مهیار عنصری ۹۶۳۲۰۹۳

سوال اول

الف) ۱.۷

جدول ضرب برای Z_4

×	۰	۱	۲	۳
۰	۰	۰	۰	۰
۱	۰	۱	۲	۳
۲	۰	۲	۰	۲
۳	۰	۳	۲	۱

جدول ضرب برای Z_5

×	۰	۱	۲	۳	۴
۰	۰	۰	۰	۰	۰
۱	۰	۱	۲	۳	۴
۲	۰	۲	۴	۱	۳
۳	۰	۳	۱	۴	۲
۴	۰	۴	۳	۲	۱

جدول جمع برای Z_5

+	۰	۱	۲	۳	۴
۰	۰	۱	۲	۳	۴
۱	۱	۲	۳	۴	۰
۲	۲	۳	۴	۰	۱
۳	۳	۴	۰	۱	۲
۴	۴	۰	۱	۲	۳

جدول ضرب برای Z_6

×	۰	۱	۲	۳	۴	۵
۰	۰	۰	۰	۰	۰	۰
۱	۰	۱	۲	۳	۴	۵
۲	۰	۲	۴	۰	۲	۴
۳	۰	۳	۰	۳	۰	۳
۴	۰	۴	۲	۰	۴	۲
۵	۰	۵	۴	۳	۲	۱

جدول جمع برای Z_6

+	۰	۱	۲	۳	۴	۵
۰	۰	۱	۲	۳	۴	۵
۱	۱	۲	۳	۴	۵	۰
۲	۲	۳	۴	۵	۰	۱
۳	۳	۴	۵	۰	۱	۲
۴	۴	۵	۵	۱	۲	۳
۵	۵	۰	۱	۲	۳	۴

در Z_4 ، ۰ و ۲ و در Z_6 ، ۰ و ۲ و ۳ و ۴ اعضای بدون وارون ضرب هستند و در Z_5 همه اعضای غیرصفر ، وارون پذیر هستند (زیرا ۵ عدد اول است)

Scanned by CamScanner

ب) ۱.۸

وارون ضرب عدد ۵ در Z_{11} برابر است با ۹:

$$5^{-1} \bmod 11 \equiv 9 \bmod 11 \Longrightarrow 5\times 9 \bmod 11 \equiv 1 \bmod 11$$

وارون ضرب عدد ۵ در Z_{12} برابر است با ۵:

$$5^{-1} \bmod 12 \equiv 5 \bmod 12 \Longrightarrow 5\times 5 \bmod 12 \equiv 1 \bmod 12$$

وارون ضرب عدد ۵ در Z_{13} برابر است با ۸:

$$5^{-1} \bmod 13 \equiv 8 \bmod 13 \Longrightarrow 5\times 8 \bmod 13 \equiv 1 \bmod 13$$

ج) ۱.۹

۱) $3^2 \bmod 13 \equiv 9 \bmod 13$

۲) $7^2 \bmod 13 \equiv 49 \bmod 13 \equiv 10 \bmod 13$

۳) $3^{10} \bmod 13 \equiv 9^5 \bmod 13 \equiv 81^2 \cdot 9 \bmod 13 \equiv 3^2 \cdot 9 \bmod 13 \equiv 81 \bmod 13 \equiv 3 \bmod 13$

۴) $7^{100} \bmod 13 \equiv 49^{50} \bmod 13 \equiv 10^{50} \bmod 13 \equiv (-3)^{50} \bmod 13 \equiv 3^{50} \bmod 13 \equiv (3^{10})^5 \bmod 13 \equiv 3^5 \bmod 13 \equiv 243 \bmod 13 \equiv 9 \bmod 13$

۵) $7^5 \bmod 13 \equiv (7\cdot 49^2) \bmod 13 \equiv 7\cdot 10^2 \bmod 13 \equiv 7\cdot(-3)^2 \bmod 13 \equiv 63 \bmod 13 \equiv 11 \bmod 13$

