنی اطمینان از عملکرد بی‌درنگ سامانه و عدم رد خدمات برای کاربران مجاز
د) مسئولیت‌پذیری (Accountability) یعنی عملیات کاربر قابل رهگیری باشد.

پاسخ: همه موارد برطبق اسلایدها صحیح است.

۵. هکرهای ……، به مبارزه با هکرهای کلاه سیاه می‌پردازند، ولی در این مبارزه هیچ مرز اخلاقی را رعایت نمی‌کنند، و بی رحمانه و به قصد نابودی به هکرهای کلاه سیاه حمله می‌کنند.

الف) کلاه صورتی
ب) کلاه خاکستری
ج) کلاه سفید
د) کلاه قرمز

پاسخ: کلاه قرمز: به نوعی شبیه هکرهای کلاه خاکستری یا حتی کلاه سفید هستند. آن‌ها به نوعی به مبارزه با هکرهای کلاه سیاه می‌پردازند، ولی در این مبارزه هیچ مرز اخلاقی را رعایت نمی‌کنند. آن‌ها بیرحمانه به هکرهای کلاه سیاه حمله می‌کنند و به نوعی قصد نابودی آن‌ها را دارند.

۶. کدام گزینه در مورد ماشین Enigma اشتباه است؟

الف) تا هفت بار عملیات جانشینی در چرخ‌دنده‌ها صورت می‌پذیرفت.
ب) در صورتی‌که فرض کنیم، آلمان‌ها در Plugboard از ده سیم استفاده می‌کردند، تعداد حالت‌های Plugboard برابر با $\frac{26!}{6!2^{10}10!}$ می‌شود.
ج) کلید در بخش چرخ‌دنده‌ها می‌تواند، فضایی برابر با $P_3^5 \times 26^3$ داشته باشد.
د) همه موارد صحیح است.

پاسخ: همه موارد یاد شده صحیح است.

۷. فضای کلید (Key Space) یک رمز جانشینی تک‌الفبایی و تک‌حرفی با نگاشت کلی کدام گزینه است؟

الف) 2^{26}
ب) $\log_2((26 \times 26)!)$
ج) $26!$
د) $(26 \times 26)!$

پاسخ: برای رمز جانشینی از نوع تک‌الفبایی و تک‌حرفی، در صورتی که یک نگاشت کلی را در نظر بگیریم، فضای کلید برابر با !26 خواهد شد. چراکه حرف اول یعنی A می‌تواند به ۲۶ حرف دیگر و حرف B می‌تواند به ۲۵ حرف دیگر نگاشت شود و همین روند را می‌توان تا آخرین حرف ادامه داد.

۸. رمز Vigenère در چه دسته‌ای از طبقه‌بندی روش‌های رمزگذاری کلاسیک قرار می‌گیرد؟

الف) رمز جایگشتی - تک‌الفبایی - تک‌حرفی
ب) رمز جانشینی - تک‌الفبایی - تک‌حرفی
ج) رمز جانشینی - چندالفبایی
د) رمز جایگشتی - چندالفبایی

پاسخ: در رمز Vigenère به مانند ماشین Enigma، هر حرف با یک حرف دیگر جایگزین می‌شود. اما نگاشت هر حرف به حرف دیگر، در طول عملیات رمزگذاری تغییر می‌کرد، بدین‌سان این ماشین در طبقه رمز جانشینی (Substitution Cipher) - چندالفبایی (Polyalphabetic) جای می‌گیرد.

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

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

پاسخ:

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

۱۰. کدام گزینه مرجع این درس و منبع کنکوری این درس محسوب می‌شود؟

الف) Stallings, William. Cryptography and network security: principles and practice. India, Pearson, 2022
ب) Stallings, William, Brown, Lawrie. Computer Security: Principles and Practice. India, Pearson, 2014
ج) Stallings, William. Network Security Essentials: Applications and Standards. Prentice Hall, 2007
د) Behrouz A. Forouzan. Introduction to Cryptography and Network Security. McGraw-Hill Higher Education, 2008

پاسخ: برطبق اسلایدها مرجع اصلی درسی کتاب Cryptography and network security: principles and practic آقای Stallings است.

