سوال ۱)

۱.۱

ساخت جدول ضرب برای Z_4

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

۱.۲

ساخت جدول جمع و ضرب برای Z_4

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

۱.۳

در Z_m هر عدد a که $\gcd(a, m) \neq 1$ باشد معکوس ضربی ندارد.

عناصری از Z_{12} که معکوس ضربی ندارند: $\{0, 2, 3, 4, 6, 8, 9, 10\}$ ← چون نسبت به ۱۲ اول نیستند.

عناصری از Z_{15} که معکوس ضربی ندارند: $\{0, 3, 5, 6, 9, 10, 12\}$ ← چون نسبت به ۱۵ اول نیستند.

چون ۱۱ یک عدد اول است، تمام عناصر نا صفر قبل از آن نسبت به آن اول هستند و برای همه ی آنها معکوس ضربی وجود دارد.

۱.۴

$m = 8 \rightarrow \quad Z^*_8 = \{1, 3, 5, 7\} \quad \rightarrow \quad \phi(8) = 4$

$m = 22 \quad \rightarrow \quad Z^*_{22} = \{1, 3, 5, 7, 9, 13, 15, 17, 19, 21\} \quad \rightarrow \quad \phi(22) = 10$

$\phi(m)$ تابع فی اویلر برابر است با تعداد اعدادی از مجموعه $\{1, 2, \ldots, m\text{-}1\}$ که نسبت به m اول هستند.

سوال ۲)

۲.۱

همانطور که میدانیم، معکوس یک عدد integer در یک حلقه، کاملا وابسته با آن حلقه است. اگر پیمانه تغییر کند معکوس هم تغییر میکند. یعنی معکوس یک المان به تنهایی معنا ندارد و باید حتما پیمانه آن ذکر گردد.

معکوس 7 در Z_9 :

$7 \times 7^{-1} = 1 \bmod 9 \rightarrow 7^{-1} = 4$

معکوس 7 در Z_{10} :

$7 \times 7^{-1} = 1 \bmod 10 \rightarrow 7^{-1} = 3$

معکوس 7 در Z_{11} :

$7 \times 7^{-1} = 1 \bmod 11 \rightarrow 7^{-1} = 8$

۲.۲

معکوس 9 در Z_7 :

$9 \times 9^{-1} = 1 \bmod 7 \rightarrow 9^{-1} = 4$

معکوس 10 در Z_7 :

$10 \times 10^{-1} = 1 \bmod 7 \rightarrow 10^{-1} = 5$

معکوس 11 در Z_7 :

$11 \times 11^{-1} = 1 \bmod 7 \rightarrow 11^{-1} = 2$

(روش دیگر حل این سوال استفاده از نکته $a^{-1} = a^{\phi(n)-1} \bmod n$ است.)

سوال ۳)

هدف یافتن مقدار x است.

1. $x = 3^3 \bmod 13 \equiv 27 \bmod 13 \equiv 1 \bmod 13$
2. $x = 3^{100} \bmod 13 \equiv 3^{99} \times 3 \bmod 13 \equiv (3^3)^{33} \times 3 \bmod 13 \equiv 1^{33} \times 3 \bmod 13 \equiv 3 \bmod 13$
3. $x = 6^2 \bmod 13 \equiv 36 \bmod 13 \equiv 10 \bmod 13$
4. $x = 6^{100} \bmod 13 \equiv (6^2)^{50} \bmod 13 \equiv 10^{50} \bmod 13 \equiv (10^2)^{25} \bmod 13 \equiv 9^{25} \bmod 13 \equiv (9^2)^{12} \times 9 \bmod 13 \equiv 3^{12} \times 9 \bmod 13 \equiv (3^3)^4 \times 9 \bmod 13 \equiv 1^4 \times 9 \bmod 13 \equiv 9 \bmod 13$
5. $7^x = 11 \bmod 13 \rightarrow x = 5$

با روش سعی و خطا مقدار x برابر با ۵ میشود. این یک مسئله لگاریتم گسسته است.

سوال ۴)

در affine cipher با داشتن دو زوج plaintext–ciphertext داریم:

$y_1 = a.x_1 + b \bmod m$ (سایز الفبا = m)

$y_2 = a.x_2 + b \bmod m$

با کم کردن دو ciphertext از هم دیگر داریم:

$y_1 - y_2 \equiv a(x_1 - x_2) \bmod m \rightarrow a \equiv (y_1 - y_2) \times (x_1 - x_2)^{-1} \bmod m$

و به این صورت a به دست می آید.

