

Security

recap

Perfect secrecy:

cyphertext reveals no information (except max length)

Man-in-the-middle:

Pretend to Alice that you're Bob, and to Bob that you're Alice

Forward secrecy:

If Eve gets the key, she still can't decrypt the past cyphertexts

(t,n)-threshold secret sharing:

require t out of n keys to recover a secret

(n,n)-threshold scheme –

distribute n bitstrings that xor to the plaintext

(t,n)-threshold scheme –

distribute n values of a $(t-1)$ -degree polynomial. $f(0) = \text{secret}$

One-time pad

encryption

plaintext

\oplus

one-time pad

=

cyphertext

decryption

cyphertext

\oplus

one-time pad

=

plaintext

Bulk encryption

ECB

plaintextplaintextplaintext

plaintext

plaintext

plaintext



cyphertext

cyphertext

cyphertext

cyphertextcyphertextcyphertext

CBC

plainplainplain

plain

plain

plain



cypher

cypher

cypher

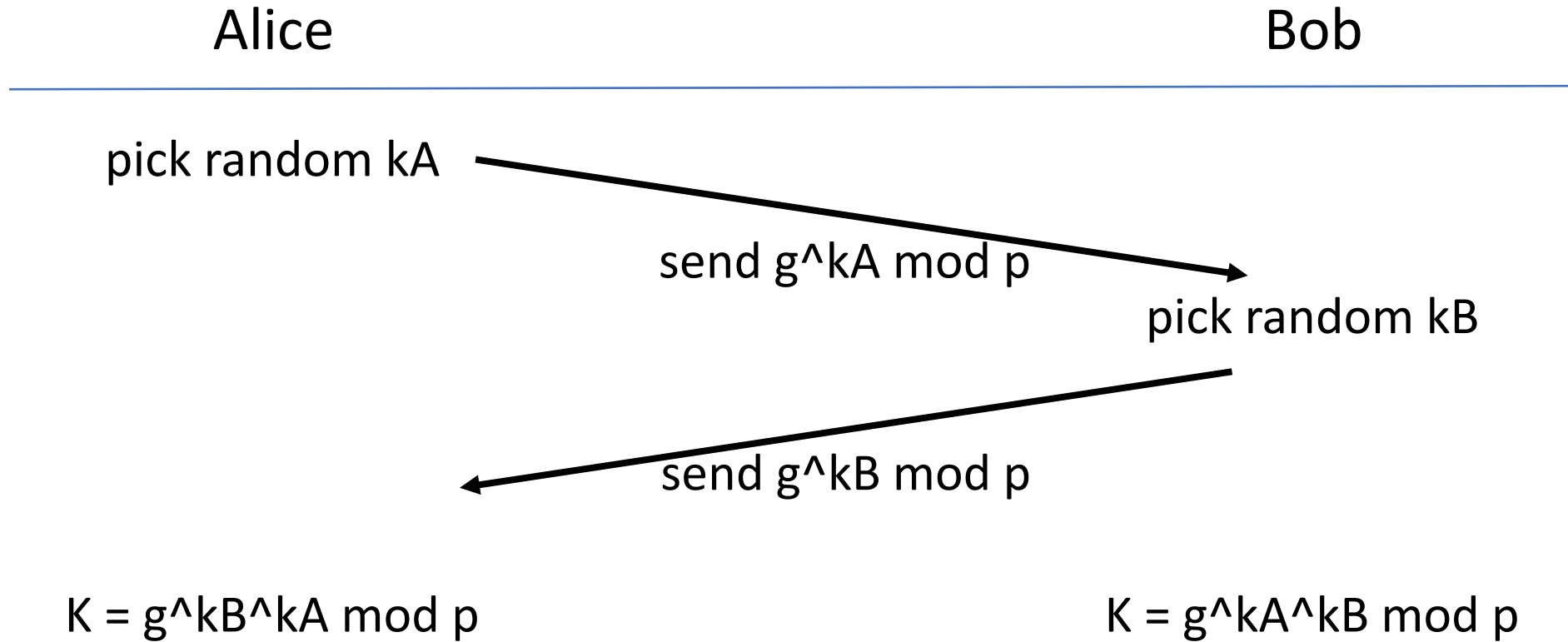
cypher

cyphercyphercyphercypher

↙ = encrypt

Diffie-Hellman Key Exchange

prime p
primitive root g



pick random k_A

send $g^{k_A} \text{ mod } p$

pick random k_B

send $g^{k_B} \text{ mod } p$

$$K = g^{k_B^{k_A}} \text{ mod } p$$

$$K = g^{k_A^{k_B}} \text{ mod } p$$

Discrete logarithm

prime p

primitive root g

It's hard to find x :

$$g^x = a \pmod{p}$$

One-time pad

encryption

plaintext

\oplus

one-time pad

=

cyphertext

decryption

cyphertext

\oplus

one-time pad

=

plaintext

Malleability:

Eve can change the cyphertext and the recipient will not notice

HMAC

With a cyphertext c , Alice will send $h(k, h(k, c))$ as well, to prove that c was sent by somebody who knows k (her)

Public key cryptography

Alice has a secret key k_s , and a public key k_p .

Bob can encrypt a message using k_p , and only Alice will be able to read it using k_s .

Alice can send her signature generated from k_s with message m . Using k_p Bob can check that Alice wrote m .

Certificate Authorities

Systems come with some trusted public keys preinstalled. They can be used to check the signatures of corresponding secret keys that can vouch for other public keys, etc.