Information security

Lecture-5

Eng. Taghreed Harfoush

Key Distribution

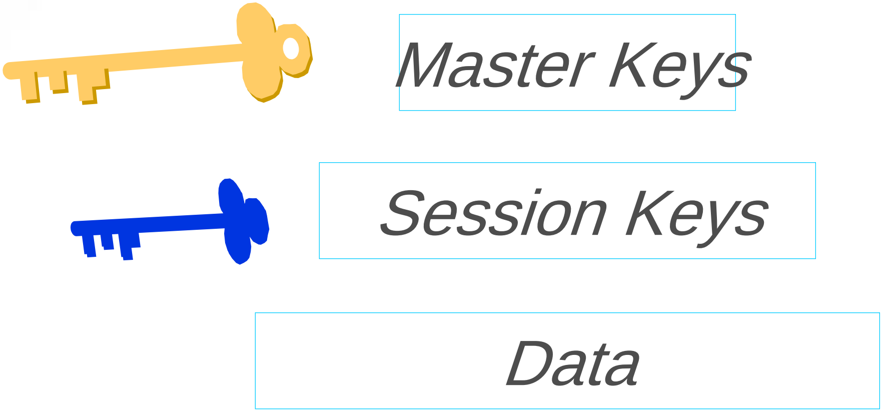
Key Distribution

- Alice's options in establishing a shared secret key with Bob include
  - **Alice selects a key and physically delivers it to Bob**
  - **Trusted third party key distribution center selects a key and physically delivers it to Alice and Bob**
  - **If Alice and Bob have previously and recently used a key, it can be used to distribute a new key**
  - **If Alice and Bob have keys with the KDC, KDC can deliver a key on the encrypted links to Alice and Bob**

Use of a Key Hierarchy

Use of a KDC is based on the use of a hierarchy of keys

- **Session key** : **temporary encryption key used between two parties**
- **Master key** : **long-lasting key used between a KDC and a party for the purpose of encrypting the transmission of session keys**

