Key Distribution

Ragesh Jaiswal
CSE, IIT Delhi

Diffie Hellman Key Exchange

g^x

g^y

Both parties share g^{xy} which is the secret key for the session.

Authentication

Diffie Hellman Key Exchange

The adversary will be able to read all messages being exchanged between Alice and Bob

Key Distribution in Public Key Setting

- Public key cryptography:

(sg, pg)

Interaction

Cert = {Alice's public key is pa}$_{sg}$

(sa, pa)

pa, Cert

Key Distribution in Public Key Setting

- Public key cryptography:

(sg, pg)

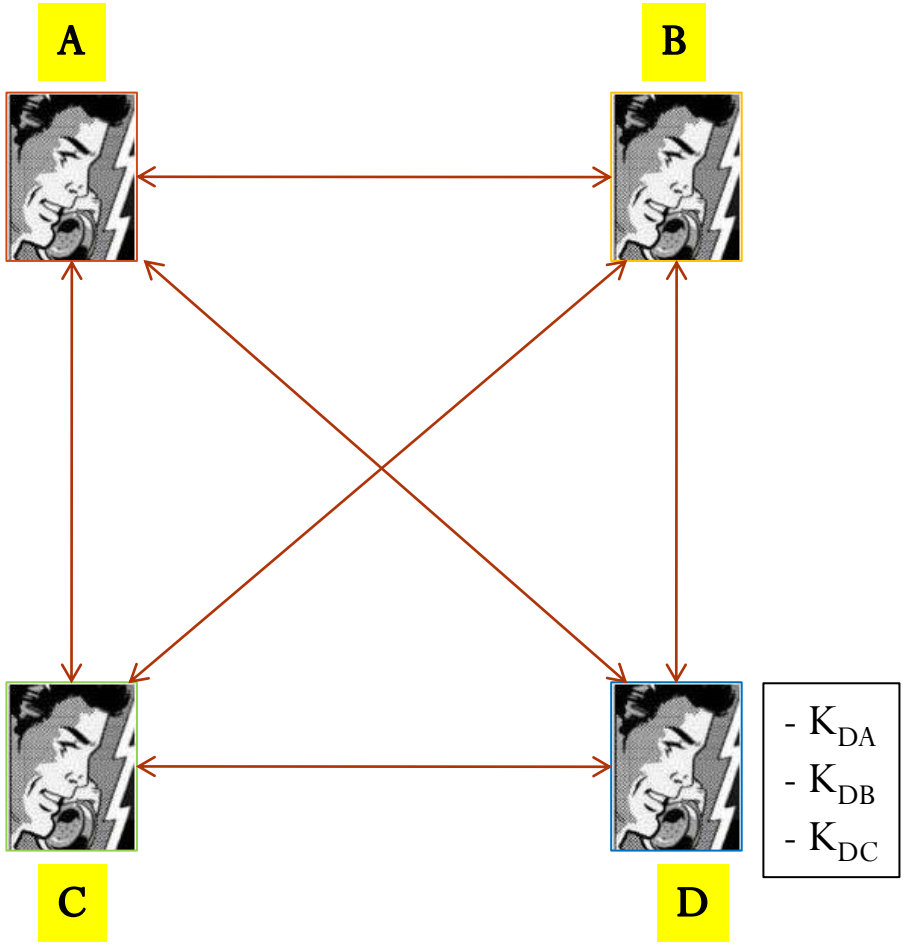
Interaction

Cert = {Alice's public key is pa}$_{sg}$

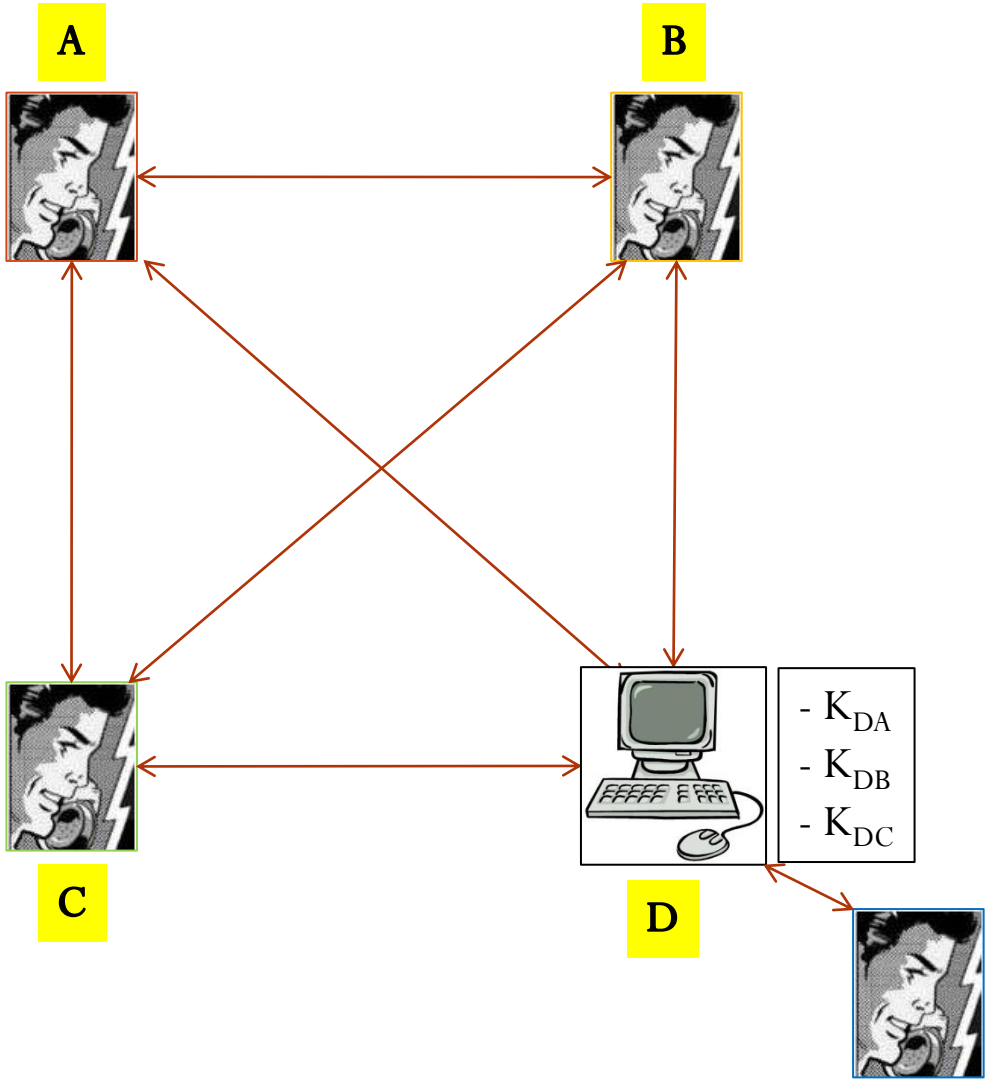
(sa, pa)

