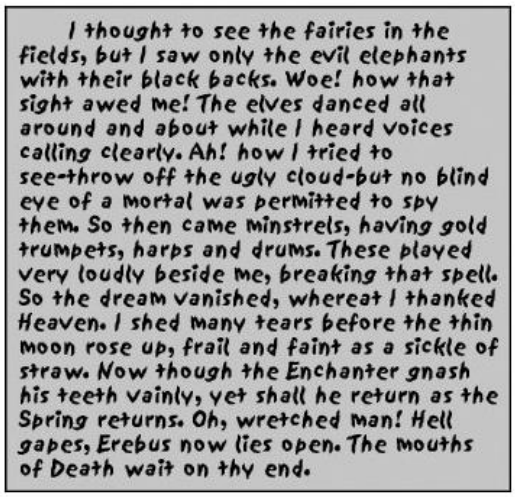
تمرین شماره ۳– رمز نگاری

۱. در یکی از داستان های Dorothy Sayers، لرد Peter با پیام رمزشده ای به شکل زیر مواجه شده است.


I thought to see the fairies in the fields, but I saw only the evil elephants with their black backs. Woe! how that sight awed me! The elves danced all around and about while I heard voices calling clearly. Ah! how I tried to see-throw off the ugly cloud-but no blind eye of a mortal was permitted to spy them. So then came minstrels, having gold trumpets, harps and drums. These played very loudly beside me, breaking that spell. So the dream vanished, whereat I thanked Heaven. I shed many tears before the thin moon rose up, frail and faint as a sickle of straw. Now though the Enchanter gnash his teeth vainly, yet shall he return as the Spring returns. Oh, wretched man! Hell gapes, Erebus now lies open. The mouths of Death wait on thy end.

کلید پیام که ترتیبی از اعداد صحیح است به صورت زیر کشف شده است:

78765654343211234345656787887876565434321123434565678788787656544332112341234

a. پیام را رمزگشایی کنید، دقت کنید این اعداد بین ۱ تا ۸ هستند که میتواند نشانه انتخاب یکی از هر ۸ دنباله کراکترها باشد.
b. اگر الگوریتم در معرض عموم باشد اما کلید را ندانیم، تا چه حدی این رویکرد امن است؟
c. اگر کلید در معرض عموم باشد اما الگوریتم را ندانیم، تا چه حدی این رویکرد امن است؟

۲. با استفاده از یک الگوریتم جایگذاری ساده ، متن رمز شده زیر محاسبه شده است.

```
53‡‡†305))6*;4826)4‡.)4‡);806*;48†8¶60))85;;]8*;:‡*8†83
(88)5*†;46(;88*96*?;8)*‡(;485);5*†2:*‡(;4956*2(5*-4)8¶8*
;4069285);)6†8)4‡‡;1(‡9;48081;8:8‡1;48†85;4)485†528806*81
(‡9;48;(88;4(‡?34;48)4‡;161;:188;‡?;
```

متن رمزشده را رمزگشایی کنید. نکات:

a. همانطور که میدانید حرف e بیشترین تکرار را در زبان انگلیسی دارد. بنابراین اولین یا دومین یا حتی سومین حرف پرتکرار در این متن به جای حرف e قرار گرفته است. همچنین حرف e

معمولاً به صورت دوتایی ظاهر میشود. مانند(meet، fleet و غیره). سعی کنید کاراکتر چایگزین e را در متن پیدا کنید.

b. پر استفاده ترین کلمه در زبان انگلیسی "the" است. از این مسئله برای پیدا کردن کاراکترهای جایگزین t و h استفاده کنید.

c. بقیه متن را با استنباط کردن سایر کلمات رمزگشایی کنید.

توجه: متن رمزگشایی شده در زبان انگلیسی معنا دارد است، گرچه ممکن است در ابتدا اینطور به نظر نرسد.

۳. الف) ثابت کنید در رمزکننده DES اگر مکمل بلوک گرفته شود و مکمل کلید رمزنگاری گرفته شود، نتیجه رمزنگاری با این مقادیر برابر مکمل متن رمزشده است.

$$\text{If } Y=DES_K(X)$$

$$\text{Then } Y`=DES_{K`}(X`)$$

راهنمایی: ابتدا نشان دهید هر برای هر دو دشته A و B داریم: $(A \oplus B)'$ برابر با $A' \oplus B'$ است.