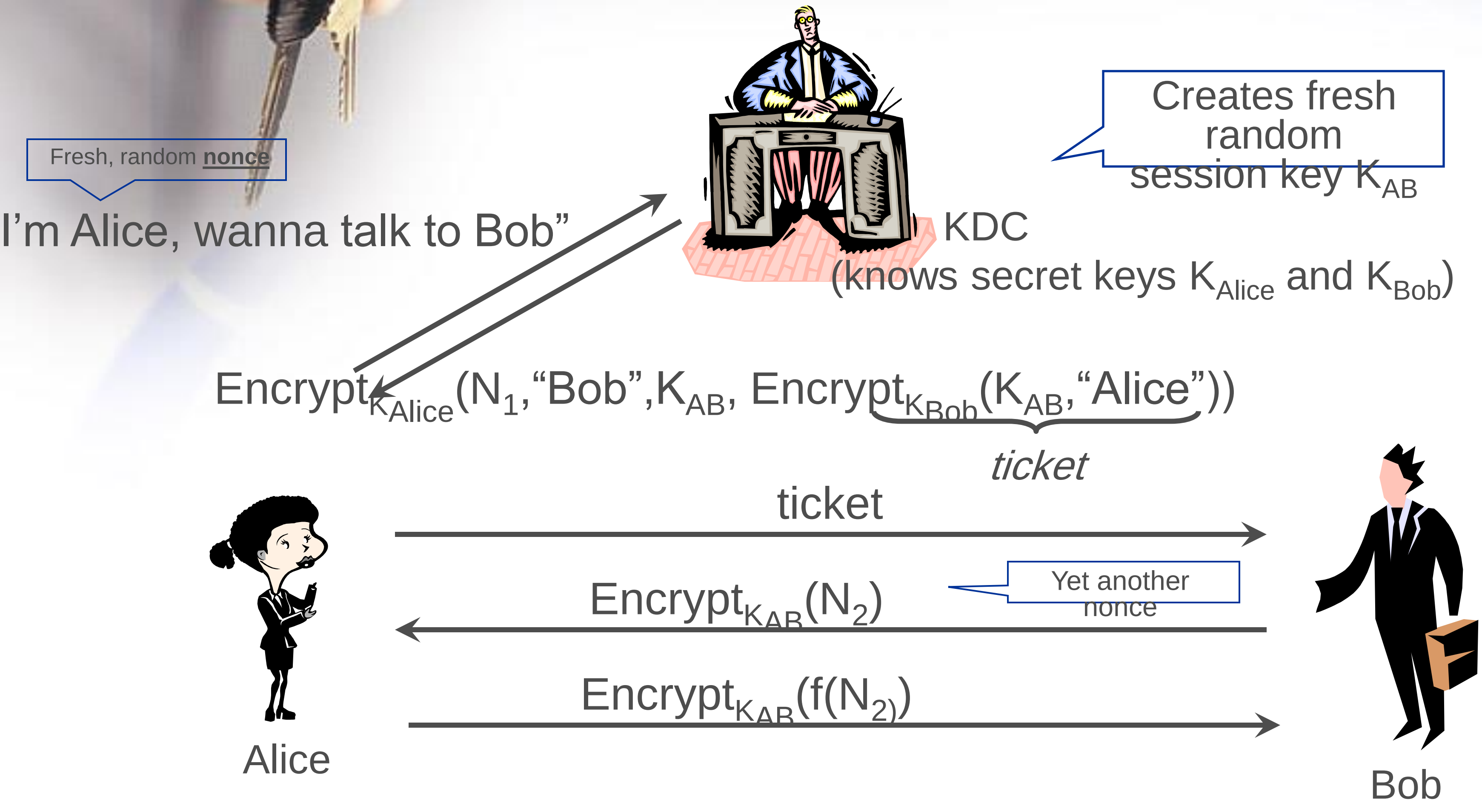


Master Keys

Session Keys

Data

Centralized Key Distribution



Fresh, random **nonce**

“I’m Alice, wanna talk to Bob”

KDC

(knows secret keys K_{Alice} and K_{Bob})

Creates fresh random session key K_{AB}

$$\text{Encrypt}_{K_{Alice}}(N_1,\text{“Bob”},K_{AB},\underbrace{\text{Encrypt}_{K_{Bob}}(K_{AB},\text{“Alice”})}_{\textit{ticket}})$$

ticket

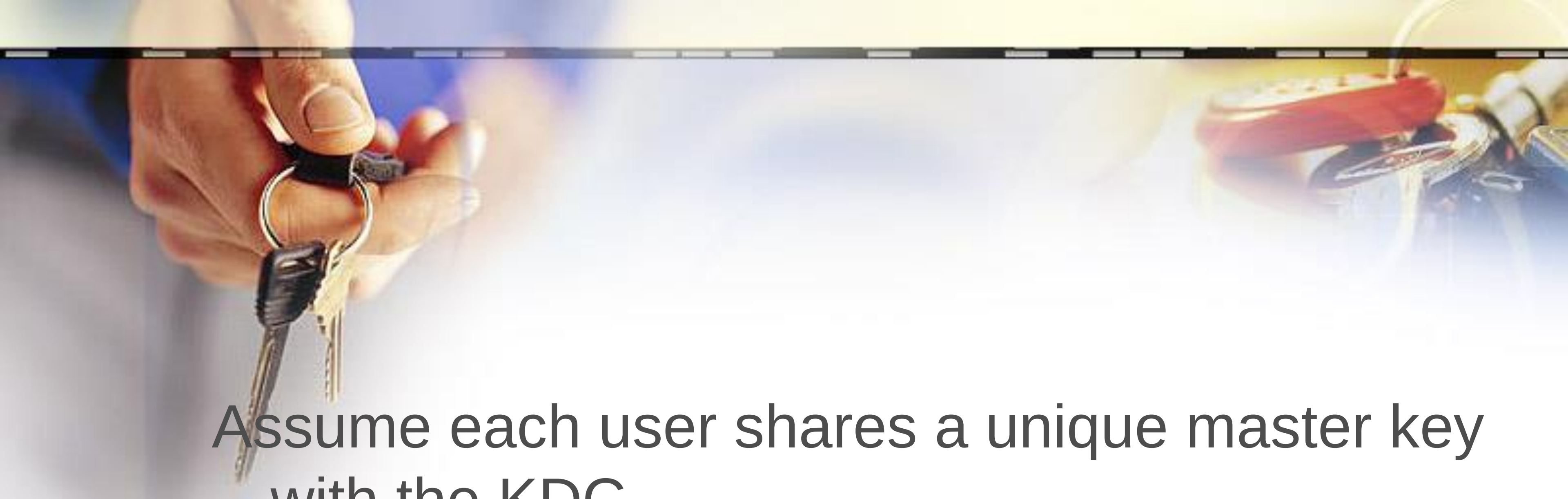
$\text{Encrypt}_{K_{AB}}(N_2)$

Yet another nonce

$\text{Encrypt}_{K_{AB}}(f(N_2))$

Alice

Bob



Assume each user shares a unique master key with the KDC

Alice desires a one-time session key to communicate with Bob

(1) Alice issues a request to the KDC for a session key to be used with Bob. Alice’s request includes a nonce to prevent replay attack

(2) KDC responds with a message encrypted under Alice’s key. The message contains the session key, the nonce, and the session key along with Alice’s identity encrypted under Bob’s key

