سوال ۱)

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.

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 ۲)

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. $x = 6^{100} \bmod 13 \equiv (6^2)^{50} \bmod 13 \equiv 10^{50} \bmod 13 \equiv (10^2)^{25} \bmod 13 \equiv 9^{25} \bmod 13 \equiv (9^2)^{12} \times 9 \bmod 13 \equiv 3^{12} \times 9 \bmod 13 \equiv (3^3)^4 \times 9 \bmod 13 \equiv 1^4 \times 9 \bmod 13 \equiv 9 \bmod 13$

سوال ۳)

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:

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

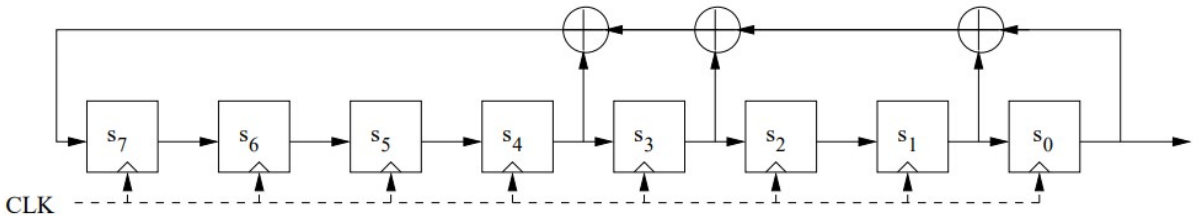
در این صورت affine cipher شکسته میشود.

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 ۴)

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

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 s7تا s1 به سمت راست شیفت داده میشوند و مقدار s7 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 ۵)

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 $\Rightarrow s_0 = 0\ ,\ s_1 = 0\ ,\ s_2 = 1$

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:

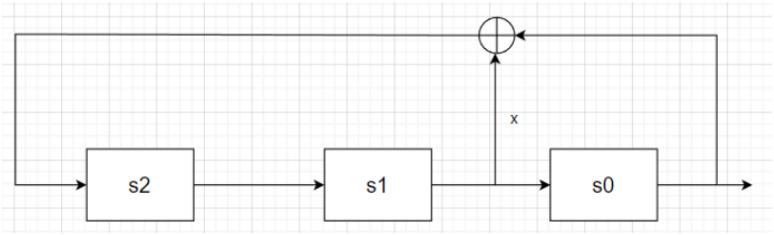
$$p_0 = 1\ ,\ p_1 = 1\ ,\ p_2 = 0$$

بنابراین چند جمله‌ای مربوط به LFSR به صورت زیر بدست می‌آید:

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

۳.

بلوک دیاگرام LFSR مورد نظر به صورت زیر است:



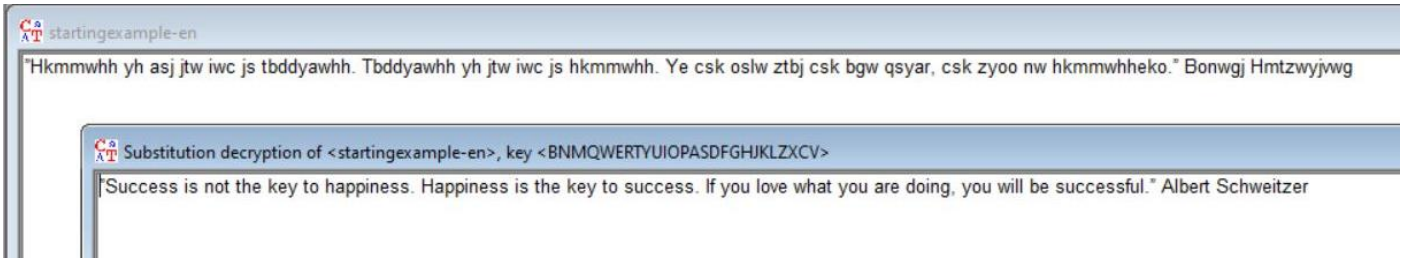
با استفاده از بلوک دیاگرام LFSR و مقدار اولیه آن، خروجی را در هر دور محاسبه می‌کنیم:

s_2	s_1	s_0	خروجی
1	0	0	0 (s_0)
0	1	0	0 (s_1)
1	0	1	1 (s_2)
1	1	0	0 (s_3)

1	1	1	1 (s_4)
0	1	1	1 (s_5)
0	0	1	1 (s_6)

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

سوال ۶)



سوال ۷)