نام و نام خانوادگی	شماره دانشجویی	نام درس	تاریخ	شماره برگه
		امنیت سیستم‌های کامپیوتری	۱۵ اسفند ۱۴۰۲	۱

نکات

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

۱. طول کلید یک رمز جانشینی تک‌الفبایی و دوحرفی با نگاشت کلی کدام گزینه است؟

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

پاسخ: برای رمز جانشینی از نوع تک‌الفبایی و دوحرفی، در صورتی که یک نگاشت کلی را در نظر بگیریم، فضای کلید برابر با $(26\times 26)!$ خواهد شد. چراکه به عنوان مثال دو حرف یعنی AA می‌تواند به 26×26 حرف دیگر و حرف AB می‌تواند به $26\times 26-$ حرف دیگر نگاشت شود و همین روند را می‌توان تا آخرین حرف ادامه داد. اما دقت کنید در این‌جا طول کلید را می‌خواهد نه فضای کلید، پس خواهیم داشت:

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

۲. جاهای خالی را پر کنید (به فارسی یا انگلیسی فرقی نمی‌کند).

❶ .....: علم اصول و روش‌های رمزگشایی متن رمز بدون اطلاع از کلید

❷ ..... علمی است متشکل از علم اصول و روش‌های رمزگذاری و علم اصول و روش‌های رمزگشایی متن رمز بدون اطلاع از کلید

❸ ..... علم اصول و روش‌های رمزگذاری

❹ .....: پیام رمزنشده

پاسخ: پاسخ در اسلایدها وجود دارد.

۳. کدام یک نادرست است؟

الف) طول کلید سزار برابر است با 4.7 بیت

ب) تحلیل رمز علمی است متشکل از علوم رمزنگاری و روش‌های رمزگذاری

ج) طول کلید رمز مستوی برابر است با 8.3 بیت

د) رمزهای چند الفبایی زیر مجموعه رمزهای جانشینی هستند

پاسخ: گزینه‌ی "تحلیل رمز علمی است متشکل از علوم رمزنگاری و روش‌های رمزگذاری" صحیح می‌باشد.

۴. 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 SQL Injection ب) حمله Phishing ج) حمله Packet sniffer 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.

۵. در ماشین Enigma تعداد حالت‌های انتخاب و قراردادن چرخ‌دنده‌ها در جایگاهشان و همچنین تعداد حالت‌های انتخاب حالت اولیه کدام گزینه است؟

الف) هیچ کدام　　ب) $P_3^5 \times 26^3$　　ج) $P_3^5 \times P_3^{26}$　　د) $\sum_{i=1}^{5} P_3^i \times 26^3$

پاسخ: در ادامه اجازه دهید فضای کلید را برای ماشین Enigma محاسبه کنیم. برای راحتی، ما کار را از چرخ‌دنده‌ها شروع می‌کنیم. در ماشین انیگما، تعداد پنج چرخ‌دنده وجود داشت که می‌بایست سه چرخ از میان انتخاب می‌شد و در جایگاه مورد نظر قرار می‌گرفت. به دلیل این که ترتیب چرخ‌دنده‌ها مهم است، خواهیم داشت:

$$P_3^5 = 60$$

هنگامی که چرخ‌دنده‌ها در جای خود قرار می‌گرفت، فرد مورد نظر می توانست آن را در یکی از ۲۶ حالت ممکن قرار دهد. در حقیقت سه مقدار حالت اولیه برای سه چرخ‌دنده داشتیم. بدین‌سان خواهیم داشت:

$$26^3 = 26 \times 26 \times 26 = 17576$$

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

الف) کارایی (Performance)　　ب) دسترس‌پذیری (Availability)
ج) سندیت (Authenticity)　　د) مسئولیت‌پذیری (Accountability)

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

۷. برای رمز مُستَوی (Affine Cipher) فضای کلید برابر با؟

الف) 676　　ب) 312　　ج) 260　　د) 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 $12 \times 26 = 312$ حالت داریم. در ضمن برای طول کلید خواهیم داشت:

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

۸. 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) SYTDIEPSETCRCNYUOOTRTNIIEFATCIL　　ب) EPSETCRCNYTCILSYTDIUOOTRTNIIEFA
ج) SYTDIETSETCRCNOUYOTRTNIIEFAPCIL　　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

۹. 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.

