



**Faculty of Engineering & Technology Electrical & Computer
Engineering Department**

Applied Cryptography– ENCS4320

HW #2

Prepared by:

Maha Maher Mali

1200746

Instructor: Dr. Mohammed Hussein

Section: 2

Date: 20-1-2024

Table of Contents

Section A 1

 Question 1 1

 Part A..... 1

 Part B..... 2

 Part C..... 2

 Question 2..... 3

 Part A..... 3

 Part B..... 4

 Part C..... 4

 Question 3..... 5

 Question 4..... 6

 Part A..... 6

 Part B..... 6

 Part C..... 7

 Part D..... 8

Section B 9

 Question 5..... 9

 Part A..... 9

 Part B..... 11

Section C 12

 Question 6..... 12

 Part A..... 12

 Part B..... 13

 Question 7..... 14

 Part A..... 14

 Part B..... 15

 Part C..... 16

References 17

Table of Figures

Figure 1:Feistel Network With 4 Round 1

Figure 2: Question 1 Part-A 1

Figure 3: Question 1 Part-B..... 2

Figure 4: Question 1 Part-C..... 2

Figure 5:Difference Between Confusion &Diffusion [2]..... 4

Figure 6: Question 3 Solution..... 5

Figure 7: Question 4-part A Solution..... 6

Figure 8 :Question 4-part B Solution..... 6

Figure 9: Question 4-part C Solution 7

Figure 10: Question 4-part D Solution..... 8

Figure 11: Question 5-part A solution..... 10

Figure 12: Question 5-part B solution..... 11

Figure 13: Question 6-part A solution..... 12

Figure 14: Question 6-part B Solution 13

Figure 15: Question 7-part A solution..... 14

Figure 16: Question 7-part B solution..... 15

Figure 17: Question 7-part C solution..... 16

Acronyms and Abbreviations

E	Encryption Process
D	Decryption Process
M	Message
P	Plaintext (Same Message)
K	Key
V	OR Operation Symbol
\oplus	XOR Operation Symbol
\parallel	Concatenation

Section A

Question 1

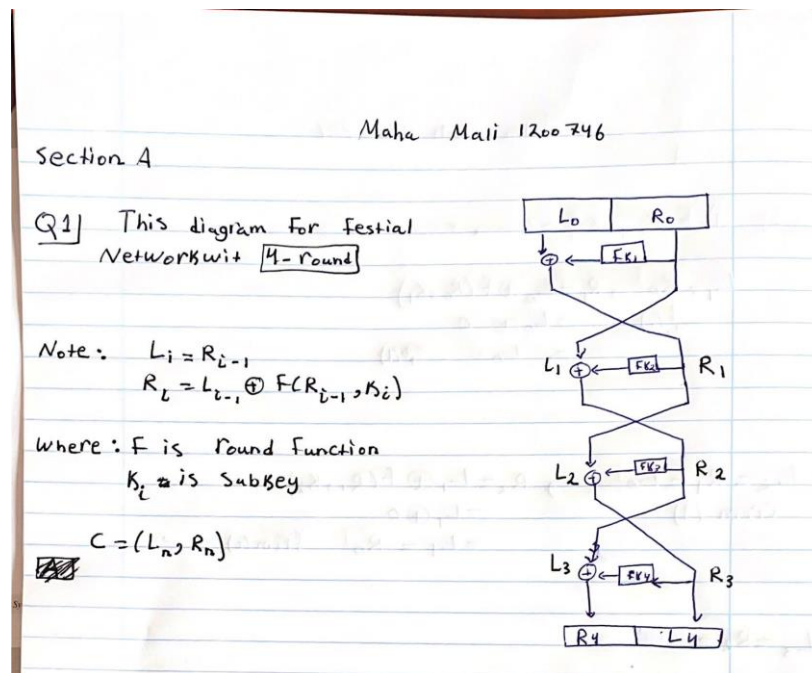


Figure 1: Feistel Network With 4 Round

Part A

[A] $F(R_{i-1}, K_i) = 0$

$L_1 = R_0$, $R_1 = L_0 \oplus F(R_0, K_1) = L_0 \oplus 0 = L_0$

$L_2 = R_1 = L_0$, $R_2 = L_1 \oplus F(R_1, K_2) = L_1 \oplus 0 = L_1 = R_0$

$L_3 = R_2 = R_0$, $R_3 = L_2 \oplus F(R_2, K_3) = L_2 \oplus 0 = L_2 = R_1 = L_0$