سپس برای b داریم:

$b \equiv y_1 - a.x_1 \bmod m$ یا $b \equiv y_2 - a.x_2 \bmod m$

در این صورت affine cipher شکسته میشود.

و شرط انتخاب x_1 و x_2 این است که معکوس $x_1 - x_2$ در پیمانه m وجود داشته باشد؛ یعنی $\gcd((x_1 - x_2), m) = 1$ باشد.

سوال ۵)

مهاجم به یک جفت متن رمزنگاری و متن اصلی با طول حداقل ۱۲۸ بیت نیاز دارد و می تواند با عملیات XOR کلید را بدست آورد.

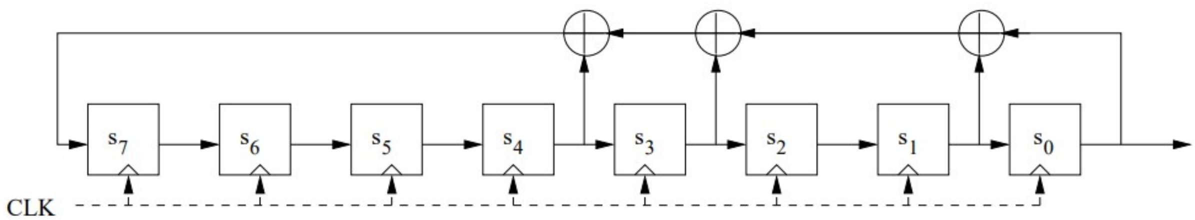
$k_i = c_i \oplus p_i$ for $i = 0,\ldots,127$

همچنین با حجم بالای داده ها، مهاجم می تواند تجزیه و تحلیل های آماری انجام دهد و اطلاعاتی درباره متن اصلی بدست آورد و الگوهایی در متن بدست آورد که منجر به حدس کلید شود.

سوال ۶)

$P(x) = x^8 + x^4 + x^3 + x + 1$

بلوک دیاگرام آن به صورت زیر خواهد بود :



با توجه به بلوک دیاگرام و مقدار اولیه آن (FF)، خروجی را در هر دور محاسبه میکنیم :

(مقادیر s_7تا s_1 به سمت راست شیفت داده میشوند و مقدار s_7 از روی بلوک بدست آورده میشود)

$s_7 = s_0 \oplus s_1 \oplus s_3 \oplus s_4$

s_7	s_6	s_5	s_4	s_3	s_2	s_1	s_0	خروجی
1	1	1	1	1	1	1	1	1(s_0)
0	1	1	1	1	1	1	1	1(s_1)
0	0	1	1	1	1	1	1	1(s_2)
0	0	0	1	1	1	1	1	1(s_3)
0	0	0	0	1	1	1	1	1(s_4)
1	0	0	0	0	1	1	1	1(s_5)
0	1	0	0	0	0	1	1	1(s_6)
0	0	1	0	0	0	0	1	1(s_7)
1	0	0	1	0	0	0	0	0(s_8)
1	1	0	0	1	0	0	0	0(s_9)

1	1	1	0	0	1	0	0	0(s_{10})
0	1	1	1	0	0	1	0	0(s_{11})
0	0	1	1	1	0	0	1	1(s_{12})
1	0	0	1	1	1	0	0	0(s_{13})
0	1	0	0	1	1	1	0	0(s_{14})
0	0	1	0	0	1	1	1	1(s_{15})

اولین ۱۶ بیت خروجی طبق جدول به صورت زیر است.

$(1001000011111111)_2 = (90FF)_{16}$

سوال ۷)

۷.۱

برای انجام یک حمله موفق، به ۵۱۲ بیت متوالی از جفت متن اصلی/ متن رمزشده (plaintext/ciphertext) نیاز داریم.

۷.۲

- ابتدا حمله‌کننده باید ۵۱۲ بیت متوالی از جفت متن اصلی/ متن رمزشده را بدست بیاورد.
- سپس می‌تواند $s_i = x_i \oplus y_i \quad , i = 0,1,\ldots,511(2m-1)$ را محاسبه کند.
- برای محاسبه ضرایب فیدبک LFSR ، باید ۲۵۶ معادله‌ی وابسته‌ی خطی زیر را تشکیل دهد:

$$s_{i+256} = \sum_{j=0}^{255} p_j \cdot s_{i+j} \quad mod\ 2$$

$$p_j \in \{0,1\} \quad , \quad i = 0,1,2,\ldots,255$$

- سپس با حل معادلات خطی می‌تواند ۲۵۶ ضریب فیدبک LFSR و کلید را بدست آورد.

