Information Security homework :-

1. 8 letter password → encoded by ASCII

there are 128 possible characters

and each character is represented by 7 bits.

(i). Keyspace needed:

$$128\text{-character} = 2^7$$

$$8 \text{ letters password} : (2^7)^8 = 2^{56}$$

(ii). Key length in bits

The key length can be mentioned in the form of 2 to the power of certain value.

$\therefore 2^{56} \Rightarrow 56 \rightarrow$ length of the key in bits.

(iii) what if there are only 26 lower case alphabets used.

then

$$(26)^8 = (2 * 13)^8$$

by taking log. and antilog

$$8 \log_2 26 \Rightarrow \text{antilog of this gives}$$

$$= 37.06$$

length of the key in bits is 37.

(2.) for $Z_n = \{0, 1, 2 \cdots n-1\}$, for any $a \in Z$ there is a multiplicative inverse if $\gcd(a, n) = 1$.

(i) $Z_4 = \{0, 1, 2, 3\}$

the number 2 doesn't have the multiplicative inverse

(ii) $Z_6 = \{0, 1, 2, 3, 4, 5\}$.

The numbers that dont have the multiplicative inverse are 2, 3, 4

since $\gcd(2, 6) \neq 1$, $\gcd(3, 6) \neq 1$, $\gcd(4, 6) \neq 1$.

(iii). Multiplicative inverse exists for all the elements in Z_5.

$Z_5 = \{0, 1, 2, 3, 4\}$.

Since all the elements present in Z_5 is Co-prime with 5 then they have the gcd of 1.

∴ there exist Multiplicative inverse for all.

(3). Multiplicative inverse of 5 in Z_{11}, Z_{12}, Z_{13}.

(i) the Multiplicative inverse of 5 in Z_{11}.

the inverse of 5 in 9 in Z_{11}

Since

$9 * 5 = 45 \mod 11 \Rightarrow 1$

(ii) the Multiplicative inverse of 5 in Z_{12} is 5, since $5 * 5 = 25 \mod 12 \Rightarrow 1$

(iii) The Multiplicative inverse of 5 in Z_{13} is 8 since $8 * 5 = 40 \mod 13 = 1$

Q.

(i) $\phi(100)$

generally $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$ such that

$GCD(m, n) = 1$

if p is a prime number

$$\phi(p^n) = p^n - p^{(n-1)} \quad (\text{or}) \quad \phi(p) = p-1$$

$\therefore \phi(100) = \phi(25) * \phi(4)$

$= \phi(5^2) * \phi(2^2)$

$= (5^2 - 5^1) * (2^2 - 2^1)$

$= (20) * 2 = 40$ is the totient of 100

(ii) $\phi(40) = \phi(8) * \phi(5)$

$= \phi(2^3) * \phi(5)$

$= \phi(2^3 - 2^2) * 4$

$= (8-4) * 4$

$= 4 * 4$

$= 16$ is the totient of 40

(iii) $\phi(101)$

Since 101 is a prime number

$\phi(101) = 101 - 1$

$= 100$ is the totient of 101.

(5) (i) $x_1 = 000000$, $x_2 = 000001$

(ii) $x_1 = 111111$, $x_2 = 100000$

verify the non-linearity of s-box 1 ?

$$s(x_1) + s(x_2) \neq s(x_1 + x_2)$$

(i). $x_1 = 000000$ $= 00 = 0^{th}$ row
$0000 = 0^{th}$ column $= 14$.

$x_2 = 000001$ $01 = 1^{st}$ row $= 0$
$0000 = 0^{th}$ column

$x_1 + x_2 = 000001$ $01 = 1^{st}$ row $= 0$
$0000 = 0^{th}$ column

$\therefore 0 \neq 0 + 14$ $\quad s_1(x_1 + x_2) \neq s(x_1) + s(x_2)$.

(ii) $x_1 = 111111$ $\quad x_2 = 100000$

$x_1 = 111111$ $11 = 3^{rd}$ row $= 13$
$1111 = 15^{th}$ column

$x_2 = 100000$ $10 = 2^{nd}$ row $= 4$
$0000 = 0^{th}$ column

$x_1 + x_2 = 011111$ $01 = 1^{st}$ row $= 8$
$1111 = 15^{th}$ column

$$s_1(x_1 + x_2) \neq s(x_1) + s(x_2)$$

$$8 \neq 13 + 4$$

Thus the non-linearity of the s-box is verified.

(6.) Explain the self-healing property of cipher block Chaining mode.