pa, Cert

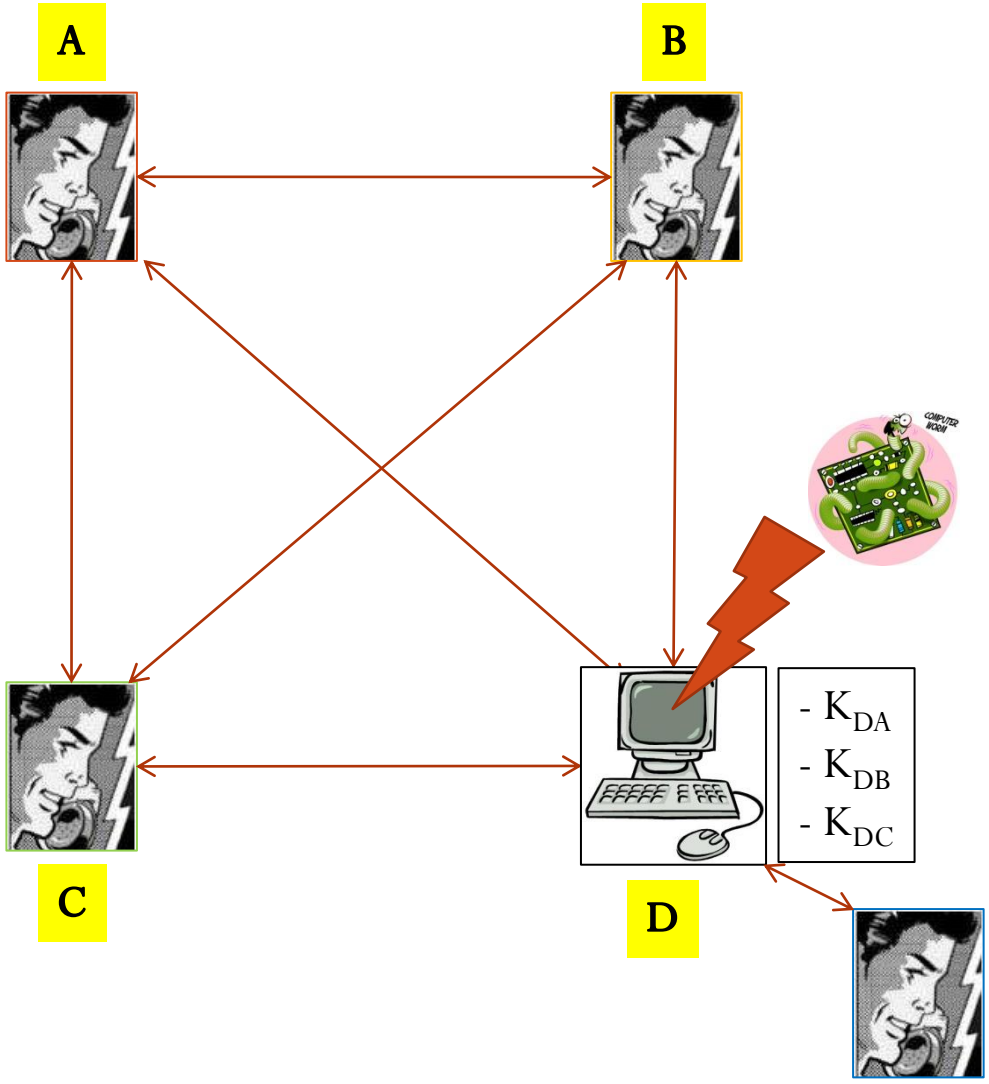
Key Distribution: Symmetric Setting



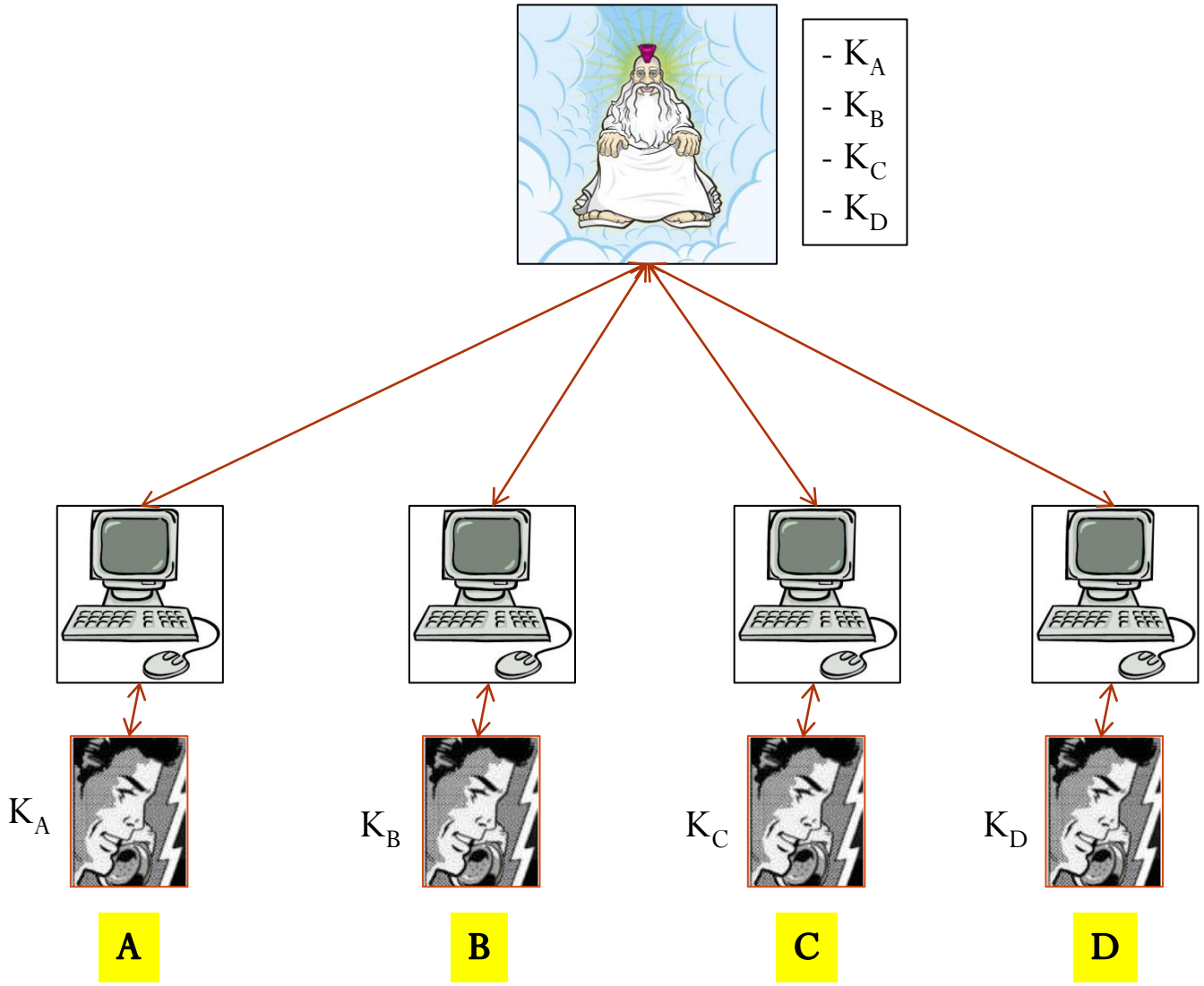
