Key Exchange Solutions

- Diffie-Hellman Protocol
- Needham Schroeder Protocol
- X.509 Certification

Diffie-Hellman Key Exchange

- The Diffie-Hellman protocol allows 2 people to use random values and yet each generate the same symmetric key without transmitting the value of the key.
- The security of the protocol lies in the discrete log problem:

  given y, g and p find x such that

  $$y = g^x \bmod p$$

Alice and Bob need to agree on a key to use in a symmetric key cryptosystem. They choose a large prime number p and generator g.

Alice	Bob
1. Generates random number a,	1. Generates random number b,
2. Computes $x=g^a \bmod p$	2. Computes $y=g^b \bmod p$
3. Sends x to Bob	3. Sends y to Alice
4. Receives y from Bob	4. Receives x from Alice
5. Computes $k=y^a \bmod p$	5. Computes $k=x^b \bmod p$

Why Diffie-Hellman works

Alice has computed

$$k = y^a \mod p$$
$$= (g^b)^a \mod p$$
$$= g^{ba} \mod p$$
$$= g^{ab} \mod p$$

Bob has computed

$$k = x^b \mod p$$
$$= (g^a)^b \mod p$$
$$= g^{ab} \mod p$$

So Alice and Bob both have the same value of k.

How secure is it?

We assume that cryptanalyst Charles knows the values of p and g and that he eavesdrops on the exchange between Alice and Bob so that he also knows x and y.

However, unless Charles can solve a DLP, he is unable to find a or b.

It is believed that it is just as hard to find k from x and y without finding a or b.

The Needham-Schroeder Protocol

This is another protocol for exchanging keys between Alice and Bob.

This time they use only symmetric key cryptography

But

They need a trusted third party (TTP) or Server (S).

- Alice and the server have a key K_{AS}
- Bob and the server have a key K_{BS}
- Alice and Bob want to establish a shared key K_{AB} so that Alice can send Bob a message.
- They communicate with each other and the server as follows:

1. Alice sends the server S the names of Alice and Bob to request that a session key be generated.

2. The server sends to Alice:
   a) The name of Bob
   b) A session key for Alice and Bob to share
   c) The name of Alice and the session key both encrypted using K_{BS}

All 3 items above are encrypted using key K_{AS}

3. Alice uses key K_{AS} to decrypt the items sent to her in step 2. Alice now knows the session key $K_{AB.}$
4. Alice sends Bob the value of 2c) which is the name of Alice and the session key K_{AB} encrypted with K_{BS}
5. Bob decrypts the name of Alice and the session key using his key $K_{BS.}$ Now Bob knows the session key K_{AB} which he uses to communicate with Alice.

Needham-Schroeder

1. A ⟶ S: A,B

2. S ⟶ A: $e_{KAS}(B, K_{AB}, e_{KBS}(A, K_{AB}))$

Alice decrypts to get B, K_{AB}, $e_{KBS}(A, K_{AB})$

3. A ⟶ B: $e_{KBS}(A, K_{AB})$

Bob decrypts to get A, K_{AB}

Needham-Schroeder 2

1. A $\longrightarrow$ S: A, B, N_A
2. S $\longrightarrow$ A: $e_{KAS}(B, N_A, K_{AB}, e_{KBS}(A, K_{AB}))$
3. A $\longrightarrow$ B: $e_{KBS}(A, K_{AB})$
4. B $\longrightarrow$ A: $e_{KAB}(N_B)$
5. A $\longrightarrow$ B: $e_{KAB}(N_B - 1)$

Certificates

A certificate consists of a public key together with an identification of the key user. The certificate is issued by a trusted third party(TTP) called a

***certification agency* (CA)**

The certification agency might be a government agency or financial institution.

The CA guarantees the link between the user and the public key by digitally signing a document which contains the user name, the public key, the name of the CA, the expiry date of the certificate and perhaps other information such as access rights.

X.509 Standard

- Bob generates a document containing his relevant information and presents himself with this document to the CA.
- The CA confirm Bob's identity.
- The CA hash the document using SHA-1 and encrypt it using their own private key.
- This is the certificate.

- If Alice wants to communicate with Bob she looks up his public key document and certificate.
- She will use the public key of the CA to decrypt the certificate.
- She will hash the document using SHA-1
- If these two items are the same then she knows that she can safely communicate with Bob using the public key since the CA has verified his identity.