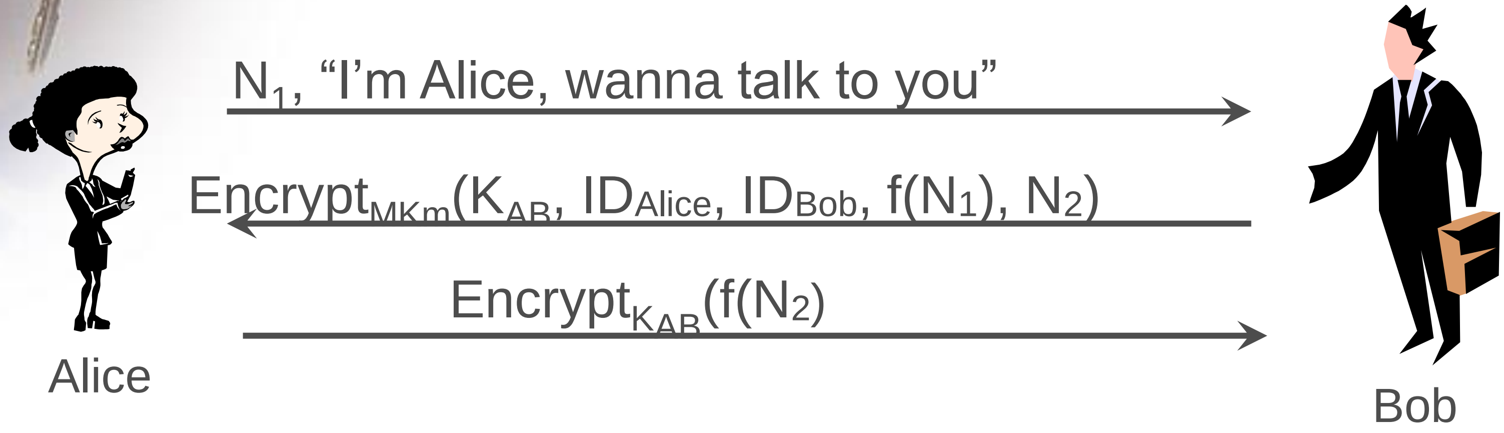
(3) Alice forwards the data encrypted under Bob’s Key to Bob

(4-5) Alice and Bob mutually authenticate under the session key

(4) Bob sends a nonce to Alice encrypted under the session key

(5) Alice applies a transformation to the nonce and sends the result back to Bob

Decentralized Key Distribution



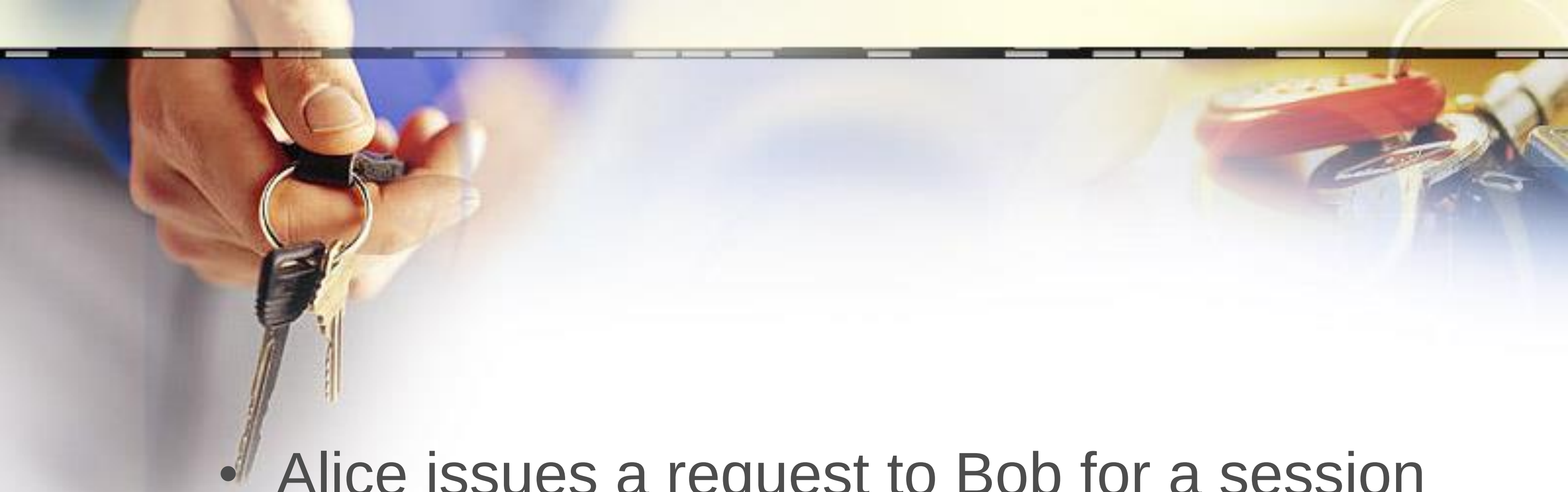
N_1, “I’m Alice, wanna talk to you”