۱۱. پیشتر در درس با یک رمز ساده رمز جایگشتی (Transposition Cipher) آشنا شدیم، که در آن متن به صورت سطری نوشته می‌شد و به صورت ستونی خوانده می‌شد. اکنون فرض کنید عبارت habitue به عنوان کلید انتخاب شده است. این بدان معنا است که تعداد ستون‌ها برابر با هفت است و همچنین ترتیب خواندن ستون‌ها نیز بر حسب جایگاه حروف است. مثلا در همین عبارت انتخاب شده به عنوان کلید، چون حرف A اولین حرف در ترتیب حروف الفبا است، ابتدا می‌بایست ستون دوم خوانده می‌شود. چون حرف بعدی از لحاظ ترتیب الفبایی حرف B است، بدین‌سان ستون سوم در مرحله دوم باید خوانده شود و همین روند را تا انتها باید ادامه داد. با این توضیحات، کدام گزینه متن رمز معادل عبارت Security protects confidentiality است؟

الف) EPSETCRCNYTCILSYTDIUOOTRTNIIEFA
ب) SYTDIETSETCRCNOUYOTRTNIIEFAPCIL
ج) SYTDIEPSETCRCNYUOOTRTNIIEFATCIL
د) EPSETTCILLSYTDICRCNYIEFARTNIUOOT

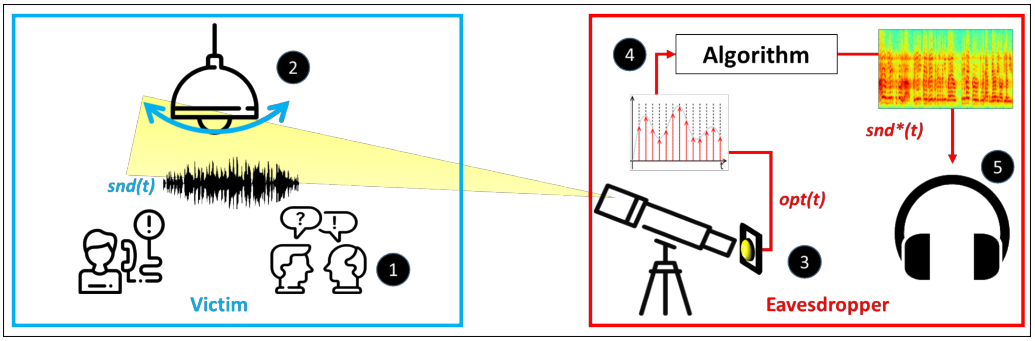
پاسخ: تصویر زیر به اندازه کافی گویای پاسخ مساله است.

Plaintext: Security protects confidentiality

H	A	B	I	T	U	E
4	1	2	5	6	7	3
S	E	C	U	R	I	T
Y	P	R	O	T	E	C
T	S	C	O	N	F	I
D	E	N	T	I	A	L
I	T	Y				

Ciphertext: EPSETCRCNYTCILSYTDIUOOTRTNIIEFA

۱۲. کدام گزینه به خوبی شکل زیر را توصیف می‌کند؟



الف) Visual Microphone ب) Remote microphone ج) Laser microphone د) Lamphone

پاسخ: ایده Lamphone در کنفرانس Blackhat 2020 برای نخستین بار مطرح گشت. سعی شده است که ایده‌ای مطرح شود که بتوان به صورت بی‌درنگ (Realtime) و بدون آشکارشدن حمله، حمله شنود را انجام داد. در این ایده که مطالعه جزئیات آن را به عهده خواننده گذاشته می‌شود، از تاثیر ارتعاش لامپ‌های نصب شده در اتاق قربانی، و همچنین واکنش نور لامپ به این ارتعاش، بهره گرفته شده تا بتوان یک حمله شنود موفق را انجام داد.