Key Distribution: Symmetric Setting



Key Distribution: Symmetric Setting



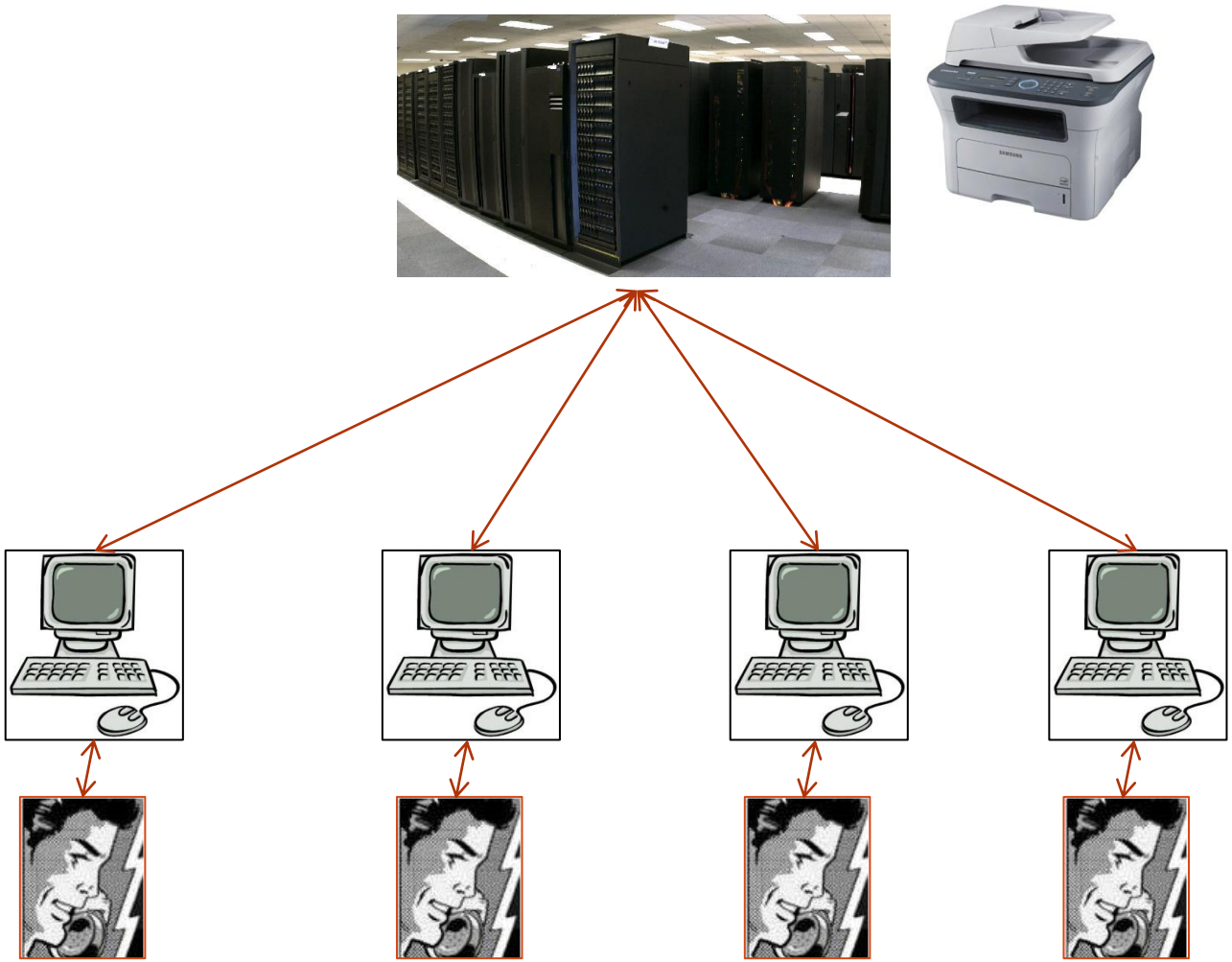
Key Distribution: Symmetric Setting