$L_4 = R_3 = L_0$, $R_4 = L_3 \oplus F(R_3, K_4) = L_3 \oplus 0 = L_3 = R_2 = R_0$

$C = (L_4, R_4) = (L_0, R_0)^*$

Figure 2: Question 1 Part-A

Part B

B $f(R_{i-1}, K_i) = R_{i-1}$ (Maha Mali 1200746)

$L_1 = R_0$, $R_1 = L_0 \oplus f(R_0, K_1) = L_0 \oplus R_0$

$L_2 = R_1 = L_0 \oplus R_0$, $R_2 = L_1 \oplus f(R_1, K_2) = R_0 \oplus R_1 = \cancel{R_0} \oplus L_0 \oplus \cancel{R_0} = L_0$

$L_3 = R_2 = L_0$, $R_3 = L_2 \oplus f(R_2, K_3) = L_2 \oplus R_2 = \cancel{L_0} \oplus R_0 \oplus \cancel{L_0} = R_0$

$L_4 = R_3 = R_0$, $R_4 = L_3 \oplus f(R_3, K_4) = L_0 \oplus R_3 = L_0 \oplus R_0$

$C = (L_4, R_4) = (R_0, L_0 \oplus R_0)$ *

Figure 3: Question 1 Part-B

Part C

C $f(R_{i-1}, K_i) = R_{i-1} \oplus K_i$ (Maha Mali 1200746)

$L_1 = R_0$, $R_1 = L_0 \oplus f(R_0, K_1) = L_0 \oplus R_0 \oplus K_1$

$L_2 = R_1 = L_0 \oplus R_0 \oplus K_1$, $R_2 = L_1 \oplus f(R_1, K_2) = R_0 \oplus R_1 \oplus K_2$

$\quad \quad \quad = \cancel{R_0} \oplus L_0 \oplus \cancel{R_0} \oplus K_1 \oplus K_2$

$\quad \quad \quad = L_0 \oplus K_1 \oplus K_2$

$L_3 = R_2 = L_0 \oplus K_1 \oplus K_2$, $R_3 = L_2 \oplus f(R_2, K_3) = L_0 \oplus R_0 \oplus K_1 \oplus R_2 \oplus K_3$

$\quad \quad \quad = \cancel{L_0} \oplus R_0 \oplus \cancel{K_1} \oplus \cancel{L_0} \oplus \cancel{K_1} \oplus K_2 \oplus K_3$

$\quad \quad \quad = R_0 \oplus K_2 \oplus K_3$

$L_4 = R_3 = R_0 \oplus K_2 \oplus K_3$, $R_4 = L_3 \oplus f(R_3, K_4) = L_0 \oplus K_1 \oplus K_2 \oplus R_3 \oplus K_4$

$\quad \quad \quad = L_0 \oplus K_1 \oplus \cancel{K_2} \oplus R_0 \oplus \cancel{K_2} \oplus K_3 \oplus K_4$

$\quad \quad \quad = L_0 \oplus K_1 \oplus R_0 \oplus K_3 \oplus K_4$

$C = (L_4, R_4) = (R_0 \oplus K_2 \oplus K_3, L_0 \oplus K_1 \oplus R_0 \oplus K_3 \oplus K_4)$ *

Figure 4: Question 1 Part-C

Question 2

Part A

Diffusion and confusion are two characteristics that help to create a safe encryption. Both confusion and diffusion are employed to stop the original message from being sent or to stop the encryption key from being discovered.[1]

Confusion: confusion is a cryptography method designed to make the cipher text more complex. The approach makes sure that the ciphertext hides any information about the plaintext. The provided approach maintains as complex of a link as possible between the value of the encryption key and the statistics of the encrypted text.[1]

The way the key was utilized to create the ciphertext is so complex that even with some control over the ciphertext statistics, so the attacker would not be able to find out the key.[1]