د) ۱.۱۰

$m=4$: $\gcd(4,n)=1 \Longrightarrow n=\{1,3\} \Longrightarrow \Phi(4)=2$

$m=5$: $\gcd(5,n)=1 \Longrightarrow n=\{1,2,3,4\} \Longrightarrow \Phi(5)=4$

$m=9$: $\gcd(9,n)=1 \Longrightarrow n=\{1,2,4,5,7,8\} \Longrightarrow \Phi(9)=6$

$m=26$: $\gcd(26,n)=1 \Longrightarrow n=\{1,3,5,7,9,11,15,17,19,21,23,25\} \Longrightarrow \Phi(26)=12$

Scanned by CamScanner

ه) ۱.۱۳)

x_1 و x_2 به شرطی انتخاب می‌شوند که $x_2 - x_1$ دارای وارون ضرب باشد یا به عبارتی $\gcd(m \text{ و } x_2 - x_1) = 1$ باشد که m تعداد حروف الفبا است. با توجه به affine cipher داریم:

$$\begin{cases} y_1 = a x_1 + b \bmod m \\ y_2 = a x_2 + b \bmod m \end{cases}$$

$$\Longrightarrow \begin{cases} a \equiv \left((x_1 - x_2)^{-1} \cdot (y_1 - y_2)\right) \bmod m \\ b = (y_1 - a x_1) \bmod m \end{cases}$$

۲-

۲-۱)

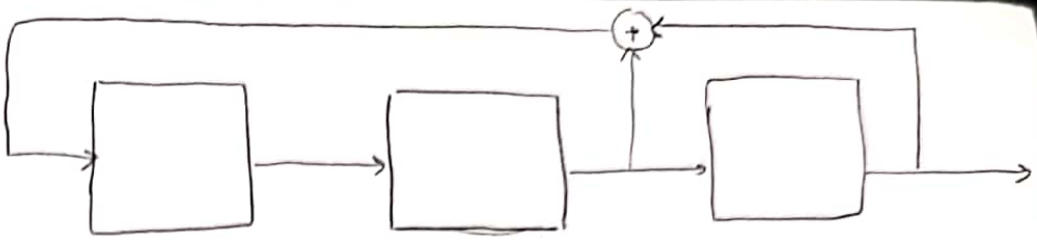
Primitive Polynomial ← یعنی LFSR هایی که دنباله تولیدی آن‌ها حداکثر $2^m - 1$ طول دارد.

Reducible Polynomial ← " " " " طول دنباله تولیدی‌شان به مقدار اولیه رجیسترها بستگی دارد و از حداکثر طول است.

Irreducible Polynomial ← یعنی LFSR هایی که حداکثر طول را تولید نمی‌کنند ولی طول آن‌ها به مقدار اولیه رجیسترها وابسته نیست.

Scanned by CamScanner

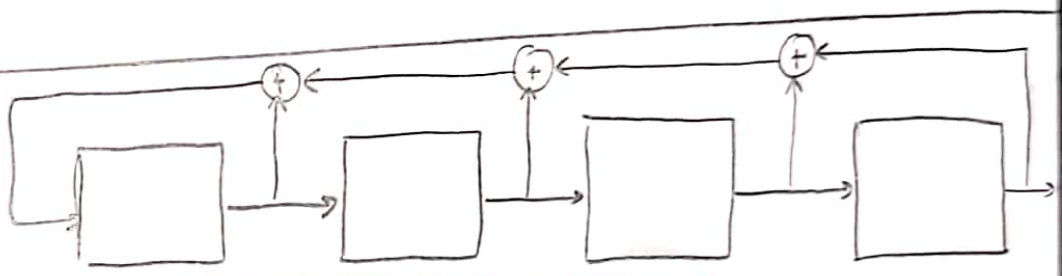
$x^3 + x + 1$



	S_2	S_1	S_0	out
۱	۰	۰	۱	۱
۲	۱	۰	۰	۰
۳	۰	۱	۰	۰
۴	۱	۰	۱	۱
۵	۱	۱	۰	۰
۶	۱	۱	۱	۱
۷	۰	۱	۱	۱
	۰	۰	۱	

initial state: ۰۰۱

$x^4 + x^3 + x^2 + x + 1$



	S_3	S_2	S_1	S_0	out
۱	۰	۰	۰	۱	۱
۲	۱	۰	۰	۰	۰
۳	۱	۱	۰	۰	۰
۴	۰	۱	۱	۰	۰
۵	۰	۰	۱	۱	۱
	۰	۰	۰	۱	۱

