Key Distribution Using Asymmetric Encryption

Diffie-Hellman Key Exchange

Section 3.5

Distribute symmetric key

Recall: ways to achieve symmetric key distribution

- A key could be selected by A and physically delivered to B
- A third party could select the key and physically deliver it to A and B
- If A and B have previously and recently used a key, one party could transmit the new key to the other, using the old key to encrypt the new key
- If A and B each have an encrypted connection to a third-party C, C could deliver a key on the encrypted links to A and B

Diffie-Hellman Key Exchange

- Solve the problem of distributing a symmetric key between A and B over unsecure channel without the assistance of third party
- There is no pre-shared secret either.

Diffie-Hellman Key Exchange

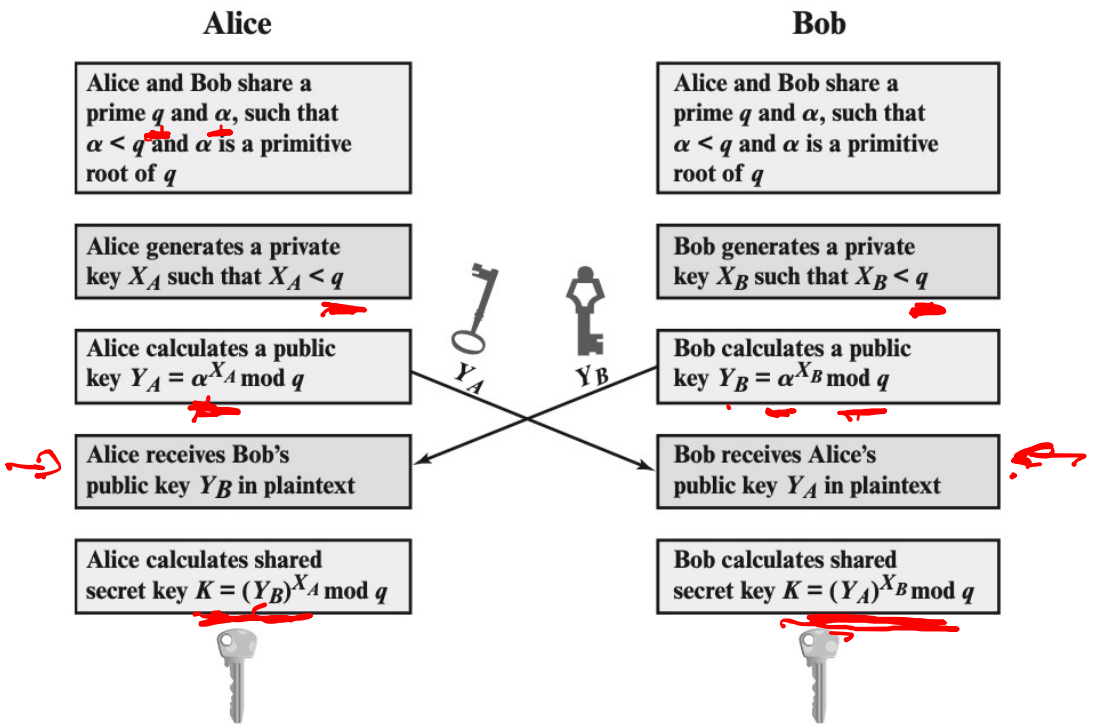
- Invented by Whitfield Diffie and Martin Hellman in 1976
- Allows Alice and Bob to exchange a key even with Eve learning it
- No third party involved
- After DHKE, a common shared key, $\alpha^{X_A X_B}$ is established, it can be used to encrypt message
- A common shared key is symmetric

