CYBER SECURITY & CRYPTOGRAPHY (5)

techworldthink • March 11, 2022

13. Apply Diffie-Hellman key exchange algorithm to compute the shared private key using the values P = 23, g = 9, a= 4, b= 3. Explain the steps in detail.

private key of A = 4

private key of B = 3

prime no, P = 23

primitive root, G = 9

Share P&G (A->B or B->A)

find?

public key of A = (g^a) mod n = (9^4) mod 23 = 6

public key of B = (g^b) mod n = (9^3) mod 23 = 16

Exchange A&B public keys

find?

A, Secret key = (Bpublic ^ a) mod n = (16^4) mod 23 = 9

B, Secret key = (Apublic ^ a) mod n = (6^3) mod 23 = 9

Extra notes

- This algorithm is used to exchange the secret key between the sender and the receiver.
- This algorithm facilitates the exchange of secret key without actually transmitting it.

Let-

- Private key of the sender = Xs
- Public key of the sender = Ys
- Private key of the receiver = Xr
- Public key of the receiver = Yr

Step-01:

- One of the parties choose two numbers 'a' and 'n' and exchange with the other party.
- 'a' is the primitive root of prime number 'n'.
- After this exchange, both the parties know the value of 'a' and 'n'.

Step-02:

- Both the parties already know their own private key.
- Both the parties calculate the value of their public key and exchange with each other.

Sender calculate its public key as-

$$Y_S = a^{X_s} \bmod n$$

Receiver calculate its public key as-

$$Y_r = a^{X_r} \bmod n$$

Step-03:

- Both the parties receive public key of each other.
- Now, both the parties calculate the value of secret key.

Sender calculates secret key as-

$$\text{Secret key} = (Y_r)^{X_s} \bmod n$$

Receiver calculates secret key as-

$$\text{Secret key} = (Y_S)^{X_r} \bmod n$$

> ***Primitive root ?***

prime ,q = 7

primitive root ,p = 3

is 3 prime root ot 7?

check p^(1 to (q-1)) should have {1,2,3,.....,q-1}

3^1 mod 7 = 3

3^2 mod 7 = 2

3^3 mod 7 = 6

3^4 mod 7 = 4

3^5 mod 7 = 5

3^6 mod 7 = 1

={1,2,3,4,5,6} , so 3 is primitive root of 7

> *square root of large numbers*

eg1:

31^500 mod 30 => (31-30)^500 mod 30 => 1

eg2:

242^329 mod 243 => (242-243)^329 mod 243 => (-1)^329 mod 243

=> 1^329 mod 243 gives 1 ,

so (-1)^329 mod 243 will be 243-1 -> 242

14. Perform encryption and decryption using RSA Algorithm with parameters: P=17, q = 11, e = 7, M = 88. Explain the steps in detail.

n = p.q = 187

φ(n)= (p-1)(q-1) = (16x10) = 160

e = 7

d = (e^-1) mod φ(n) => (7^-1) mod 160 = 23

> *d = (e^-1) mod φ(n)*

> *ed = 1 mod φ(n)*

> *ed mod φ(n) = 1*

> *7.x mod 160 =1*
>
> *7.x = 160+1*
>
> *so, x = 161/7=23*

M = 88

C = (M^e) mod n = (88^7) mod 187 = 11

M = (C^d) mod n = (11^23) mod 187 = 88

.... **Explanations** ....

p,q are 2 prime numbers

n = p*q

calculate euler totient, φ(n)= (p-1)(q-1)

which means, φ(n) *numbers are relatively prime to n*

select integer e as encryption key, gcd(φ(n),e)=1 , 1< e < φ(n)

calculate decryption key d , d = (e^-1) mod φ(n)

public key = {e,n}

private key = {d,n}

Ciphertext, C = (M^e) mod n

plaintext, M = (C^d) mod n