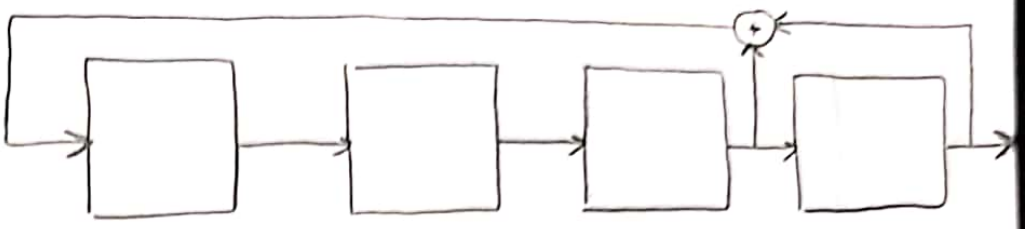
	S_3	S_2	S_1	S_0	out
۱	۰	۰	۱	۰	۰
۲	۱	۰	۰	۱	۱
۳	۰	۱	۰	۰	۰
۴	۱	۰	۱	۰	۰
۵	۰	۱	۰	۱	۱
	۰	۰	۱	۰	۰

	S_3	S_2	S_1	S_0	out
۱	۰	۱	۱	۱	۱
۲	۱	۰	۱	۱	۱
۳	۱	۱	۰	۱	۱
۴	۱	۱	۱	۰	۰
۵	۱	۱	۱	۱	۱
	۰	۱	۱	۱	۱

CS - 001

Scanned by CamScanner

$x^4 + x + 1$



	S_3	S_2	S_1	S_0	out
۱	۰	۱	۰	۰	۰
۲	۰	۰	۱	۰	۰
۳	۱	۰	۰	۱	۱
۴	۱	۱	۰	۰	۰
۵	۰	۱	۱	۰	۰
۶	۱	۰	۱	۱	۱
۷	۰	۱	۰	۱	۱
۸	۱	۰	۱	۰	۰
۹	۱	۱	۰	۱	۱
۱۰	۱	۱	۱	۰	۰
۱۱	۱	۱	۱	۱	۱
۱۲	۰	۱	۱	۱	۱
۱۳	۰	۰	۱	۱	۱
۱۴	۰	۰	۰	۱	۱
۱۵	۱	۰	۰	۰	۰
	۰	۱	۰	۰	

۳-۲) x^3+x+1 ← چون دنباله تولید شده توسط چندجمله ای طول 2^3-1 دارد و به initial state وابسته نیست پس یک چندجمله ای Primitive (Primitive Polynomial) است.

$x^4+x^3+x^2+x+1$ ← دنباله تولید شده همیشه طول ۵ دارد و به initial state وابسته نیست پس یک چندجمله ای از نوع irreducible Polynomial است.

x^4+x+1 ← دنباله تولید شده طول 2^4-1 دارد و وابستگی به inital state ندارد پس از نوع Primitive است

۴-۲)

$x^4+x^3+x^2+x+1 \rightarrow \max(5,5,5)=5$

$x^3+x+1 \rightarrow 2^3-1=7$

$x^4+x+1 \rightarrow 2^4-1=15$

Scanned by CamScanner

۳) a) برای یک حمله موفق نیاز به ۵۱۲ جفت بیت (x_i و y_i) داریم.

---

۳) b)

LFSR Sequence $\equiv x_i + y_i \bmod 2$ و $i = 0, \dots, 512$

LFSR Equation $\rightarrow s_{i+255} \equiv \sum_{j=0}^{255} P_j \cdot s_{i+j} \bmod 2$

حال برای iهای مختلف رابطه فوق را می‌نویسیم :

$$i=0 \Longrightarrow s_{256} \equiv \sum_{j=0}^{255} P_j \cdot s_j \bmod 2 \equiv P_0 s_0 + P_1 s_1 + \dots + P_{255} s_{255}$$

$$i=1 \Longrightarrow s_{257} \equiv \sum_{j=0}^{255} P_j \cdot s_{j+1} \bmod 2 \equiv P_0 s_1 + P_1 s_2 + \dots + P_{255} s_{256}$$

$$i=255 \Longrightarrow s_{511} \equiv \sum_{j=0}^{255} P_j \cdot s_{j+255} \bmod 2 \equiv P_0 s_{255} + P_1 s_{256} + \dots + P_{255} s_{510}$$

