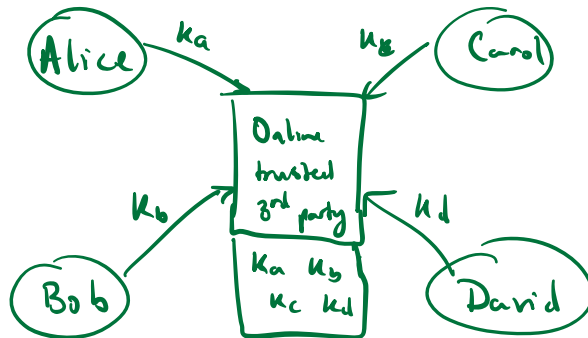


Key Exchange

Trusted Third Party (TTP) model

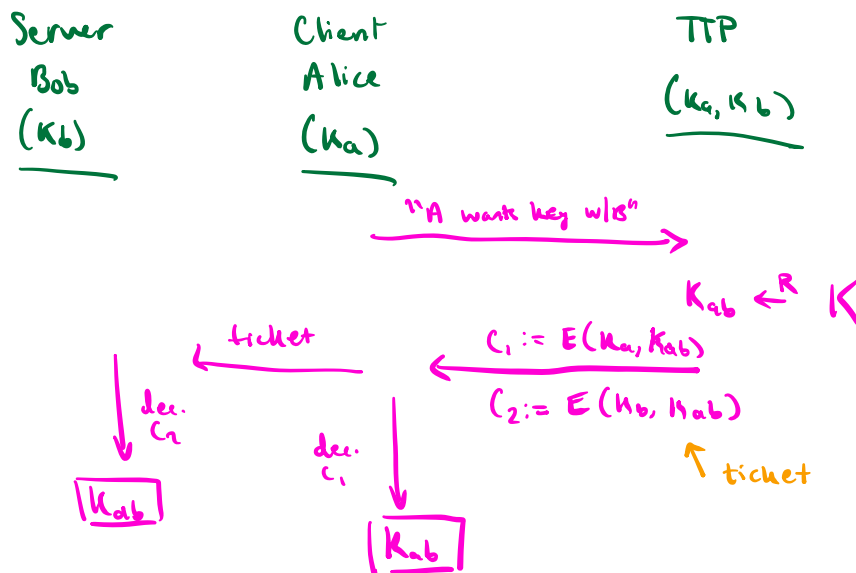
Problem:



Key exch.: a toy protocol (secure against eavesdropping)

Need: CPA-secure cipher (E, D) w/ key space \mathcal{K}

Alice wants key w/ Bob



Eavesdropper sees: $E(K_A, K_{AB}), E(K_B, K_{AB})$

(E, D) CPA-secure: eavesdropper learns nothing about K_{AB}

Notes:

1. TTP needed for key exch, needs to be permanently online
2. TTP knows all session keys (backdoor heaven)
3. This is basics of Kerberos system (windows)

Basic question: can we generate shared session key w/o TTP?

Answer: Yes! starting point of public-key crypto

Public-key Cryptography

Merkle (1974): use only symmetric ciphers
however, impractical (can't be improved)

⇒ Need more structure than previous primitives
(algebra)

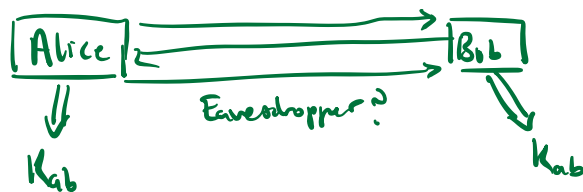
→ Diffie-Hellman (1976)

→ RSA (1977)

→ Elliptic-Curve Crypto (1984)

⋮

Key-exch w/o online TTP (eavesdropping security)



Basic Diffie-Hellman key exch

(eavesdropping security)

Fix a large prime p (e.g. 600 digits)

Fix integer g where $1 < g < p$

Alice

$$a \xleftarrow{R} \{1 \dots p-1\}$$

$$A \leftarrow g^a \pmod{p}$$

Bob

$$b \xleftarrow{R} \{1 \dots p-1\}$$

$$B \leftarrow g^b \pmod{p}$$

$$K_{ab} = g^{ab} \pmod{p}$$

$$= A^b = (g^a)^b \pmod{p}$$

$$= B^a = (g^b)^a \pmod{p}$$

\Rightarrow both sides obtain same key

Eavesdropping security:


eavesdropper sees $p, g, g^a, g^b \pmod{p}$

can it compute $g^{ab} \pmod{p}$?

(cannot prove - requires $P \neq NP$ proof)

believed to be hard when p sufficiently large

[broken w/ quantum computers : $O(\log^3 p)$]

 cubic-time protocol