The Diffie-Hellman Key Exchange

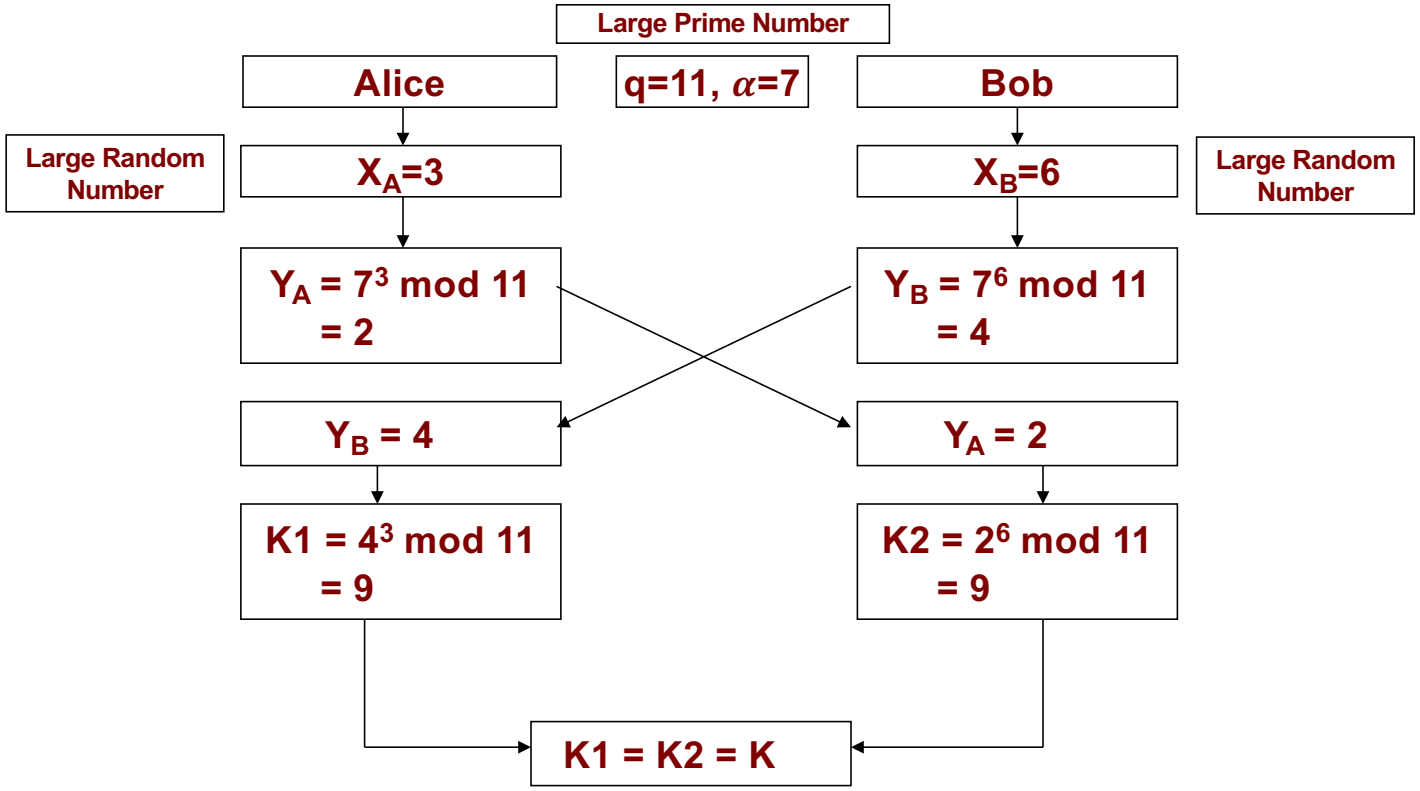
- From A's view
- $K = {Y_B}^{X_A} \ mod \ q$

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

  $= \alpha^{X_B X_A} \ mod \ q$



Example of the Diffie -Hellman algorithm



Note: X_A, X_B, K1, K2 are Private

Analysis of DHKE - Attack

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

- Adversary gets q, α, Y_A, Y_B.
- She needs to compute either X_A or $X_B = dlog_{\alpha,q} Y_B$
- Secure?

Discrete Log Problem

Cryptographic assumptions:

- **Discrete logarithm problem** (**discrete log problem**): Given $\alpha, q, \alpha^{X_A} \ mod \ q$ for random X_A, it is computationally hard to find X_A
- **Diffie-Hellman assumption**: Given $\alpha, q, \alpha^{X_A} \ mod \ q$, and $\alpha^{X_B} \ mod \ q$ for random X_A, X_B, no polynomial time attacker can distinguish between a random value R and $\alpha^{X_A X_B} \ mod \ q$.
  - Intuition: The best known algorithm is to first calculate X_A and then compute $(\alpha^{X_B})^{X_A} \ mod \ q$, but this requires solving the discrete log problem, which is hard!
- Note: Multiplying the values doesn't work, since you get $\alpha^{X_A+X_B} \ mod \ p \ \neq \ \alpha^{X_A X_B} \ mod \ p$

Ephemerality of Diffie-Hellman

- Diffie-Hellman can be used ephemerally (called Diffie-Hellman ephemeral, or DHE)
  - **Ephemeral**: Short-term and temporary, not permanent
  - Alice and Bob discard X_A, X_B and $K = \alpha^{X_A X_B} \ mod \ q$ when they're done
  - Because you need X_A and X_B to derive K, you can never derive K again!
  - Sometimes K is called a **session key**, because it's only used for an ephemeral session
- Eve can't decrypt any messages she recorded: Nobody saved X_A, X_B or K, and her recording only has $\alpha^{X_A} \ mod \ q$ and $\alpha^{X_B} \ mod \ q$!

Diffie-Hellman is susceptible to man-in-the-middle attacks

- David can alter messages, block messages, and send her own messages
- **DH is not** secure against a MITM attacker: David can just do a DH with both sides!

Diffie-Hellman: Security