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

الف) رمز جایگشتی - چندالفبایی

ب) رمز جانشینی - چندالفبایی

ج) رمز جایگشتی - تک‌الفبایی - تک‌حرفی

د) رمز جانشینی - تک‌الفبایی - تک‌حرفی

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.

۱۱. جاهای خالی را پر کنید؟ (فارسی یا انگلیسی مهم نیست)

❶ نام ..... از نام اسب تروا یونان گرفته شده است. در داستان اصلی، مردم تروا یک اسب چوبی غول پیکر را وارد شهر کردند و فکر کردند که این نشان دهنده تسلیم شدن دشمنان آنها است اما سربازان یونانی که در اسب پنهان شده بودند شبانه از آن بیرون آمدند و دروازه شهر را برای بقیه ارتش خود باز کردند. ..... کامپیوتری دقیقا به همین شیوه عمل می کنند. شما به جای یک اسب بزرگ؛ برنامه ای دریافت خواهید کرد که مفید و بی ضرر به نظر می رسد. اما در واقع، در پشت صحنه کارهای مخربی را انجام می دهد.

❷ ..... احتمالا خطرناک ترین نوع بدافزار موجود است. این بدافزار یک قطعه کد بدافزار نیست بلکه مجموعه ای از برنامه های کاربردی است که بر روی یک سیستم نصب شده است. این برنامه ها با هم کنترل کامپیوتر را در سطح پایینی به دست می گیرند. منظور از سطح پایین؛ در سطح خود سیستم عامل است که به سازنده آن اجازه می دهد کاملا هر کاری را که می خواهد با سیستم کامپیوتری و داده های آن انجام دهد.

❸ بر خلاف بدافزارها؛ ..... به طور کلی هر کاری که در سیستم انجام می دهید را نظارت می کنند و بعد با گزارش اطلاعاتی در این مورد به سازنده کار خود را انجام می دهند. این اطلاعات می تواند شامل انواع مختلفی باشد. به عنوان مثال، نرم افزارهای جاسوسی ممکن است از اسنادی که روی آنها کار می کنید اسکرین شات بگیرد. ..... حتی ممکن است اطلاعات مالی شما را گزارش دهند.

❹ ..... نوعی بدافزار است که داده های شما را از بین نمی برد بلکه آنها را رمزگذاری و قفل می کند. بعد سازندگان باج افزار از شما می خواهند در قبال دادن کلید به آنها پول یا همان باج را بدهید.

❺ ..... و ویروس ها از یک نظر بسیار شبیه به هم هستند؛ آنها بار خود (معمولا مخرب) را روی سیستم های کامپیوتری تکثیر کرده و اجرا می کنند. تفاوت آنها در نحوه انتشار است. یک ویروس برای آلوده کردن نیاز به یک برنامه میزبان دارد و به کاربران متکی است تا برنامه آلوده را با استفاده از دستگاه های ذخیره سازی قابل حمل، ایمیل یا روش انتقال مشابه دیگر پخش کنند.

پاسخ: جاهای خالی به ترتیب Trojan، Rootkit، Spyware، Ransomware و Worm است.

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

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

۱۳. 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.

