Semester : VI Subject : CSS Academic Year: 2023-2024

DIFFIE-HELLMAN KEY EXCHANGE ALGORITHM:

→ Diffie Hellman key exchange Algorithm is a method for securely exchanging cryptographic keys over a public communication channel.

→ Keys are not actually exchanged – they are jointly derived.

→ It is not used to encypt any message.

Algorithm:

Step 1: Choose the global public elements
- q — Prime Numbers.
- α — $\alpha < q$, α is a primitive root of q

Step 2: User A Key generation
- Select private random Number X_A.
- Calculate public Y_A.

$$Y_A = \alpha^{X_A} \bmod q \quad \text{—— (1)}$$

Step 3: User B Key generation
- Select private random Number X_B.
- Calculate public Y_B.

$$Y_B = \alpha^{X_B} \bmod q \quad \text{—— (2)}$$

Step 4: Exchange public values between A and B.

A $\xrightarrow{Y_A}$ B.

A $\xleftarrow{Y_B}$ B.

Semester : VI Subject : CSS Academic Year: 2023 - 2024

Step 5: Generation of secret key by User A.

$$K = (Y_B)^{X_B} \bmod q.$$

Step 6: Generation of secret key by User B.

$$K = (Y_A)^{X_B} \bmod q.$$

Here both the K is equal.

Proof for the equality of K values.

$$K = (Y_B)^{X_A} \bmod q$$

From eqn (2) substitute Y_B.

$= (\alpha^{X_B} \bmod q)^{X_A} \bmod q$ According to modulus arithmetic

$= (\alpha^{X_B})^{X_A} \bmod q$ Interchange X_A and X_B.

$= (\alpha^{X_A})^{X_B} \bmod q$

$= (\alpha^{X_A} \bmod q)^{X_B} \bmod q$ According to equation (1)

$= (Y_A)^{X_B} \bmod q = K.$

Example 1:
Consider $q = 5$, the primitive root $\alpha = 3$, the secret value of A and B are 4 and 6. Calculate the shared secret key Diffie-Hellman Key Exchange.

Solution:

Given : $q = 5$, $\alpha = 3$.

Semester : VI Subject : CSS Academic Year: 2023-2024

A (Sender)

$X_A = 4$.

Calculate Y_A.

$Y_A = \alpha^{X_A} \bmod q$.

$= 3^4 \bmod 5$

$= 81 \bmod 5$

$\boxed{Y_A = 1}$

B (Receiver)

$X_B = 6$.

Calculate Y_B.

$Y_B = \alpha^{X_B} \bmod q$

$= (3)^6 \bmod q$.

$= 729 \bmod 5$

$\boxed{Y_B = 4}$

$Y_A = 1$ ---------->

<---------- $Y_B = 4$

Calculate K.

$K = (Y_B)^{X_A} \bmod q$.

$= (4)^4 \bmod 5$

$= 256 \bmod 5$.

$\boxed{K = 1}$

$K = (Y_A)^{X_B} \bmod q$.

$= (1)^6 \bmod 5$

$\boxed{K = 1}$

What do you mean by primitive root of a number?
For example, consider $q = 5$ which is a prime number.
So $\alpha < q$.

if $\alpha = 3$:

x	3^x	$3^x \bmod 5$
1	3	3
2	9	4
3	27	2
4	81	1

If you get 1,2,3,4 (all values of x. then it is primitive root. It can be any order.

Because 5 is my q. Consider only till 4.

if $\alpha = 4$.

x	4^x	$4^x \bmod 5$
1	4	4
2	16	1
3	64	4
4	256	1

It is not a primitive root.

Semester : VI Subject : CSS Academic Year: 2023-2024

Example 2:

Consider a Diffe-Hellman scheme with a common prime $q = 13$ and the primitive root $\alpha = 7$.

(i) If the public key of A is 3. Calculate the shared secret key of A?

(ii) If the public key of B is 9. Calculate the shared secret key of B?.

Solution:

Given :- $q = 13$, $\alpha = 7$.

A (Sender)

$X_A = 3$.

$Y_A = (\alpha)^{X_A} \bmod q$.

$= (7)^3 \bmod 13$.

$Y_A = 5$

B (Receiver).

$X_B = 9$.

$Y_B = (\alpha)^{X_B} \bmod q$

$= (7)^9 \bmod 13$

$Y_B = 8$.

$Y_A = 5$ ---------->

<---------- $Y_B = 8$.

Calculate K.

$K = (Y_B)^{X_A} \bmod q$.

$= (8)^3 \bmod 13$

$K = 5$

Calculate K.

$K = (Y_A)^{X_B} \bmod q$

$= (5)^9 \bmod 13$

$K = 5$