BLOCKCHAIN TUTORIAL 10

Diffie-Hellman key exchange

BLOCKCHAIN TUTORIAL 10

Diffie-Hellman key exchange

DIFFIE-HELLMAN KEY EXCHANGE

- Diffie-Hellman key exchange is a method to securely establish a shared secret between two parties (Alice and Bob) over a public channel.

1. Alice and Bob agrees on the publicly shared domain parameters α (generator) and p (modulus). For example $\alpha = 3$, $p = 17$

2. Alice generates a random number. This is Alice private key.

   priv $\text{key}_{\text{alice}} \in \{2,..\ p-2\}$ example: priv $\text{key}_{\text{alice}} = 15$ Note: $\in$ means element of

3. Bob also generates a random number. This is Bob private key.

   priv $\text{key}_{\text{bob}} \in \{2,..\ p-2\}$ example: priv $\text{key}_{\text{bob}} = 13$

DIFFIE-HELLMAN KEY EXCHANGE

4. Alice calculates her public key.

   $\text{pub key}_{\text{alice}} = \alpha^{\text{priv key alice}} \pmod{p} = 3^{15} \pmod{17}$

5. Bob also calculates his public key.

   $\text{pub key}_{\text{bob}} = \alpha^{\text{priv key bob}} \pmod{p} = 3^{13} \pmod{17}$

6. Alice sends her public key to Bob over the public channel.

7. Bob sends his public key to Alice over the public channel.

DIFFIE-HELLMAN KEY EXCHANGE

8. Alice takes Bob public key and calculates the secret key:

   $\text{secret key} = \text{pub key}_{\text{bob}}{}^{\text{priv key alice}} \pmod{p} = \text{pub key}_{\text{bob}}{}^{15} \pmod{17}$

9. Bob takes Alice public key and calculates the secret key (same as Alice):

   $\text{secret key} = \text{pub key}_{\text{alice}}{}^{\text{priv key bob}} \pmod{p} = \text{pub key}_{\text{alice}}{}^{13} \pmod{17}$

10. Alice and Bob can use the secret key (also known as session key) in a symmetric key algorithm for example AES to encrypt and decrypt their messages.

DIFFIE-HELLMAN KEY EXCHANGE

- Proof that Alice and Bob secret keys are the same:

$a = \alpha^{\text{priv key alice}}$

$b = \alpha^{\text{priv key bob}}$

$\text{pub key}_{\text{alice}} = \alpha^{\text{priv key alice}} \pmod p$

$\text{pub key}_{\text{bob}} = \alpha^{\text{priv key bob}} \pmod p$

$\text{Alice: secret key} = \text{pub key}_{\text{bob}}{}^{\text{priv key alice}} \pmod p = \alpha^{ba} \pmod p$

$\text{Bob: secret key} = \text{pub key}_{\text{alice}}{}^{\text{priv key bob}} \pmod p = \alpha^{ab} \pmod p = \alpha^{ba} \pmod p$

DIFFIE-HELLMAN KEY EXCHANGE

- Can Eve calculate the secret key?

- Eve has intercepted Alice and Bob public key and she knows α and p:

$$\text{pub key}_{\text{alice}} = \alpha^{\text{priv key alice}} \pmod{p}$$

She needs to calculate the discrete logarithm, which is very hard to do (p $\geq$ 1024 bits):

$$\text{priv key}_{\text{alice}} = \log_{\alpha} \text{pub key}_{\text{alice}} \pmod{p}$$

in another form:

$$\text{pub key}_{\text{alice}} = \alpha^{\text{priv keyalice}} \pmod{p}$$