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

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

ب) کلید باید به صورت کاملا تصادفی تولید شود.

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

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

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

۱۴. کدام گزینه جزو ویژگی‌های امنیتی یک سامانه محسوب نمی‌شود؟

الف) مسئولیت‌پذیری (Accountability) ب) کارایی (Performance)

ج) سندیت (Authenticity) د) دسترس‌پذیری (Availability)

پاسخ: برطبق تعریف امنیت گزینه کارایی (Performance)، گزینه صحیح است.

۱۵. فرض کنید که ما از رمز مُستَوی استفاده کردیم برای عملیات رمزگذاری ($\mathrm{E}_k(m) = 7m + 3$). اگر یک حرف متن رمز به صورت D باشد، حرف متن اصلی متناظر آن چیست؟

الف) A　　ب) Y　　ج) X　　د) B

پاسخ: نکته مهم این سوال این بود که به ما تابع رمزگذاری را دادند یعنی تابع $\mathrm{E}_k(m) = 7m + 3 \mod 26$. برای بدست‌آوردن متن اصلی متناظر یک متن رمز، ما نیاز به تابع رمزگشایی داریم که عکس تابع رمزگذاری است. به صورت سعی‌وخطایی می‌توانید این تابع را بدست آوردید، اما بعدها در همین درس نحوه بدست آوردن آن گفته خواهد شد. در نهایت برای تابع رمزگشایی خواهیم داشت:

$$\mathrm{E}_k(m) = 7m + 3 \mod 26 \quad \Longrightarrow \quad \mathrm{D}_k(c) = 7^{-1}(c - 3) = 15c + 7 \mod 26$$

کافی است در معادله فوق، شماره D یعنی سه را قرار دهید:

$$m = \mathrm{D}_k(3) = 15 \times 3 + 7 \mod 26 = 0$$

که معادل حرف A است.

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

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

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

۱۷. ماشین Enigma در چه دسته‌ای از طبقه‌بندی روش‌های رمزگذاری کلاسیک قرار می‌گیرد؟

الف) رمز جانشینی - تک‌الفبایی - تک‌حرفی　　ب) رمز جایگشتی - تک‌الفبایی - تک‌حرفی
ج) رمز جانشینی - چندالفبایی　　د) رمز جایگشتی - چندالفبایی

پاسخ: اگر به خاطر داشته‌باشید، در ماشین Enigma هر حرف با یک حرف دیگر جایگزین می‌شود. اما نگاشت هر حرف به حرف دیگر، در طول عملیات رمزگذاری تغییر می‌کرد، بدین‌سان این ماشین در طبقه رمز جانشینی (Substitution Cipher) - چندالفبایی (Polyalphabetic) جای می‌گیرد.

۱۸. می‌خواهیم عبارت THIS IS AN EXAMPLE را با استفاده از الگوریتم Vigenère رمز کنیم. اگر کلمه کلید HELLO باشد، متن رمز کدام گزینه است؟

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

الف) ALZW WZ EE ILHQGPS
ب) LHCW WK AH ILSMJPS
ج) ALTD WZ EY PLHQAWS
د) LHTS UK AY EJSMALQ

پاسخ: به عنوان مثال برای رمزکردن حرف اول کافی است که عنصر (T,H) را در جدول Vigenère پیدا کنیم که برابر خواهد شد با A. برای حرف دوم متن رمز باید (H,E) را پیدا کنیم، که خواهد شد L. با روش مشابه برای حرف سوم، باید به دنبال عنصر (I,L) بگردیم که در نهایت با حرف T مواجه خواهیم شد.

۱۹. کدام گزینه بیانگر، علم اصول و روش‌های رمزگذاری است؟

الف) رمزنگاری (Cryptography)
ب) رمزشناسی (Cryptology)
ج) تحلیل رمز (Cryptanalysis)
د) نهان‌سازی اطلاعات (Information Hiding)

پاسخ: علم اصول و روش‌های رمزگذاری را اصطلاحا رمزنگاری (Cryptography) می‌نامیم.