Diffusion: A cryptographic method known as diffusion was developed to make the plaintext more redundant and hidden its statistical structure in order to prevent attempts to figure out the key.[1]

No one can figure out the original key because of the complex relationship between the long-range statistics of the ciphertext and the statistical structure of the plaintext which might disappear during diffusion. [1]

This is done by distributing each plaintext digit across a large number of ciphertext digits. For example, if a single bit of the plaintext changes the entire ciphertext must be affected or the change must occur on the entire ciphertext.[1]

Features	Confusion	Diffusion
Definition	It is a cryptography technique utilized to create vague ciphertext.	It is employed to generate cryptic plain texts.
Achieved through	It is achieved via the substitution technique.	It is achieved via the transposition technique.
Seeks to	The relationship between the ciphertext statistics and the encryption key value is complicated.	The plain text's statistical structure is dispersed into the ciphertext's long-range statistics.
Used by	It utilizes only block cipher.	It utilizes both stream and block cipher.
Modifications	If one bit in secret is changed, most bits in the cipher text will be changed.	If one image within the plain text changes, most images within the cipher text will also change.
Resultant	Vagueness is increased	Redundancy is increased
Relations	It conceals the relation between the key and the ciphertext.	It conceals the relation between the plaintext and the ciphertext.

Figure 5: Difference Between Confusion & Diffusion [2]

Part B

Confusion in DES is caused by unique boxes known as **S-boxes**. These boxes take in a group of 6 bits and give out a completely other set of 4 bits. This procedure is similar to a secret in that the output may be completely changed through changing a small number of bits in the input. Anyone trying to estimate the output without knowing the secret key will find it extremely difficult to do. So, DES confusion might be compared to a challenge in which one small change in the initial picture gives an entirely different solution.

Part C

In DES diffusion is accomplished by use of permutation operations. Diffusion is built into DES by the **Expansion boxes** which is applied in permutation, which distribute each bit's effect over a number of bits in the achieving success rounds. In order to guarantee that a change in one bit of the input affects several bits in the output, the permutation operation rearranges the bits. This enables the information's spread across the ciphertext and dissipation of the statistical structure.

Question 3

Maha Mali 1200746

Q3 Compute $(345^{28567} \times 23^{567} + 1078) \mod 29$, given 29 is prime

I will use Fermat little theorem to solve this

Question $\Rightarrow \frac{a^{p-1}}{\text{integer}} \equiv 1 \mod p$ \hookrightarrow primenumber

$\phi(p) = p-1$
 $= 29-1$
 $= 28$

Sol: $= (345^{28560+7} \times 23^{560+7} + 1078) \mod 29$

$= (345^{10 \times 28 + 7} \times 23^{20 \times 28 + 7} + 1078) \mod 29$

$= \left[(345^{10 \times 28}) (345^7) (23^{20 \times 28}) (23^7) + 1078 \right] \mod 29$

