Jessica Braganza
BE Comp 2
A17112151

PAGE NO :
DATE :

ICO Assignment 5

1) Explain Diffie - Hellman key exchange algorithm.

Ans Diffie Hellman algorithm is widely known as key exchange algorithm or key agreement algorithm.

Steps :

i) The first step is that if Ramesh wants to communicate with Suresh, they must agree on two large prime nos p and q.

ii) Ramesh selects another secret large random integer number 'a' and calculate 'R' such that $R = q^a \bmod p$.

iii) Ramesh sends R to Suresh

iv) Suresh independently selects another secret large random integer number b, and calculate S such that $S = q^b \bmod p$

v) Suresh sends the number S to Ramesh.

vi) Now Ramesh is calculating his secret key by using $R_K = S^a \bmod p$

vii) Suresh is calculating his secret key S_K by using $S_K = R^b \bmod p$

viii) If $R_K = S_K$ then Ramesh and Suresh can agree for future communication called as key agreement algorithm.

ix) We have $R_K = S_K = K$ hence proved (K is called the symmetric key)

2) Define

i) Public key -

A cryptographic key that can be obtained and used by anyone to encrypt messages intended for a particular recipient, such that the encrypted messages can be deciphered only by using a second key that is known only to the recipient.

ii) Private key -

It is also known as a secret key, is a variable in cryptography that is used with an algorithm to encrypt

and decrypt code. They are only shared with the key's generator, making it highly secure. It plays an important role in symmetric cryptography, asymmetric cryptography and cryptocurrencies.

3) Solve the problem.

Suppose the 2 parties A and B wish to setup a common secret key (D-H key) between themselves using the Diffie-Hellman key exchange technique. They agree on 7 as the modules and 3 as the primitive root. Party A chooses 2 and party B chooses 5 as their respective secrets their D-H key is ?.

→ Primitive root = $g = 3$

modulus = $p = 7$

$X_a = 2$ and $X_b = 5$

$Y_a = 3^2 \bmod 7 = 2$

$Y_b = 3^5 \bmod 7 = 5$

We assume D-H key to be K

$K = Y_a^{X_b} \bmod 7$

$K = 2^5 \bmod 7 = 4$

∴ Their D-H key is 4.