Mahdi Alikhasi 9530483

1.

با انجام ضرب های مورد نظر تحت جمله ی تحویل ناپذیر داده شده، نهایتاً جدول ضرب زیر را داریم::

	0	1	X	X + 1	X^2	$X^2 + 1$	$X^2 + X$	$X^2 + X + 1$
0 (000)	0	0	0	0	0	0	0	0
1 (001)	0	1	X	X + 1	X^2	$X^2 + 1$	$X^2 + X$	$X^2 + X + 1$
X (010)	0	X	X^2	$X^2 + X$	X + 1	1	$X^2 + X + 1$	$X^2 + 1$
X + 1 (011)	0	X + 1	$X^2 + X$	$X^2 + 1$	$X^2 + X + 1$	X^2	1	X
X^2 (100)	0	X^2	X + 1	$X^2 + X + 1$	$X^2 + X$	X	$X^2 + 1$	1
$X^2 + 1$ (101)	0	$X^2 + 1$	1	X^2	X	$X^2 + X + 1$	X + 1	$X^2 + X$
$X^2 + X$ (110)	0	$X^2 + X$	$X^2 + X + 1$	1	$X^2 + 1$	X + 1	X	X^2
$X^2 + X + 1$ (111)	0	$X^2 + X + 1$	$X^2 + 1$	X	1	$X^2 + X$	X^2	X + 1

2.

با استفاده از غربال میتوان به دست آورد که::

روش : جملات از درجه ی یک تنها دو جمله ی x+1 و x هستند. از حاصل ضرب این جمله در یک دیگر دو جمله ی $x^2 + x$ و x^2 و $x^2 + 1$ هستند. پس از تمامی چند جمله‌ای های درجه ی دو این سه جمله حذف شده (زیرا تحویل پذیر اند) و بقیه ی جملات از درجه ی دو تحویل ناپذیر هستند که تنها جمله ی $x^2 + x + 1$ باقی می ماند. به همین ترتیب جملات مرحله ی بالاتر را غربال میکنیم و برای درجه ی سه و درجه ی چهار تنها جملات زیر باقی می ماند.

a) $1 + x + x^3$, $1 + x^2 + x^3$

b) $1 + x + x^4$, $1 + x + x^2 + x^3 + x^4$, $1 + x^3 + x^4$

3.

a)

در این سؤال k0 قبل از شروع همه چی با ورودی xor می‌شود و پس از پایان مراحل substitution و shiftRow و permutation دوباره با k1 که کلید دوم است xor میشود.

میتوان ورودی و کلید ها را به صورت آرایه ی 4*4 نشان داد که هر خانه 1 بایت است. بنابراین

k0 = w0 w1 w2 w3

2B	28	AB	09
7E	AE	F7	CF
15	D2	15	4F
16	A6	88	3C

و ورودی ما به صورت زیر است

01	00	00	00
00	00	00	00
00	00	00	00
00	00	00	00

حال در ابتدا k0 با ورودی xor می‌شود (دقت کنید تنها خانه ی بالا سمت چپ در ورودی صفر نیست)
نتیجه میشود

2A	28	AB	09
7E	AE	F7	CF
15	D2	15	4F
16	A6	88	3C

در مرحله ی بعد، Byte Substitution انجام میشود. پس از آن داریم:

E5	34	62	01
F3	E4	68	8A
59	B5	59	84
47	24	C4	EB

پس از آن مرحله ی shiftRow است. پس از این مرحله داریم

E5	34	62	01
E4	68	8A	F3
59	84	59	B5
EB	47	24	C4

نهایتاً مرحله ی Mix Column اعمال می‌شود که شامل یک ضرب میدانی است.
نهایتاً پس از انجام ضرب داریم :

54	13	3C	7D
36	34	A2	FC
95	86	36	D4
44	3E	3D	D6

و نهایتاً در کلید k1 = W4 W5 W6 W7 ضرب میکنیم و خروجی نهایی به شکل

F4CC6B539B60AA8F1F010F045790A2D3 است.

b)
مراحل فوق را دوباره اجرا میکنیم. این بار با ورودی کاملاً صفر. بنابر این پس از مرحله ی اول که k0 در ورودی xor می‌شود، چون ورودی کاملاً صفر است خروجی همان k0 است.

2B	28	AB	09
7E	AE	F7	CF
15	D2	15	4F
16	A6	88	3C

پس از آن Byte Substitution را انجام میدهیم:

F1	34	62	01
F3	E4	68	8A
59	B5	59	84
47	24	C4	EB

(تنها خانه ی بالا سمت چپ با مرحله ی نظیر در قسمت a متفاوت است)

حال ShiftRow را انجام میدهیم:

F1	34	62	01
E4	68	8A	F3
59	84	59	B5
EB	47	24	C4

(همچنان تنهای خانه ی بالا سمت چپ با مرحله ی نظیر در قسمت a متفاوت است)

و نهایتاً Mix column را انجام میدهیم:

