04/23/22. Chapter -4:-

1) Diffie-Hellman:-

We know that, prime(P) = 17 and generator(g) = 3.

Alice's private exponent $a = 9$ and,

Bob's private exponent $b = 5$.

a.) Alice

Alice to Bob
$g^a \bmod P$.

let $Y_A = g^a \bmod P$.

$y_A = 3^9 \bmod 17$.

$\therefore y_A = \underline{14}$.

Bob

Bob to Alice
$g^b \bmod P$.

let $Y_B = g^b \bmod P$.

$y_B = 3^5 \bmod 17$.

$\therefore y_B = \underline{5}$.

b.) Key generated by Alice

Let $K_1 = y_B^a \bmod P$

$K_1 = 5^9 \bmod 17$.

$\therefore K_1 = \underline{12}$.

Key generated by Bob

Let $K_2 = y_A^b \bmod P$.

$K_2 = 14^5 \bmod 17$.

$\therefore K_2 = \underline{12}$.

$\therefore \underline{K_1 = K_2}$.

c) Alice | Bob

a (Alice's private key) | b (Bob's private key)

$y_A = g^a \bmod p$ | $y_B = g^b \bmod p$.

y_A → Trudy ← y_B

$t = 7$

y_B' → $K_1 = (y_B')^a \bmod p$

y_A' → $K_2 = (y_A')^b \bmod p$.

$$y_A' = y_A^t \bmod p$$

$$y_B' = y_B^t \bmod p.$$

$\therefore y_A' = 14^7 \bmod 17$. (Since we know y_A)

$\therefore y_A' = 6.$

$\therefore y_B' = 5^7 \bmod 17$ (Since we know y_B)

$\therefore y_B' = 10.$

$\therefore K_1 = (y_B')^a \bmod p$ | $\therefore K_2 = (y_a')^b \bmod p$

$\therefore K_1 = (10)^9 \bmod 17$ | $\therefore K_2 = (6)^5 \bmod 17.$

$\therefore K_1 = 7.$ | $\therefore K_2 = 7.$

$\therefore K_1 = K_2.$

2.) <u>RSA asymmetric cipher:-</u>

we know that, $e = 7$ and $N = 221$.

a.) we know, Plain Text $(M) = 2$.

In RSA algorithm, the encryption formula is:

$$\text{Encrypted data} = (M^e) \bmod N.$$

$$\therefore \text{Encrypted data} = (2^7) \bmod 221 = \underline{128}$$

For the private key, we calculate prime factors of 'N', say 'P' and 'Q'.

$\therefore$ The prime Factorization of 'N', i.e 221 is 13×17.

Here, $P = 13$ and $Q = 17$.

Therefore by finding the prime factors, Trudy can easily calculate the private key of Bob and decrypt the data

b.) Private key is calculated as follows

$$d \times e \bmod ((P-1) \times (Q-1)) = 1$$

$$d \times 7 \bmod ((13-1) \times (17-1)) = 1$$

$$d \times 7 \bmod (12 \times 16) = 1$$

$$d \times 7 \bmod (192) = 1$$

$\therefore d = 55$ (Private key of Bob).

3.) Why is it a bad Idea to use the same RSA key pair for both signing and decryption?

Ans.) It is a bad Idea because,

→ The keys for signing and decryption have different requirements in terms of access control, and hence if there is a leak in the key, then the confidentiality of all the previous documents is at risk.

→ If the attacker tries to manipulate the private key holder, then it could lead to forgery and the damage will be massive if the key is lost.

Chapter-7:-

4.) problem 7 (Txt-Book, Pg: 255):-

a) Case, when Trudy wants to crack Alice's password with her dictionary.

We know that the size of the Trudy's dictionary $= 2^{30}$ words.

and the size of the hashed password file $= 2^{10}$ hashed passwords.

i) <u>Unsalted case:</u> Trudy's dictionary

words	precomputed hashes of words
1) word 1	$h(\text{words}_1) = y_1$
2) word 2	$h(\text{words}_2) = y_2$
⋮	⋮
2^{30}) word 2^{30}	$h(\text{word } 2^{30}) = y_{2^{30}}$.

→ The amount of work, Trudy needs to do, i.e.,

# of hashes Trudy needs to compute $= 0 \cdot \frac{1}{6} = 0$

→ The length of the passwords = 8 characters.

→ No. of possible values = 128.

∴ There are, $128^8 = 2^{56}$ different passwords are possible.

→ If Alice's password not in the dictonary, Trudy needs to compute $\frac{2^{56}}{2} = 2^{55}$

hashes on average.

$\therefore$ The expected amount of work for Trudy on average is,

$$\left(\frac{3}{4} \cdot 2^{55}\right).$$

b.) <u>salted case:-</u> Trudy dictonary

1) word 1

2) word 2

$\vdots$

2^{30}) word 2^{30}

Prob[Alice Picking a dictonary Pswd] $= \frac{1}{4}$.

Prob[Alice not Picking a dictonary Pswd] $= \frac{3}{4}$.

→ If Alice's Pswd is in the dictonary, Trudy on an avg needs to compute

$$\frac{2^{30}}{2} = 2^{29} \text{ hashes.}$$

→ In worst case, Trudy needs to compute 2^{30} dictonary hashes, if Alice picks a dictonary Password.