ب)گفته می شود در حمله brute force بر DES فضای نام 2^{56} کلید باید جستجو شود. آیا نتیجه بخش الف تاثیری روی این سئوال دارد؟

۴. فرض کنید دو تابع درهم سازf و g وجود دارد. میدانیم فقط یکی از این توابع در برابر تصادم مقاوم(Collision Resistant) است، اما نمی دانیم کدام یکی از آنها در برابر تصادم مقاوم است. می خواهیم تابع جدید h را درست کنیم که در برابر تصادم مقاوم باشد. کدام یک از توابع زیر در برابر تصادم مقاوم بوده و کدام یک مقاوم نیست، در باره آن بحث کنید و مثالی بیاورید.

1. $h(x) = f(x) \circ g(x)$
2. $h(x) = f(g(x))$
3. $h(x) = f(g(x)) \circ g(f(x))$

۵. توابع زیر را درنظر بگیرید: $f1(x1) = z1;\ f2(x2, y2) = z2;\ f3(x3, y3) = z3.$ که کلیه مقادیر اعداد صحیحی بین 1 تا N هستند. تابع f1 را میتوان توسط ماتریس M1 به طول N نشان داد که kامین مدخل آن مقدار f1(k) است. f2 و f3 هم با ماتریس های N*N ، M2 و M3 نشان داده شده اند.هدف نشان دادن رمزنگاری و رمزگشایی با جستجو در جداول با مقادیر بزرگ N است. راه حل به این صورت است:

ساخت M1 با اعداد تصادفی بین ۱ تا N به طوریکه هر عدد تنها یکبار در M1 ظاهر شود. ساخت M2 به طوریکه هر سطر شامل جایگشت تصادفی از اعداد ۱ تا N باشد. در نهایت ساخت M3 که شرط زیر را داشته باشد: $f3(f2(f1(k),p),k) = p$. به عبارت دیگر:

- M1 ورودی K را گرفته و X را در خروجی می دهد.
- M2، X و P را به عنوان ورودی گرفته و Z را در خروجی می دهد.
- M3 وردی Z و K را گرفته و P را درخروجی می دهد.

سه جدول پس از ساخته شدن در معرض عموم قرار می گیرند.

الف- در مثال زیر جدول M3 را پر کنید

M1 =

5
4
2
3
1

M2 =

5	2	3	4	1
4	2	5	1	3
1	3	2	4	5
3	1	4	2	5
2	5	3	4	1

M3 =

iامین عنصر از M1 برابر با $k = i$ است. i امین سطر از M2 برابر با $x = i$ است و j امین ستون از M2 برابر با $p = j$ است و i امین سطر از M3 برابر با $z = i$ است و .j امین ستون از M3 برابر با $k = j$ است.

ب- رمزنگاری و رمزگشایی را با استفاده از این جدول های بین دو کاربر بیان کنید.

ج- در مورد امنیت این روش بحث کنید.

۶. به سئوال زیر پاسخ دهید:

Consider a very simple symmetric block encryption algorithm in which 32-bits blocks of plaintext are encrypted using a 64-bit key. Encryption is defined as

$$C = (P \oplus K_0) \boxplus K_1$$

where C = ciphertext, K = secret key, K_0 = leftmost 64 bits of K, K_1 = rightmost 64 bits of K, $\oplus$ = bitwise exclusive OR, and $\boxplus$ is addition mod 2^{64}.

a. Show the decryption equation. That is, show the equation for P as a function of C, K_0, and K_1.

b. Suppose and adversary has access to two sets of plaintexts and their corresponding ciphertexts and wishes to determine K. We have the two equations:

$$C = (P \oplus K_0) \boxplus K_1; C' = (P' \oplus K_0) \boxplus K_1$$

First, derive an equation in one unknown (e.g., K_0). Is it possible to proceed further to solve for K_0?

۷. به سئوال زیر پاسخ دهید:

For any block cipher, the fact that it is a nonlinear function is crucial to its security. To see this, suppose that we have a linear block cipher EL that encrypts 128-bit blocks of plaintext into 128-bit blocks of ciphertext. Let $EL(k, m)$ denote the encryption of a 128-bit message m under a key k (the actual bit length of k is irrelevant). Thus,

$$EL(k, [m_1 \oplus m_2]) = EL(k, m_1) \oplus EL(k, m_2) \text{ for all 128-bit patterns } m_1, m_2$$

Describe how, with 128 chosen ciphertexts, an adversary can decrypt any ciphertext without knowledge of the secret key k. (A "chosen ciphertext" means that an adversary has the ability to choose a ciphertext and then obtain its decryption. Here, you have 128 plaintext–ciphertext pairs to work with, and you have the ability to chose the value of the ciphertexts.)

