Vaibhav Sharma
200365101
Assignment 2 – Cs435

1. (10 points) Finish the following table:

Assignment 2

1 →

	Encrypt	Decrypt
CBC		$P_i = D_K(C_i) \oplus C_{i-1}$
CFB	$C_i = E_K(C_{i-1}) \oplus P_i$ $C_0 = IV$	$P_i = E_K(C_{i-1}) \oplus C_i$, $C_0 = IV$
OFB	$C_j = P_j \oplus O_j$ $O_j = E_K(I_j)$ $I_j = O_{j-1}$ $I_0 = IV$	$P_j = C_j \oplus O_j$
CTR	$C_i = E(K_1, counter) \oplus P_i$ $C_j = E(K_1, counter_j) \oplus P_j$	$P_i = E(K_1, counter) \oplus C_i$ $P_j = E(K_1, counter_j) \oplus C_j$

Solution –

2. (15 points)

Alice and Bob agree to communicate privately via email using a scheme based on RC4, but they want to avoid using a new secret key for each transmission. Alice and Bob privately agree on a 128-bit key k. To encrypt a message m, consisting of a string of bits, the following procedure is used.

1. Choose a random 80-bit value v
2. Generate the ciphertext $c = \mathrm{RC4}(v \parallel k) \oplus m$
3. Send the bit string $(v \parallel c)$

a. Suppose Alice uses this procedure to send a message m to Bob. Describe how Bob can recover the message m from $(v \parallel c)$ using k.
b. If an adversary observes several values $(v_1 \parallel c_1), (v_2 \parallel c_2), \ldots$ transmitted between Alice and Bob, how can he/she determine when the same key stream has been used to encrypt two messages?
c. Approximately how many messages can Alice expect to send before the same key stream will be used twice? Use the result from the birthday paradox described
d. What does this imply about the lifetime of the key k (i.e., the number of messages that can be encrypted using k)?

Solution -

A-

the value of v, c and k is not unknown so we can decrypt the message by using rc4 (v||k)⊕ c

B -

The adversary can validate the same key stream used to encrypt both Mi and Mj if we can confirm Vi = Vj for unique value of i and j

C -

The selection is random key is produced from 80bit v. so we deduce that key will be repeated after every key has been used once which is (sq.root of 2^80)

D -

We can find the lifetime of a key from the equation used in C

(sq.root of 2^80) = 2^40

3. (10 points)

Compare AES to DES. For each of the following elements of DES, indicate the comparable element in AES or explain why it is not needed in AES.

a. XOR of subkey material with the input to the f function
b. XOR of the f function output with the left half of the block
c. f function
d. permutation P
e. swapping of halves of the block

Solution -

A-

The added round key stage in all 10 rounds plays the role of xor of subkey in AES

B -

AES is process in parallel so XOR of the f function output with the left half of the block is not required.

C-
AES have substitution bytes, shift rows, added roundley and mix columns which indirectly plays the role of f function

D-
The shift rows during 10 rounds in AES is the closest to permutation P in DES

E-
Same answers a B

4. (10 points)
In AES, show the first eight words of the key expansion for a 128-bit key of all zeros.

Solution - The first 4 subkeys are zeros

W0, W1, W2, W3 = 00000000
W5 = temp XOR W[i-4]
W5 = 00000000 XOR 00000000
W5 = 62636363

Similarly,
W6 = temp (62636363) XOR W[i-4]
W6 = 6263636363 XOR 00000000
W6 = 62636363

W7 = 62636363
W8 = 62636363

5. (20 points)

Given the plaintext {000102030405060708090A0B0C0D0E0F} and the key {01010101010101010101010101010101}:

a. Show the original contents of **State**, displayed as a 4×4 matrix.
b. Show the value of **State** after initial AddRoundKey.
c. Show the value of **State** after SubBytes.
d. Show the value of **State** after ShiftRows.
e. Show the value of **State** after MixColumns.

Solution -

5

a) $= \begin{bmatrix} 00 & 04 & 08 & 0C \\ 01 & 05 & 09 & 0D \\ 02 & 06 & 0A & 0E \\ 03 & 07 & 0B & 0F \end{bmatrix}$

b) adding 0^{th} round key

$$key = \begin{bmatrix} 01 & 01 & 01 & 01 \\ 01 & 01 & 01 & 01 \\ 01 & 01 & 01 & 01 \\ 01 & 01 & 01 & 01 \end{bmatrix}$$

$$\begin{bmatrix} 00 & 04 & 08 & 0C \\ 01 & 05 & 09 & 0D \\ 02 & 06 & 0A & 0E \\ 03 & 07 & 0B & 0F \end{bmatrix} \oplus \begin{bmatrix} 01 & 01 & 01 & 01 \\ 01 & 01 & 01 & 01 \\ 01 & 01 & 01 & 01 \\ 01 & 01 & 01 & 01 \end{bmatrix}$$

$$= \begin{bmatrix} 01 & 05 & 09 & 0D \\ 00 & 04 & 08 & 0C \\ 03 & 07 & 0B & 0F \\ 02 & 06 & 0A & 0E \end{bmatrix}$$

c State after SubBytes

$$\begin{bmatrix} 01 & 05 & 09 & 0D \\ 00 & 04 & 08 & 0C \\ 03 & 07 & 0B & 0F \\ 02 & 06 & 0A & 0E \end{bmatrix} \rightarrow \begin{bmatrix} 7C & 6B & 01 & D7 \\ 63 & F2 & 30 & FE \\ 7B & C5 & 2B & 76 \\ 77 & 6F & 67 & AB \end{bmatrix}$$