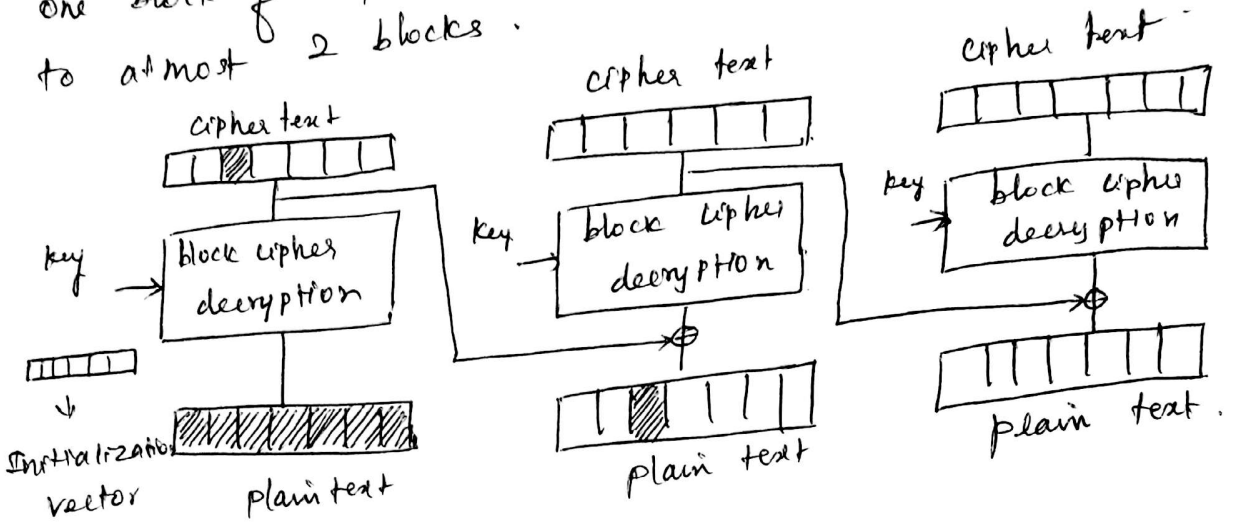
The cipher block chaining mode does the Exclusive-o the current plaintext with previous cipher text block

$C_0 = E_k (m_0 \oplus I)$

$C_i = E_k (m_i \oplus c_{i-1})$ → for $I > 0$

I = Initialization vector.

The self healing property in the CBC is that if one block of ciphertext is altered the error propagates to almost 2 blocks.



(7.)

(i). $P = 3 \quad q = 11 \; ; \; e = 7 \; ; \; M = 3$

final ciphertext:

$C = M^e \bmod N$

$N = p * q = 3 * 11 = 33$

$C = 3^7 \bmod 33$

$\boxed{C = 14.}$

(ii). $p = 5 \quad q = 17 \quad e = 3 \quad m = 9$

$C = M^e \bmod N$

$N = p * q = 5 * 17 = 85$

$C = 9^3 \bmod 85$

$= 729 \bmod 85$

$\boxed{C = 49}$

(8) $p = 11$; $q = 13$ · $e = 11$; $c = 106$

find the plaintext.

$$M = c^d \bmod N$$

$$N = p * q = 11 * 13 = 143$$

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

$$\phi(N) = \phi(143) = \phi(11) * \phi(13)$$

$$= 10 * 12$$

$$= 120$$

$$d = e^{-1} \bmod N$$

$$= (11)^{-1} \bmod 120$$

$$= \frac{1}{11} \bmod 120$$

$$d = 11$$

$$M = (106)^{11} \bmod 143$$

plaintext = 7

(9) $c = 10$ $e = 5$, $n = 35$

find plaintext

$$M = c^d \bmod N$$

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

$$\phi(N) = \phi(5) * \phi(7)$$

$$= 4 * 6$$

$$= 24.$$

$$d = 5^{-1} \bmod 24$$

$$= 5$$

$$M = 10^5 \bmod 35 \Rightarrow 5$$

plaintext = 5

(10)

Common prime = 71 = P

Primitive root = 7 = α

(i). Alice Private key $K_{pr,A} = 5$ what is the public key

By Diffie-Hellman key exchange method

$$K_{pub,A} = \alpha^a \bmod P$$

$$= 7^5 \bmod 71$$

$$= 51$$

(ii). Bob's private key $K_{pr,b} = 12$ what is the public key.

$$K_{pub,b} = \alpha^b \bmod P$$

$$= 7^{12} \bmod 71$$

$$= 4.$$

(iii). shared key:

To find the shared key.

$$(K_{pub,B})^{K_{pr,A}} \bmod P = (4)^5 \bmod 71 = 30$$

$$(K_{pub,A})^{K_{pr,B}} \bmod p = (51)^{12} \bmod 71 = 30$$

$\therefore$ the shared key = 30.