$\text{Encrypt}_{MKm}(K_{AB}, ID_{Alice}, ID_{Bob}, f(N_1), N_2)$

$\text{Encrypt}_{KAB}(f(N_2))$

Alice

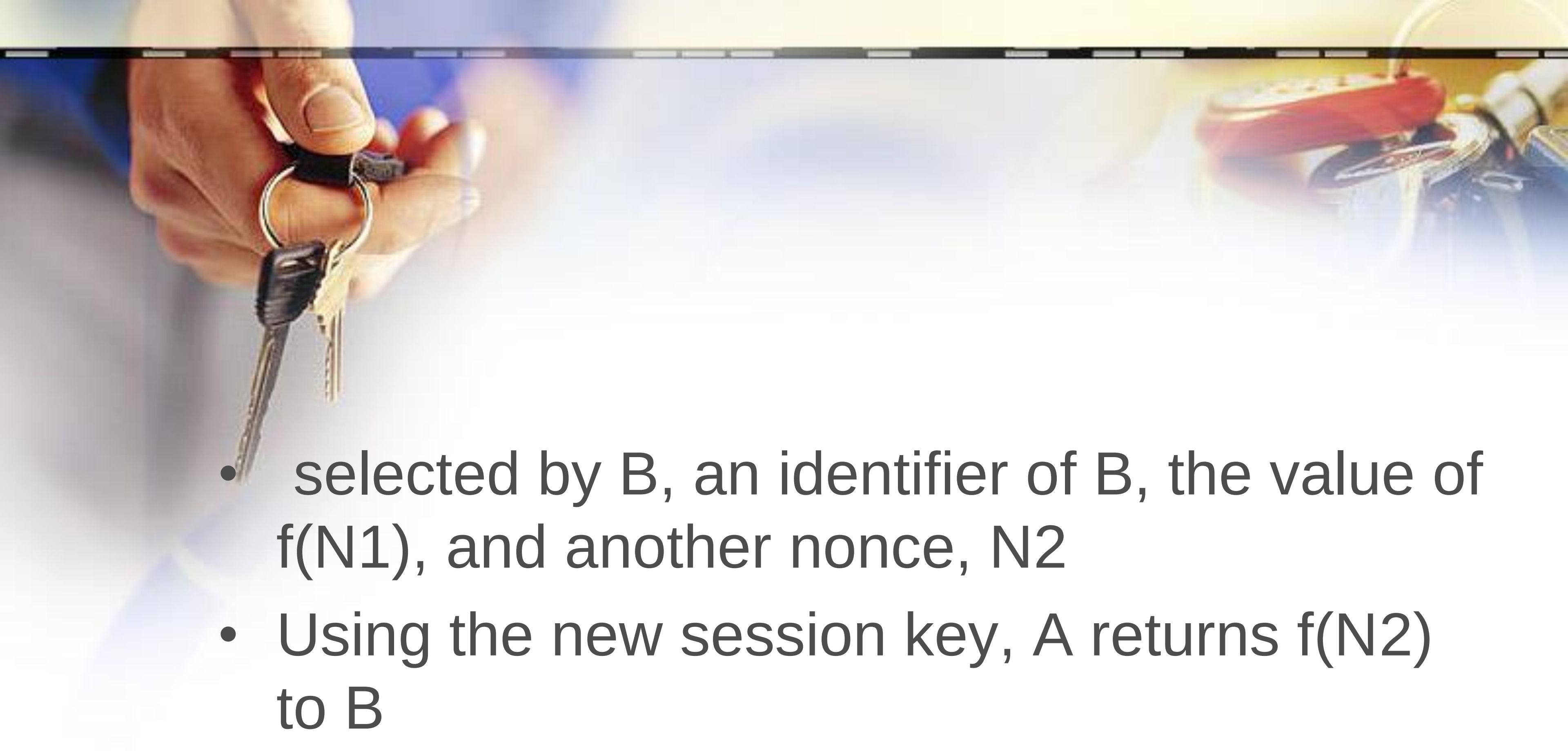
Bob



- Alice issues a request to Bob for a session key and

  includes a nonce, N1

- Bob responds with a message encrypted using the shared master key. Response includes the session key



- selected by B, an identifier of B, the value of f(N1), and another nonce, N2
- Using the new session key, A returns f(N2) to B