d State after Shifting Rows

$$\begin{bmatrix} 7C & 6B & 01 & D7 \\ 63 & F2 & 30 & FE \\ 7B & C5 & 2B & 76 \\ 77 & 6F & 67 & AB \end{bmatrix} \rightarrow \begin{bmatrix} 7C & 6B & 01 & D7 \\ F2 & 30 & FE & 63 \\ 2B & 76 & 7B & C5 \\ AB & 77 & 6F & 67 \end{bmatrix}$$

e State after mixing Columns

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} 7C & 6B & 01 & D7 \\ F2 & 30 & FE & 63 \\ 2B & 76 & 7B & C5 \\ AB & 77 & 6F & 67 \end{bmatrix}$$

$$= \begin{bmatrix} 74 & E7 & 0F & A2 \\ 55 & E6 & 04 & 22 \\ 3E & 2E & B8 & 8C \\ F6 & 15 & 58 & 0B \end{bmatrix}$$

6. (15 points) Perform encryption and decryption using the RSA algorithm, for the following:

a. $p = 3; q = 11, e = 7; M = 5$
b. $p = 5; q = 11, e = 3; M = 9$
c. $p = 7; q = 11, e = 17; M = 8$
d. $p = 11; q = 13, e = 11; M = 7$
e. $p = 17; q = 31, e = 7; M = 2$

Hint: Decryption is not as hard as you think; use some finesse.

Solution -

6 (a)

$n = pq = 3 \times 11 = 33$

$\phi(n) = (p-1)(q-1) = 20$

$\gcd(20, 7) = 1$

$d = e^{-1} (\mathrm{mod}\ \phi(n))$

$d \times e \bmod \phi(n) = 1$

$7d \bmod 20 = 1$

$d = 3$

Public key $= \{e, n\} = \{7, 33\}$

private key $= \{d, n\} = \{3, 33\}$

Encryption:

$5^7 \bmod 33$

$= 14$

decryption:

$14^3 \bmod 33$

$= 5$

2 $n = 5 \times 11 = 5$

$\phi(n) = (5-1)(11-1) = 40$

$\gcd(\phi(n), e) = \gcd(40, 3) = 1$

$d = e^{-1} \pmod{\phi(n)}$

$d \times e \bmod \phi(n)) = 1$

$3d \bmod 40 = 1$

$d = 27$ ——— ①

$pu = \{e, n\} = \{3, 55\}$

$br = \{d, n\} = \{27, 55\}$

Encryption =

$C = m^e \bmod n = 9^3 \bmod 55 = 14$

Decryption =

$M = c^d \bmod n = 14^{27} \bmod 55 = 9$

3. $n = (7)(11) = 77$

$\phi(n) = (7-1)(11-1) = 60$

$\gcd(\phi(n), e) = \gcd(60, 17) = 1$

$d = e^{-1} \bmod \phi(n)$

$d \times e \bmod 60 = 1$

$17d \bmod 60 = 1$

$d = 53$ — 1

$pu = \{17, 77\}$

$pr = \{53, 77\}$

Encryption →

$C = m^e \bmod n = 8^{17} \bmod 77 = 57$

Decryption →

$m = c^d \bmod n = 57^{53} \bmod 77 = 8$

4. $n = (11)(13) = 143$

$\phi(n) = (11-1)(13-1) = 120$

$\gcd(\phi(n), e) = \gcd(120, 11) = 1$

$d = e^{-1} \bmod \phi(n)$

$d \times e \bmod 120 = 1$

$11d \bmod 120 = 1$

$d = 11$ ——— ①

$Pu = \{11, 143\}$

$Pr = \{11, 143\}$

Encryption ->

$C = m^e \bmod n = 7^{11} \bmod 143 = 106$

Decryption ->

$m = C^d \bmod n = 106^{11} \bmod 143 = 7$

5 $n = (17) * (31)$

$\phi n = (17-1)(31-1)$

$= 480$

$\gcd(\phi(n), e) = \gcd(480, 7) = 1$

$d = e^{-1} \bmod \phi n$

$d \times e \bmod 480 = 1$

$7d \bmod 480 = 1$

$d = 343$ — 1

$pu = \{7, 527\}$

$pr = \{343, 527\}$

Encryption $\Rightarrow 2^7 \bmod 527 = 128$

Decryption $\Rightarrow 128^{343} \bmod 527 = 2$

7. (10 points) In the RSA public-key encryption scheme, each user has a public key, e, and a private
key, d. Suppose Bob leaks his private key. Rather than generating a new modulus, he decides to
generate a new public and a new private key. Is this safe?

Solution -
Looking at how RSA algorithm works,
If a hacker have pr1(private key) and pu1(public key) and pu2 then one can produce p and q by using the chinese remainder theorm to deduce the prime numbers used. Once the hacker knows p and q, then one can produce the plain and cipher text. So, it's not safe for bob to generate new public and private keys based on old modules.

8. (10 points) In using the RSA algorithm, if a small number of repeated encodings give back the
plaintext, what is the likely cause?

Solution -

Cycle attacks can be reason if RSA algorithm is giving back plain text after small number of repeated encodings.