\hookrightarrow Fermat rule \hookrightarrow Fermat rule

$= [(345^7) (23^7) + 1078] \mod 29$

$= [(23 \times 15)^7 (23^7) + 1078] \mod 29$

$= [(23)^{7 \times 2} (15)^7 + (7^2 \times 22)] \mod 29$

$= [(3 \times 5)^7 \times 23^2 + (2 \times 7^2 \times 11)] \mod 29$

$= (12 \times 28) \mod 29 + (2 \times 20 \times 11) \mod 29$

$= (17 \times 1 + 5) \mod 29$

$= 22 \mod 29$

answer = 22

Figure 6: Question 3 Solution

Question 4

Part A

Maha Mali 1200746

Q4) A) $\gcd(999, 19)$ using Extend Euclidean Algorithm

$$999 = (52) \cdot 19 + 11 \quad \text{remainder} = 11$$

$$19 = (1) \cdot 11 + 8$$

$$11 = (1) \cdot 8 + 3$$

$$8 = (2) \cdot 3 + 2$$

$$3 = (1) \cdot 2 + 1 \rightarrow \text{This is gcd} \Rightarrow 1$$

$$2 = (2) \cdot 1 + 0 \text{ stop}$$

$$\gcd(999, 19) = 1$$

Figure 7: Question 4-part A Solution

Part B

B) linear Combination of 999 and 19

From the equation in part A we start from equation *

$$1 = 1 \cdot 3 - 1 \cdot 2$$

$$1 = 1 \cdot 3 - 1 \cdot (8 - 2 \cdot 3)$$

$$1 = -1 \cdot 8 + 3 \cdot 3$$

$$1 = -1 \cdot 8 + 3 \cdot (11 - 1 \cdot 8)$$

$$1 = 3 \cdot 11 - 4 \cdot 8$$

$$1 = 3 \cdot 11 - 4 \cdot (19 - 1 \cdot 11)$$

$$1 = -4 \cdot 19 + 7 \cdot 11$$

$$1 = -4 \cdot 19 + 7 \cdot (999 - 52 \cdot 19)$$

$$1 = 7 \cdot 999 - 368 \cdot 19 \quad *$$

$999x + 19y = 1$ has solution
of $(x, y) = (7, -368)$

Figure 8: Question 4-part B Solution

Part C

c) multiplicative inverse 19 mod 999

$$19^{-1} \pmod{999}$$

$$s_0 = 1, s_1 = 0$$

$$t_0 = 0, t_1 = 1$$

$$r_0 = 999, r_1 = 19$$

L	Quotient $q = r_0 \div r_1$	Reminder $r = r_0 - q r_1$	$s = s_0 - q s_1$	$t = t_0 - q t_1$
1		999	1	0
2		19	0	1
3	$999 \div 19 = 52$	$999 - 52 \times 19 = 11$	$1 - 52 \times 0 = 1$	$0 - 52 \times 1 = -52$
4	$19 \div 11 = 1$	$19 - 1 \times 11 = 8$	$0 - 1 \times 1 = -1$	$1 - 1 \times -52 = 53$
5	$11 \div 8 = 1$	$11 - 1 \times 8 = 3$	$1 - 1 \times -1 = 2$	$-52 - 1 \times 53 = -105$
6	$8 \div 3 = 2$	$8 - 2 \times 3 = 2$	$-1 - 2 \times 2 = -5$	$53 - 2 \times -105 = 263$
7	$3 \div 2 = 1$	$3 - 1 \times 2 = 1$	$2 - 1 \times -5 = 7$	$-105 - 1 \times 263 = -368$
8	$2 \div 1 = 2$	$2 - 2 \times 1 = 0$ stop	$-5 - 2 \times 7 = -19$	$263 - 2 \times -368 = 999$

* We take row ~~2~~ 7 as answer because it is the last non zero row for reminder $r=1$ (gcd)

$$s = 7$$

$t = -368$, because t negative we add 999

$$t = -368 + 999 = 631$$

$$19^{-1} \pmod{999} = 631$$

Figure 9: Question 4-part C Solution

Part D

D) multiplicative inverse of 999 mod 19

$$999^{-1} \pmod{19}$$

$$s_0 = 1, s_1 = 0$$

$$t_0 = 0, t_1 = 1$$

$$r_0 = 19, r_1 = 999$$

i	Quotient $q = r_0 \div r_1$	Reminder $r = r_0 - q r_1$	$s = s_0 - q s_1$	$t = t_0 - q t_1$
1		19	1	0
2		999	0	1
3	$19 \div 999 = 0$	$19 - 0 \times 999 = 19$	$1 - 0 \times 0 = 1$	$0 - 0 \times 1 = 0$
4	$999 \div 19 = 52$	$999 - 52 \times 19 = 11$	$0 - 52 \times 1 = -52$	$1 - 52 \times 0 = 1$
5	$19 \div 11 = 1$	$19 - 1 \times 11 = 8$	$1 - 1 \times -52 = 53$	$0 - 1 \times 1 = -1$
6	$11 \div 8 = 1$	$11 - 1 \times 8 = 3$	$-52 - 1 \times 53 = -105$	$1 - 1 \times -1 = 2$
7	$8 \div 3 = 2$	$8 - 2 \times 3 = 2$	$53 - 2 \times -105 = 263$	$-1 - 2 \times 2 = -5$
8	$3 \div 2 = 1$	$3 - 1 \times 2 = 1$	$-105 - 1 \times 263 = -368$	$2 - 1 \times -5 = 7$
9	$2 \div 1 = 2$	$2 - 2 \times 1 = 0$	$263 - 2 \times -368 = 999$	$-5 - 2 \times 7 = -19$
		stop		