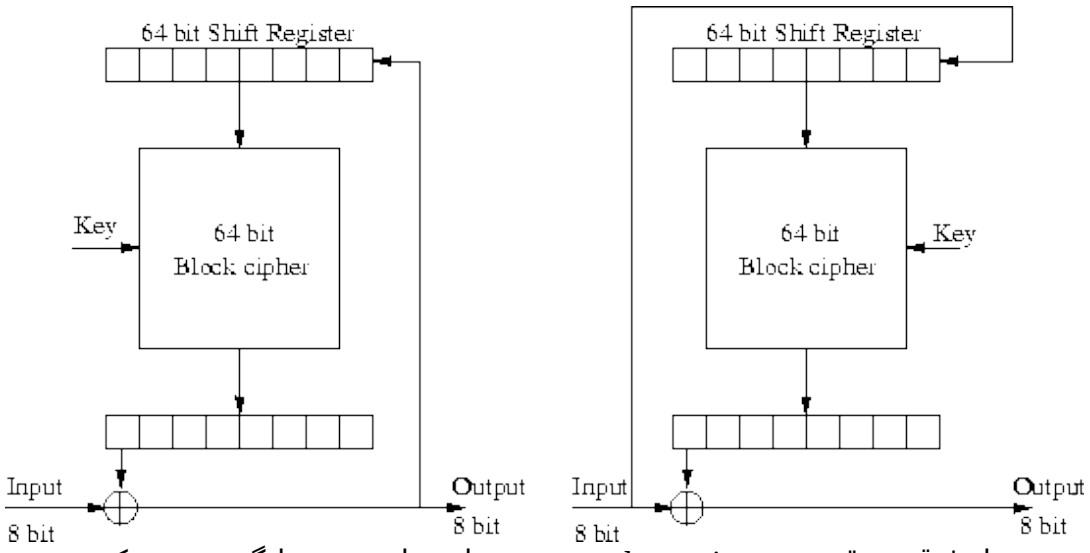
7C	13	3C	7D
22	34	A2	FC
81	86	36	D4
78	3E	3D	D6

در این مرحله به دلیل غیر خطی بودن ضرب میدانی انجام شده نتیجه با قسمت a کاملاً متفاوت میشود. نهایتاً حاصل را در k1 ضرب (xor) کرده و خروجی راند 1 به شکل زیر است

DCD87F6F9B60AA8F1F010F045790A2D3

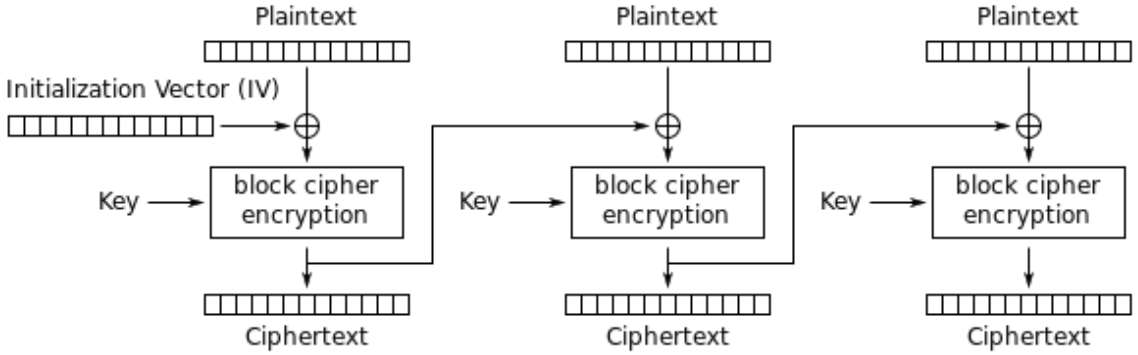
c)
با مقایسه ی دو مقدار به دست آمده در قسمت a و b میتوان دریافت که 10 بیت با یکدیگر متفاوت شده اند.

4.



با توجه به نمودار فوق در قسمت dceryption، در صورت اشتباه شدن یا گم شدن یک بیت نهایتاً پس از k+1 دور، شیفت رجیستر بالایی (که اندازه ی آن K است. در تصویر فوق k = 64 است) بیت مورد نظر از شیفت رجیستر خارج شده و سیستم به روال عادی خودش باز گشته و به صورت صحیح رمزگشایی میکند. توجه شود که در این حالت با استفاده از شیفت رجیستر ما در هر دور یک بیت را رمزگشایی میکنیم.

5.



Cipher Block Chaining (CBC) mode encryption

با توجه به ساختار CBC که در تصویر فوق مشخص شده است، برای به دست آوردن IV کافی است ابتدا با استفاده از کلیدی که در اختیار داریم بلاک اول داده‌ای که plainText آن را میدانیم 0xFF است را رمزگشایی کنیم. حاصل به دست آمده همان xor بین IV و PlainText است.
پس حاصل به دست آمده را دوباره با 0xFF که همان مقدار plaintext است xor میکنیم تا مقدار IV به دست بیاید.
حال با داشتن IV و همچنین کلیدی که از قبل داشتیم میتوانیم فایلی که محتوا آن را نمیدانیم را نیز به سادگی رمزگشایی کنیم.