۷.۳

۲۵۶ ضریب فیدبک LFSR در واقع کلید این سیستم را مشخص می‌کنند.

با توجه به این‌که مقادیر اولیه LFSR ، بدون تغییر از آن شیفت داده و خارج می‌شوند و سپس با ۲۵۶ بیت اولیه متن اصلی XOR می‌شوند، بنابراین محاسبه آن به راحتی امکان‌پذیر بوده و نباید به عنوان کلید مورد استفاده قرار بگیرند.

سوال ۸)

۸.۱

با توجه به این‌که درجه LFSR برابر با ۳ است، بنابراین ۳ بیت ابتدایی کلید با مقدار اولیه LFSR برابر است (۳ بیت ابتدایی بدون تغییر از LFSR خارج می‌شوند).

LFSR Initialization Vector = 001 $\Rightarrow\ s_0 = 0\ ,\ s_1 = 0\ ,\ s_2 = 1$

۸.۲

با استفاده از ضرایب فیدبک LFSR ، معادلات مربوط به ۳ بیت بعدی (s_3 تا s_5) را تشکیل می‌دهیم: (توجه کنید که مقادیر این ۳ بیت با استفاده از کلید مشخص است و فقط ضرایب فیدبک LFSR مجهول‌اند)

$$s_2p_2 + s_1p_1 + s_0p_0 = s_3$$
$$s_3p_2 + s_2p_1 + s_1p_0 = s_4$$
$$s_4p_2 + s_3p_1 + s_2p_0 = s_5$$

اکنون به کمک مقدار کلید (0010111) ، ضرایب فیدبک را بدست می‌آوریم:

$$s_0 = 0\ ,\ s_1 = 0\ ,\ s_2 = 1 \quad \Rightarrow \quad 1p_2 + 0p_1 + 0p_0 = 0\ (s_3)$$
$$s_1 = 0\ ,\ s_2 = 1\ ,\ s_3 = 0 \quad \Rightarrow \quad 0p_2 + 1p_1 + 0p_0 = 1\ (s_4)$$
$$s_2 = 1\ ,\ s_3 = 0\ ,\ s_4 = 1 \quad \Rightarrow \quad 1p_2 + 0p_1 + 1p_0 = 1\ (s_5)$$

با حل ۳ معادله و ۳ مجهول بالا، ضرایب فیدبک به صورت زیر بدست می‌آیند:

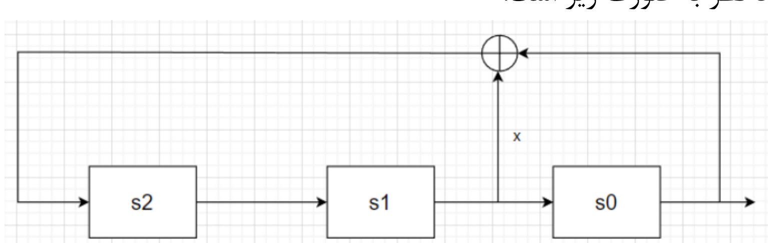
$$p_0 = 1\ ,\ p_1 = 1\ ,\ p_2 = 0$$

بنابراین چندجمله‌ای مربوط به LFSR به صورت زیر بدست می‌آید:

$$P(x) = x^3 + p_2x^2 + p_1x + p_0 \quad \Rightarrow \quad P(x) = x^3 + x + 1$$

۸.۳

بلوک دیاگرام LFSR مورد نظر به صورت زیر است:



با استفاده از بلوک دیاگرام LFSR و مقدار اولیه آن، خروجی را در هر دور محاسبه می‌کنیم:

خروجی	s_0	s_1	s_2
0 (s_0)	0	0	1
0 (s_1)	0	1	0
1 (s_2)	1	0	1
0 (s_3)	0	1	1
1 (s_4)	1	1	1
1 (s_5)	1	1	0
1 (s_6)	1	0	0

همان‌طور که مشاهده می‌شود، خروجی LFSR با کلید ما یکی است؛ بنابراین صحت نتایج بررسی می‌شود.