* We take row 8 as answer because it is the last non zero row for reminder $r=1$ (gcd)

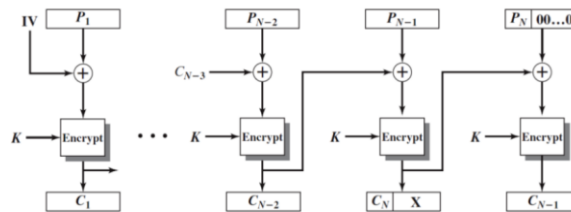
$$s = -368, t = 7$$

$$999^{-1} \pmod{19} = 7$$

Figure 10: Question 4-part D Solution

Section B

Question 5



⊗ Decryption Sequence:

$$P_i = C_{i-1} \oplus \text{Dec}(C_i, K)$$

Part A

Q5) A) To find P_N Maha Mali 1200746

$$C_{N-1} = \text{Enc}((P_N || 00\dots 0) \oplus (C_N || X), K) \quad || \Rightarrow \text{concatination}$$

Decryption each side:

$$\text{Dec}(C_{N-1}, K) = (P_N || 00\dots 0) \oplus (C_N || X)$$

$$\text{we need } P_N \Rightarrow P_N || 00\dots 0 = \text{Dec}(C_{N-1}, K) \oplus (C_N || X)$$

We take left part to find P_N (P_N is the left hand portion of $P_N || 00\dots 0$)

To find P_{N-1} :

$$C_N || X = \text{Enc}((P_{N-1} \oplus C_{N-2}), K)$$

Decryption each side:

$$\text{Dec}(C_N || X, K) = P_{N-1} \oplus C_{N-2}$$

$$P_{N-1} = \text{Dec}(C_N || X, K) \oplus C_{N-2}$$

To find P_{N-2} :

$$C_{N-2} = \text{Enc}(P_{N-2} \oplus C_{N-3}, K)$$

Decryption each side:

$$\text{DEC}(C_{N-2}, K) = P_{N-2} \oplus C_{N-3}$$

$$P_{N-2} = \text{DEC}(C_{N-2}, K) \oplus C_{N-3}$$

To find P_1 :

$$C_1 = \text{Enc}(P_1 \oplus \text{IV}, K)$$

Decryption each side:

$$\text{DEC}(C_1, K) = P_1 \oplus \text{IV}$$

$$P_1 = \text{IV} \oplus \text{DEC}(C_1, K)$$

Figure 11: Question 5-part A solution

Part B

Q5) B) if a single bit error occurs in the storage of cipher text C_i (20)

Assume error happened to the ciphertext $C_1 \equiv L \equiv 1$

\Rightarrow this cipher text will be used to Recover P_1 & P_2 because the Decryption equation is:

$$\text{Dec}(C_1, K) = IV \oplus P_1$$

$IV \Rightarrow$ Initial Vector

$$\therefore P_1 = \text{Dec}(C_1, K) \oplus IV$$

\Rightarrow but C_1 has an error

So let error $C_1 = M$

$$P_1 = \text{Dec}(M, K) \oplus IV \neq \text{Dec}(C_1, K) \oplus IV$$

Also $P_2 = \text{Dec}(C_2, K) \oplus C_1 \Rightarrow$ but $C_1 = M$ ciphertext with error

$$\therefore P_2 = \text{Dec}(C_2, K) \oplus M \neq \text{Dec}(C_2, K) \oplus C_1$$

$\therefore P_1$ & P_2 will not be restored correctly by the Decryption Algorithm

Figure 12: Question 5-part B solution

Section C

Question 6

Part A

Q6] A) The question will be solve using Birthday Attack Approach

Given hash function generate 12 bit output \Rightarrow

$$N = 2^{12} = 4096 \text{ possible output}$$

Given: 1024 Randomly selected message

$$\text{expected number of collision} = \frac{q(q-1)}{2N} \text{ where } q \text{ is}$$

Randomly selected

message $\Rightarrow 1024$

$$= \frac{1024(1024-1)}{2(4096)}$$

$$= \frac{1047552}{8192} = 127.875$$

\Rightarrow 128 Collision will found

Figure 13: Question 6-part A solution

Part B

Q6) B) What is the expected number of hashes that must be computed to find 25 collisions?

