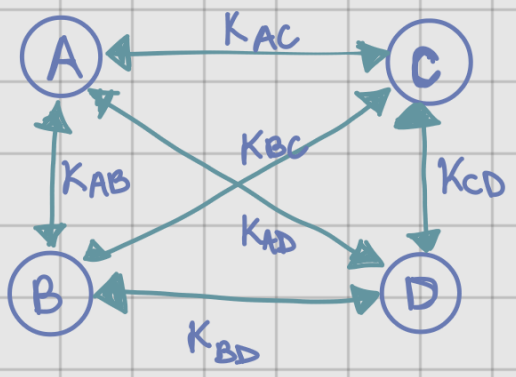
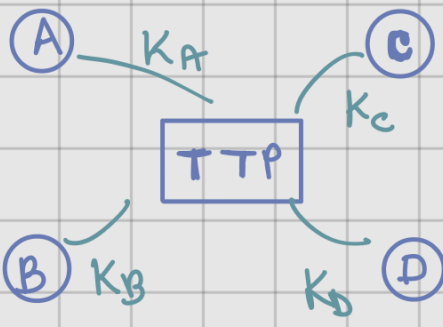
BASIC Key EXCHANGE



→ Uma chave para cada enlace... Ruim de gerenciar.

Uma solução melhor:



Online Trusted 3rd Party

Gerando chaves:
"Protocolo de Brinquedo"

Generating keys: a toy protocol

Alice wants a shared key with Bob. Eavesdropping security only.

K_A K_B

Bob (k_B) **Alice** (k_A) **TTP**

"Alice wants key with Bob"

choose random k_{AB}

$E(K_A, \text{"A,B"} \| K_{AB})$

ticket = $E(K_B, \text{"A,B"} \| K_{AB})$

ticket

k_{AB} k_{AB}

(E,D) a CPA-secure cipher

CRIPTO. SIMETRICA

(Kerberos)

VULNERÁVEL!

Mas, é possível gerar chaves sem uma terceira parte confiável online?

Sim!

Merkle (1974), Diffie-Hellman (1976) e RSA (1977).
(para cripto. de chave pública).

Ao passar dos anos, novas ideias: * Identity based Encryption
* Functional Encryption