۲۰. Jeff Moss می خواست در سال ۱۹۹۳ یک مهمانی خداحافظی برای یکی از دوستانش ترتیب داده بود. گرچه به خاطر بروز مشکلی، مهمانی برگزار نشد، ولی او تصمیم گرفت که صد نفر از دوستانش که همگی هکر بودند را به لاس‌وگاس دعوت کند تا یک مهمانی جایگزین تشکیل دهند. این رویداد برای بسیاری از شرکت‌کنندگان بسیار جذاب و جالب بود. تقاضای برگزاری این مهمانی سال‌های بعد نیز تکرار شد، و از همین نقطه بود که ..... بوجود آمد. این همایش، سبک و سیاق کنفرانس‌های رسمی را ندارد، و عملا یک دورهمی بین هکرهای سرتاسر دنیا محسوب می‌شود.

الف) Positive Hack Days
ب) Hope
ج) BlackHat
د) Def Con

پاسخ: همایش Def Con

۲۱. برای رمز مُستَوی (Affine Cipher) طول کلید برابر با؟

الف) $\log_2(676)$
ب) $\log_2(312)$
ج) $\log_2(260)$
د) $\log_2(26!)$

پاسخ: رمز مُستَوی یک حالت کلی‌تر از رمز سِزار است. البته باید دقت کرد که در این نوع از رمزنگاری می بایست، مقادیر a و $n = 26$ باید نسبت به هم اول باشند. پس ما برای a تنها ۱۲ حالت بیشتر نمی توانیم داشته باشیم. برای b نیز ۲۶ حالت. پس در حالت کلی 12×26 حالت داریم. پس برای طول کلید خواهیم داشت:

$$L = \log_2(|\mathcal{K}|) = log_2(12 \times 26) = \log_2(312) \text{ [bit]}.$$

۲۲. فرض کنید قصد داریم بر روی یک اثر هنری دیجیتال، یک امضا قرار دهیم. به‌گونه‌ای که در صورتی که هرگونه تغییری در اثر صورت گیرد، امضا نابود شود. از سوی‌دیگر، امضا در نمای اثر تاثیری نگذارد. کدام گزینه در رسیدن به این هدف به شما کمک می‌کند؟

الف) نشان‌گذاری از نوع Invisible و شکننده
ب) نشان‌گذاری از نوع Invisible و غیرشکننده
ج) نشان‌گذاری از نوع Visible و غیرشکننده
د) نشان‌گذاری از نوع Visible و شکننده

پاسخ: چون در صورت سوال گفته شده است که یک امضا بر روی اثر می‌خواهیم و مهم نیست که کسی بفهمد که اثر امضا شده است یا خیر، پس باید به سراغ نشان‌گذاری (Watermarking) برویم. در ضمن می‌خواهیم که در صورت هرگونه تغییری در اثر، امضا به طور کامل نابود شود و این یعنی باید نشان‌گذاری ما از نوع شکننده باشد. در ضمن قرار است نمای اثر را خراب نکند، پس از نوع Invisible خواهد بود.

۲۳. هکرهای ……، دانش کمی در این حوزه دارند و به تازگی وارد این حوزه شدند. گرچه در تلاش هستند که سطح دانشی خود را بالا ببرند و به یک هکر حرفه‌ای تبدیل شوند.

الف) کلاه خاکستری
ب) کلاه صورتی
ج) کلاه سبز
د) جوجه هکر

پاسخ: کلاه سبز: معمولا دانش کمی در این حوزه دارند و به تازگی وارد حوزه حک شدند. گرچه آن‌ها در تلاش هستند که سطح دانشی خود را در این حوزه بالا ببرند و به یک هکر حرفه‌ای تبدیل شوند.

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

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

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

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

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

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