۱۴. 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) BlackHat
ب) Hope
ج) Positive Hack Days
د) Def Con

پاسخ: همایش Def Con

۱۵. فرض کنید که ما از رمز مُستَوی استفاده کردیم برای عملیات رمزگذاری ($\mathrm{E}_k(m) = 9m + 4$). اگر یک حرف متن رمز به صورت B باشد، حرف متن اصلی متناظر آن چیست؟

الف) پارامترها معتبر نیستند
ب) R
ج) A
د) Y

پاسخ: نکته مهم این سوال این بود که به ما تابع رمزگذاری را دادند یعنی تابع $\mathrm{E}_k(m) = 9m + 4 \mod 26$. 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 آورید، اما بعدها در همین درس نحوه بدست آوردن آن گفته خواهد شد. در نهایت برای تابع رمزگشایی خواهیم داشت:

$$\mathrm{E}_k(m) = 9m + 4 \mod 26 \implies \mathrm{D}_k(c) = 9^{-1}(c - 4) = 3c + 14 \mod 26$$

کافی است در معادله فوق، شماره B یعنی یک را قرار دهید:

$$m = \mathrm{D}_k(3) = 3 \times 1 + 14 \mod 26 = 17$$

که معادل حرف R است. البته شما ممکن است معکوس گرفتن در Mod را به خاطر نداشته باشید، که در این صورت باید از روش سعی و خطا استفاده کنید.

۱۶. 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.

۱۷. اگر شما یک وب سایت داشته باشیم و بخواهید آن را از حملات مشابه Mirai برای خارج کردن سایت شما از دسترسی، محافظت کنید، مهم‌ترین راه‌کار شما چه خواهد بود؟

الف) همه موارد
ب) تعیین چندین DNS Server برای آن
ج) بستن دسترسی پورت SSH
د) تعیین رمز غیرپیش‌فرض برای پورت SSH

۱۸. 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 1 petaFLOPS چقدر طول می‌کشد تا به صورت Brute-force این الگوریتم را بشکنیم؟

الف) 50000 ثانیه ب) 50 ثانیه ج) 5000 ثانیه د) 500 ثانیه

پاسخ: اگر یک کامپیوتر با قدرت 10 petaFLOPS در اختیار داشته باشیم، انتظار داریم در هر ثانیه این کامپیوتر برای ما 10^{15} 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:

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

$$\text{Time} = \frac{5 \times 10^{19}}{10^{15}} = 5 \times 10^{4} \text{ [Min]}$$

۱۹. 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 سفید ج) کلاه خاکستری 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.

۲۰. کدام گزینه راه‌کار بهتری برای جلوگیری از حملات تحلیل CDR است؟

الف) استفاده از رمزنگاری‌های قوی‌تر در روند ارتباطی
ب) وارد کردن داده‌های Fake، به عنوان مثال داده‌های تماس Fake برای برهم زدن ارتباط
ج) استفاده از Integrity در ارتباط بین دو نقطه برای جلوگیری از دستکاری اطلاعات
د) همه موارد

پاسخ: از حملات CDR را نمی‌توان با روش‌های مرسوم، جلوگیری کرد. پس گزینه (وارد کردن داده‌های Fake، به عنوان مثال داده‌های تماس Fake برای برهم زدن ارتباط)، صحیح است.

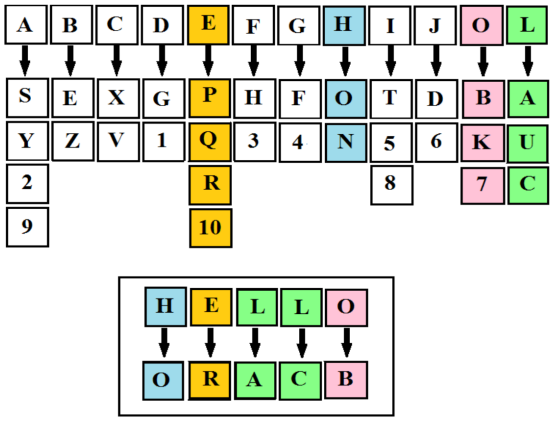
۲۱. می‌خواهیم عبارت THIS IS AN EXAMPLE را با استفاده از الگوریتم Vigenère رمز کنیم. اگر کلمه کلید CRYPT باشد، متن رمز کدام گزینه است؟

	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) VYGH BU RL TQCDNAX
د) ALTD WZ EY PLHQAWS

پاسخ: به عنوان مثال برای حرف اول باید برای حرف T، باید ستون T و سطر C را مشاهده کنیم، که می‌شود V.

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



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

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