

Lecture 28

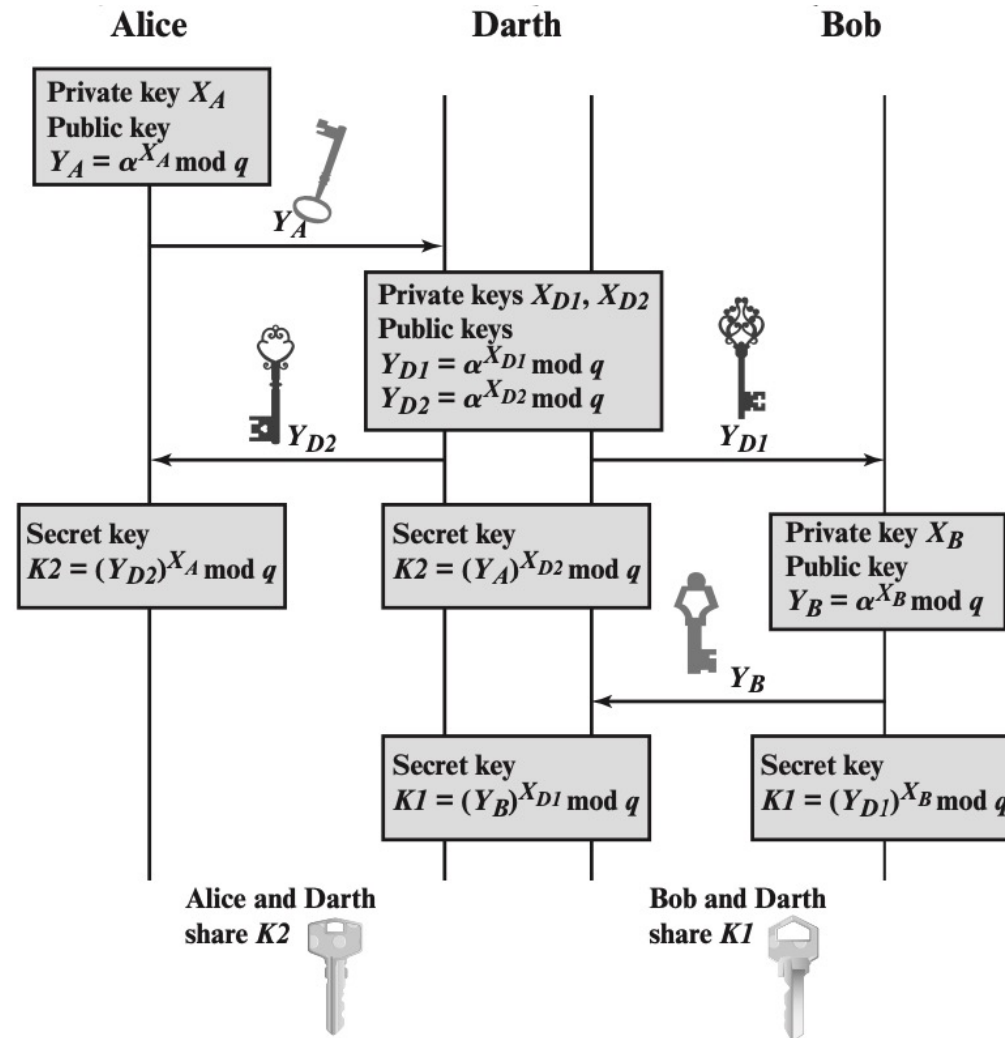
Ephemerality of Diffie-Hellman

- 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 $K = \alpha^{X_A X_B} \bmod q$ 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 $\alpha^{X_A} \bmod q$ and $\alpha^{X_B} \bmod q$!

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



Diffie-Hellman: issues

- Diffie-Hellman is not secure against a MITM adversary
- DHE is an *active protocol*: Alice and Bob need to be online at the same time to exchange keys
 - What if Bob wants to encrypt something and send it to Alice for her to read later?
- Diffie-Hellman does not provide *authentication*
 - You exchanged keys with someone, but Diffie-Hellman makes no guarantees about who you exchanged keys with; it could be David!

Diffie-Hellman Key Exchange: Summary

- Algorithm:
 - Alice chooses X_A and sends $\alpha^{X_A} \bmod q$ to Bob
 - Bob chooses X_B and sends $\alpha^{X_B} \bmod q$ to Alice
 - Their shared secret is $(\alpha^{X_A})^{X_B} = (\alpha^{X_B})^{X_A} = \alpha^{X_A X_B} \bmod q$
- Diffie-Hellman provides forwards secrecy: Nothing is saved or can be recorded that can ever recover the key
- Diffie-Hellman can be performed over other mathematical groups, such as elliptic-curve Diffie-Hellman (ECDH)
- Issues
 - **Not** secure against MITM
 - Both parties must be online
 - Does not provide authenticity

Homework – no submission

- SW, “Network Security Essentials”, 6th Edition, 2017

- Problems – 3.21

Consider a Diffie-Hellman scheme with a common prime $q = 11$ and a primitive root $\alpha = 2$.

- a. if user A has public key $Y_A = 9$, what is A's private key X_A ?
- b. If user B has public key $Y_B = 3$, what is the shared secret key K ?

Next

- PKI and Certificates
 - Section 4.5