Given number of collision = 25 collisions

Given Hash function generates 12 bit output \Rightarrow

$$N = 2^{12}$$

Required to find number of hashes which is q

$$\text{number of collision} = \frac{q(q-1)}{2N}$$

$$q = \sqrt{2N * \text{number of collision}} = \sqrt{2 * 2^{12} * 25}$$

$$= \sqrt{204800}$$

$$= 452.54 \approx 453 \text{ number of hashes}$$

Figure 14: Question 6-part B Solution

Question 7

Part A

Maha Mali 1200746

Q7) A) $H(m) = \sum_{i=1}^I D_i \bmod n$, $m = D_1, D_2, \dots, D_I$

$H(m) \bmod n$, not pre image resistance (not satisfy one way property)

pre image resistance: means that given a hash Value h it should be computationally infeasible to find a message m such that $H(m) = h$

\Rightarrow in this case if we know the hash Value h , we can find multiple messages m that satisfy $H(m) = h$

\Rightarrow This is because there are different combination of D_i that can result the same sum when taken modulo n

Example: $n=10$, $I=2$, $H(m) = \sum_{i=1}^2 D_i \bmod 10$, hash Value $h=7$

Sol: There are multiple solutions :-

1) if $D_1=3, D_2=4 \Rightarrow H(m) = (3+4) \bmod 10 = 7$

2) if $D_1=5, D_2=2 \Rightarrow H(m) = (5+2) \bmod 10 = 7$

\Rightarrow We have two different message $m_1 = (3, 4)$ and $m_2 = (5, 2)$ that hash the same Value $h=7$. So this function not pre image because it is not satisfy the pre image condition. If n is not large enough.

\Rightarrow An Attacker could easily find multiple message that hash the same Value

Figure 15: Question 7-part A solution

Part B

B) **Collision Resistance**: hash function should be computationally infeasible to find two different inputs $m_1 \neq m_2$ such that $H(m_1) = H(m_2)$

$$H(m) = \sum_{i=1}^I D_i^2 \bmod n, \quad m = D_1, D_2, \dots, D_I$$

Example: $n=10, I=2, H(m) = (D_1^2 + D_2^2) \bmod 10$

$$m_1 = (2, 1) \Rightarrow H(m_1) = (2^2 + 1^2) \bmod 10 = \boxed{5}$$

$$m_2 = (3, 1) \Rightarrow H(m_2) = (3^2 + 1^2) \bmod 10 = \boxed{2}$$

$H(m_1) \neq H(m_2) \Rightarrow$ so these two messages do not collision

\Rightarrow The square operation introduce a **non linearity** into the hash function making it **less** likely to find collision

\Rightarrow The collision resistance of the hash function depends on the specifics of the **mathematical operations** and the size n

\Rightarrow if n is large this most likely have satisfy collision Resistance.

Figure 16: Question 7-part B solution

Part C

(Q7) C) $m = (189, 632, 900, 722, 349)$, $n = 989$

$$H(m) = \sum_{i=1}^I D_i^2 \pmod{n}$$

$$H(m) = (189^2 + 632^2 + 900^2 + 722^2 + 349^2) \pmod{989}$$

$$H(m) = (35721 + 399424 + 810000 + 521284 + 121801) \pmod{989}$$

$$= 1888230 \pmod{989}$$

$H(m) = 229$

Figure 17: Question 7-part C solution

References

[1] <https://techdifferences.com/difference-between-confusion-and-diffusion.html> .

Accessed on 18-1-2024 at 10:50 AM.

[2] <https://www.javatpoint.com/difference-between-confusion-and-diffusion-in-cryptography> .

Accessed on 18-1-2024 at 11:50 AM.

[3] <https://www.youtube.com/watch?v=3Cb0ys-jppU> .

Accessed on 20-1-2024 at 11:30 AM.