Lecture 28

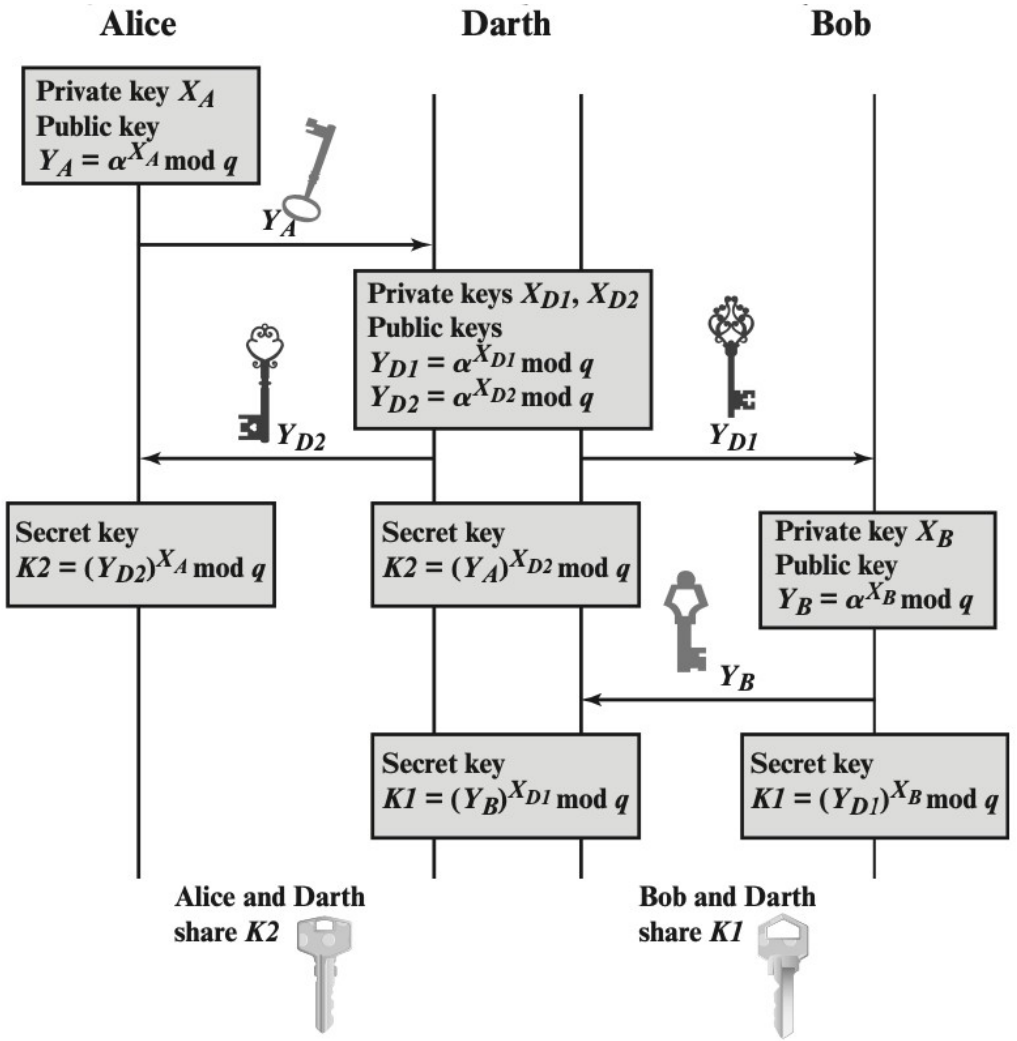
Ephemerality of Diffie-Hellman

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

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 and sends to Bob
  - Bob chooses and sends to Alice
  - Their shared secret is
- 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 = 11 and a primitive root = 2.

  a. if user A has public key = 9, what is A’s private key ?

  b. If user B has public key = 3, what is the shared secret key ?

Next

- PKI and Certificates
  - Section 4.5