→ The expected amount of work on average Trudy needs to compute ψ.

$$\left(\frac{1}{4} \cdot 2^{29}\right)$$

∴ The total amount of work, Trudy needs to do for cracking Alice's password in the average case ψ:

$$\left(\frac{1}{4} \cdot 2^{29} + \frac{3}{4} \cdot 2^{55}\right).$$

and in the worst case, the total amount of work, Trudy needs to do for cracking Alice's Pswd ψ:

$$\left(\frac{1}{4} \cdot 2^{30} + \frac{3}{4} \cdot 2^{56}\right)$$

c) probability [1 Password appearing in Trudy's dictionary] $= \frac{1}{4}$.

Probability [1 Password not appearing in Trudy's dictionary] $= \frac{3}{4}$.

So, probability [$2^{10} = 1024$ passwords not appearing in Trudy's dictionary]

$$= \underbrace{\frac{3}{4} \times \frac{3}{4} \times \frac{3}{4} \times \cdots \times \frac{3}{4}}_{1024 \text{ times}} = \left(\frac{3}{4}\right)^{1024}.$$

$\therefore$ Probability [At least 1 password out of 2^{10} passwords appearing in Trudy's dictionary]

$$= 1 - \left(\frac{3}{4}\right)^{1024}$$

5.) <u>problem 10 (Text book, pg. 256):-</u>

→ The length of the passwords = 8 characters

→ No. of possible values = 64 values.

→ The size of the the Trudy's dictionary $= 2^{30}$ passwords.

→ The size of the hashed password file $= 256$ password hashes (2^8).

a) $\therefore$ There are $64^8 = (2^6)^8 = 2^{48}$ different passwords are possible.

b.) → If administrators pwd is not in the dictionary, Trudy need to compute $\frac{2^{48}}{2}$

$= 2^{47}$ hashes on average.

$\therefore$ The expected amount of work for Trudy on average is, $\left(\frac{3}{4} \cdot 2^{47}\right)$.

→ If administrator's pswd is in the dictionary, Trudy needs to compute $\frac{2^{30}}{2}$

$= 2^{29}$ hashes on average.

∴ The expected amount of work for Trudy on average is $\left(\frac{1}{4} \cdot 2^{29}\right)$.

∴ The total amount of work Trudy needs to do for cracking the administrator's password on average is

$$\frac{\left(\frac{1}{4} \cdot 2^{29} + \frac{3}{4} \cdot 2^{47}\right)}{64} \text{ seconds.}$$

c.) probability [1 Password appearing in Trudy's dictionary] $= \frac{1}{4}$.

Probability [1 Password not appearing in Trudy's dictionary] $= \frac{3}{4}$.

So,
Probability [$2^8 = 256$ passwords not appearing in Trudy's dictionary]

$$= \underbrace{\frac{3}{4} \times \frac{3}{4} \times \cdots \times \frac{3}{4}}_{256 \text{ times}} = \left(\frac{3}{4}\right)^{256}$$

∴ The probability [at least 1 Password out of 256 pswds is in the pswd file in the dictionary]

$$= 1 - \left(\frac{3}{4}\right)^{256}.$$

d.) The Amount of work, Trudy needs to do to crack any salted Password with her dictionary is,

$$\left(\frac{3}{4}\right)^0 \cdot \frac{1}{4}\left(2^{29}\right) + \left(\frac{3}{4}\right)^1 \cdot \frac{1}{4}\left(2^{29} + 2^{30}\right) +$$

$$\left(\frac{3}{4}\right)^2 \cdot \frac{1}{4}\left(2^{29} + 2 \cdot 2^{30}\right) + \cdots\cdots$$

$$+ \cdots\cdots + \left(\frac{3}{4}\right)^{255}.$$

$$\frac{1}{4}\left[2^{29} + 255 \cdot 2^{30}\right]$$

$$\therefore < 2^{32} \text{ hashes.}$$

6.) <u>problem 26 (Text book, Pg. 260) :-</u>

→ The probability [False match] $= 10^{10}$.

→ The No. of Fingerprints, the database contains is, 10^7

a.) → The no. of suspects' fingerprints is, 10^5.

∴ The total number of comparisions when comparing the suspects Fingerprints with that of the entire database is, Probability [No. of fingerprints in

the database] × Probability [No. of suspects fingerprints] $= 10^7 \times 10^5 = 10^{7+5} = \underline{10^{12}}$.

∴ The No. of false matches that will occur is,

$$\frac{\text{Probability [Total No. of comparisions]}}{\text{Probability [False match]}}$$

$$= \frac{10^{12}}{10^{10}} = 10^{12-10} = \underline{10^2}.$$

b) For any individual suspect, the chance of a false match is,

The Probability [1 in 10^{10} Fingerprints is a false match] $= \underline{1 - 10^{10}}$.

∴ The Probability [of an individual suspect the chance of a false match is]

$$1 - \frac{10^{10}}{10^{10}} = 1 - 10^{10-10} = 1 - 10^0$$

$$\therefore = 1 - 1 = \underline{0}.$$