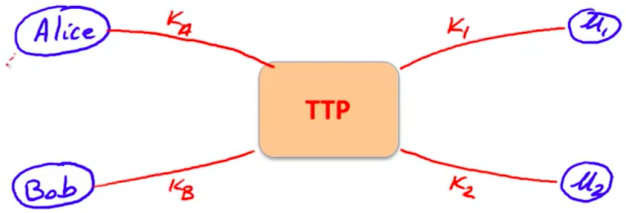
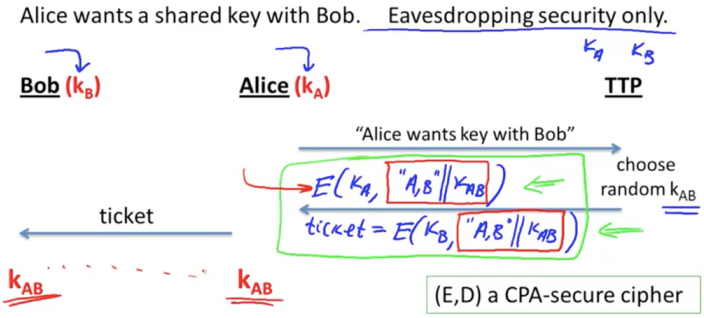
5.9 - Key Distribution through trusted 3rd party

- One way to handle the key management is Online Trusted 3rd party (TTP)

Online Trusted 3rd Party (TTP)



- Generating shared keys – a Toy Protocol.



Step 1. Alice and Bob need a shared secret key for communication, so Alice requests TTP for a shared key.
Step 2. TTP choose a random key K_{AB} and encrypts it with Alice's secret key and sends it back to Alice and Also it sends a Ticket which is encrypted with Bob's key and Shared key.
Step 3. Alice will recover the shared key by decrypting the message sent by TTP with her secret key.
Step 4. Bob also recover the shared key by decrypting the ticket sent by TTP with his secret key.

Disadvantages of TTP (Why it is not practical)

1. Generated keys are random numbers. However, the computer generated keys are not real random numbers which gives some kind of predictability to the attacker.
2. No freshness in the generated key. That is we don't get to know when the key was generated and when it is going to expire. Which causes the replay attack.
3. Since the TTP has whole lot of information, it will become target to attacker which is very dangerous.
4. In reality it becomes difficult to find two peers/nodes who agree on a common third party to generate the key.

Note: This is a very basic protocol which is secure only against eavesdropper.

- TTP need for every key exchange
- TTP knows all session keys.
- Insecure against active attacks and **replay attack.**

We can exchange the keys without online trusted third party.