۸. به سئوال زیر پاسخ دهید:

consider the problem: Use an encryption algorithm to construct a one-way hash function. Consider using RSA with a known key. Then process a message consisting of a sequence of blocks as follows: Encrypt the first block, XOR the result with the second block and encrypt again, and so on. Show that this scheme is not secure by solving the following problem. Given a two-block message B1, B2, and its hash, we have

$$RSAH(B1, B2) = RSA(RSA(B1) \oplus B2)$$

Given an arbitrary block C1, choose C2 so that $RSAH(C1, C2) = RSAH(B1, B2)$. Thus, the hash function does not satisfy weak collision resistance.

۹. به سئوال زیر پاسخ دهید:

Consider a Diffie-Hellman scheme with a common prime $q = 11$ and a primitive root $\alpha = 2$.

a. If user A has public key $Y_A = 9$, what is A's private key X_A?
b. If user B has public key $Y_B = 3$, what is the shared secret key K?

۱۰. به سئوال زیر پاسخ دهید:

There are three typical ways to use nonces as challenges. Suppose N_a is a nonce generated by A, A and B share key K, and f() is a function (such as increment). The three usages are

Usage 1	Usage 2	Usage 3
(1) A → B: N_a (2) B → A: $E(K, N_a)$	(1) A → B: $E(K, N_a)$ (2) B → A: N_a	(1) A → B: $E(K, N_a)$ (2) B → A: $E(K, f(N_a))$

Describe situations for which each usage is appropriate.

۱۱. به سئوال زیر پاسخ دهید:

In addition to providing a standard for public-key certificate formats, X.509 specifies an authentication protocol. The original version of X.509 contains a security flaw. The essence of the protocol is

$$\begin{aligned} \text{A} \rightarrow \text{B:} &\quad \text{A}\{t_A, r_A, ID_B\} \\ \text{B} \rightarrow \text{A:} &\quad \text{B}\{t_B, r_B, ID_A, r_A\} \\ \text{A} \rightarrow \text{B:} &\quad \text{A}\{r_B\} \end{aligned}$$

where t_A and t_B are timestamps, r_A and r_B are nonces, and the notation X {Y} indicates that the message Y is transmitted, encrypted, and signed by X.

The text of X.509 states that checking timestamps t_A and t_B is optional for three-way authentication. But consider the following example: Suppose A and B have used the preceding protocol on some previous occasion, and that opponent C has intercepted the preceding three messages. In addition, suppose that timestamps are not used and are all set to 0. Finally, suppose C wishes to impersonate A to B. C initially sends the first captured message to B:

$$\text{C} \rightarrow \text{B:} \quad \text{A}\{0, r_A, ID_B\}$$

B responds, thinking it is talking to A but is actually talking to C:

$$\text{B} \rightarrow \text{C:} \quad \text{B}\{0, r'_B, ID_A, r_A\}$$

C meanwhile causes A to initiate authentication with C by some means. As a result, A sends C the following:

$$\text{A} \rightarrow \text{C:} \quad \text{A}\{0, r'_A, ID_C\}$$

C responds to A using the same nonce provided to C by B.

$$\text{C} \rightarrow \text{A:} \quad \text{C}\{0, r'_B, ID_A, r'_A\}$$

A responds with

$$\text{A} \rightarrow \text{C:} \quad \text{A}\{r'_B\}$$

This is exactly what C needs to convince B that it is talking to A, so C now repeats the incoming message back out to B.

$$\text{C} \rightarrow \text{B:} \quad \text{A}\{r'_B\}$$

So B will believe it is talking to A, whereas it is actually talking to C. Suggest a simple solution to this problem that does not involve the use of timestamps.

۱۲. به سئوال زیر پاسخ دهید:

Consider a one-way authentication technique based on asymmetric encryption:

$$\begin{aligned} \text{A} \rightarrow \text{B:} &\quad ID_A \\ \text{B} \rightarrow \text{A:} &\quad R_1 \\ \text{A} \rightarrow \text{B:} &\quad \text{E}(PR_a, R_1) \end{aligned}$$

a. Explain the protocol.
b. What type of attack is this protocol susceptible to?