می‌توانیم این دستگاه معادلات را به فرم ماتریسی بازنویسی کنیم.

$$\begin{bmatrix} s_0 & s_1 & \cdots & s_{255} \\ s_1 & s_2 & \cdots & s_{256} \\ \vdots & \vdots & \ddots & \vdots \\ s_{255} & s_{256} & \cdots & s_{510} \end{bmatrix} \begin{bmatrix} P_0 \\ P_1 \\ \vdots \\ P_{255} \end{bmatrix} = \begin{bmatrix} s_{256} \\ s_{257} \\ \vdots \\ s_{511} \end{bmatrix}$$

حال می‌توانیم با روش‌های مختلف حل دستگاه معادلات مثل روش کرامر یا گاوس جردن این دستگاه را حل کنیم.

---

۳) c) کلید سیستم بردار شامل P_i ها است. یعنی ۲۵۶ طول دارد.

استفاده از شرایط اولیه به این دلیل غیرمنطقی است که اگر ۲۵۶ خروجی پیاپی از LFSR را ببینیم، می‌توانیم به کلید دسترسی پیدا کنیم و متن را رمزگشایی کنیم. (به عنوان طرف سوم)

Scanned by CamScanner

۴-۱) کد ارسال شده است.

۴-۲)

WPI : 10110 01111 01000

Ciphertext: 01001 11111 00000

۵ حرف اول Ciphertext را با WPI ، XOR می‌کنیم،

S : 11111 10000 01000 $\Longrightarrow$ Initalizing vector : 11111

۴-۳)

S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}
1	1	1	1	1	1	0	0	0	0	0	1

$$\begin{cases} S_5P_5 + S_4P_4 + S_3P_3 + S_2P_2 + S_1P_1 = S_6 \\ S_6P_5 + S_5P_4 + S_4P_3 + S_3P_2 + S_2P_1 = S_7 \\ S_7P_5 + S_6P_4 + S_5P_3 + S_4P_2 + S_3P_1 = S_8 \\ S_8P_5 + S_7P_4 + S_6P_3 + S_5P_2 + S_4P_1 = S_9 \\ S_9P_5 + S_8P_4 + S_7P_3 + S_6P_2 + S_5P_1 = S_{10} \\ S_{10}P_5 + S_9P_4 + S_8P_3 + S_7P_2 + S_6P_1 = S_{11} \end{cases}$$

با حل این معادلات داریم:

$P_0 = P_1 = 1$, $P_2 = P_3 = P_4 = P_5 = 0$

۴-۴) استرالیا

۴-۵) Known Plaintext attack

Scanned by CamScanner

سوال اختیاری:

با xor کردن ciphertext و Pluintext به کلید + nonce می‌رسیم.

BARACKOBAMA $\xrightarrow[\text{ASCII}]{}$ ۶۶, ۶۵, ۸۲, ۶۵, ۶۷, ۷۵, ۷۹, ۶۶, ۶۵, ۷۷, ۶۵

→ Plaintext:	01000010	01000001	01010010	01000001	01000011	01001010	01001111	01000001
Ciphertext:	01000011	00011011	00010010	00110000	11111000	10100111	10001110	11101001
	00000001	01011010	01000000	01110001	10111011	11101100	11000001	10101011

01000001	01001101	01000001
00010100	00011110	01100100
01010101	01010000	00101001

→ nonce = ۲

خروجی حاصله برای nonce=۱ است ولی برای decrypt قسمت بعد به (کلید + ۲) نیاز داریم پس اعداد فوق را بعلاوه ۱ می‌کنیم و حاصل را با ciphertext، xor می‌کنیم.

00000010	01101101	01000001	01110010	10111100	11101101	11000010	10101100	01101110
01000110	00010100	00001111	00110011	11110000	10101001	10010110	11111110	00000011
01000100	01001111	01001110	01000001	01001100	01000100	01010100	01001010	01010101
۶۸	۷۹	۷۸	۶۵	۷۶	۶۸	۸۴	۸۲	۸۵

01010001	01100110
00011100	01110110
01001101	01010000
۷۷	۸۰

→ DONALDTRUMP

Scanned by CamScanner