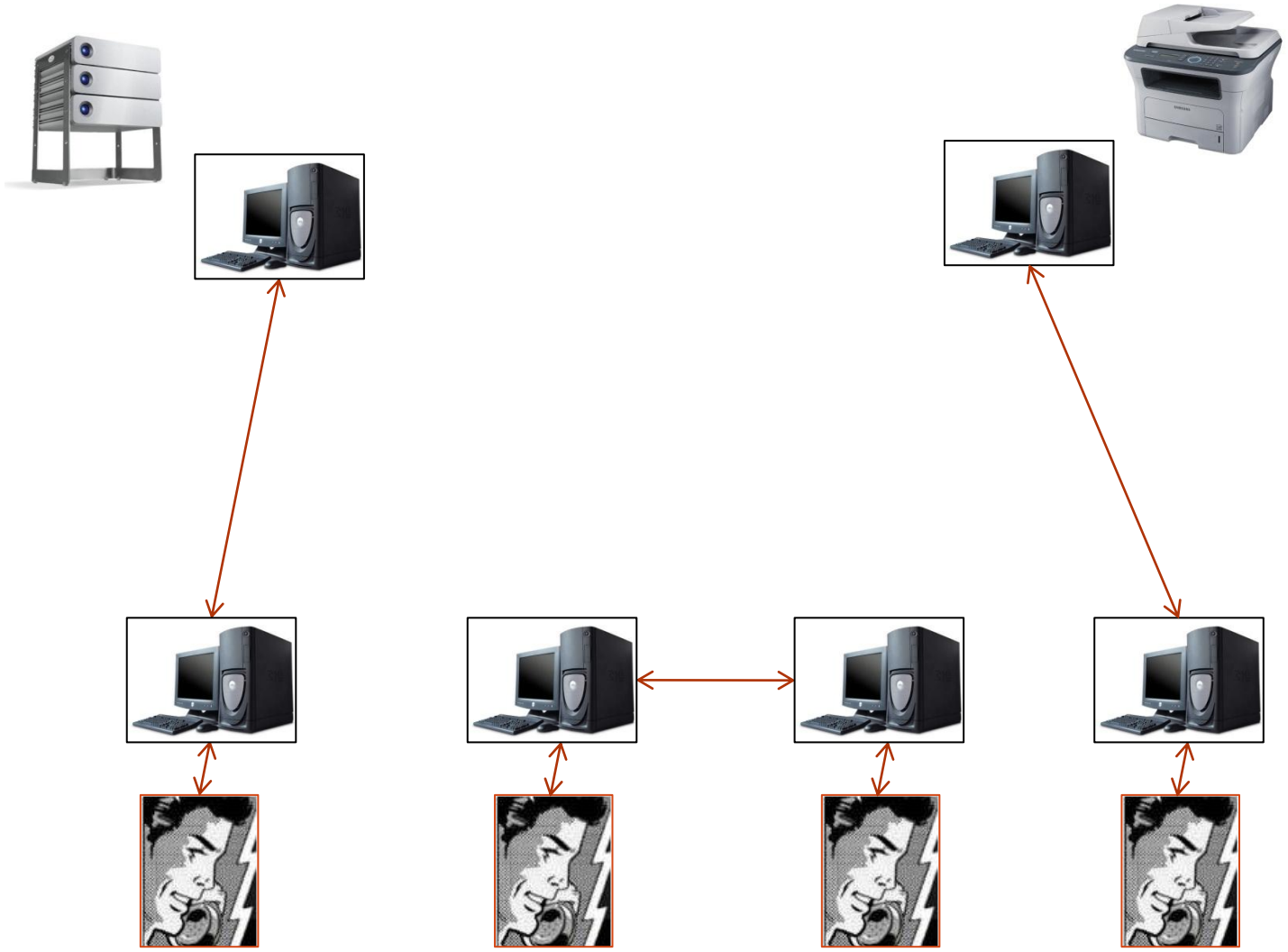
Key Distribution: Kerberos

Best understood using a dialogue in four scenes

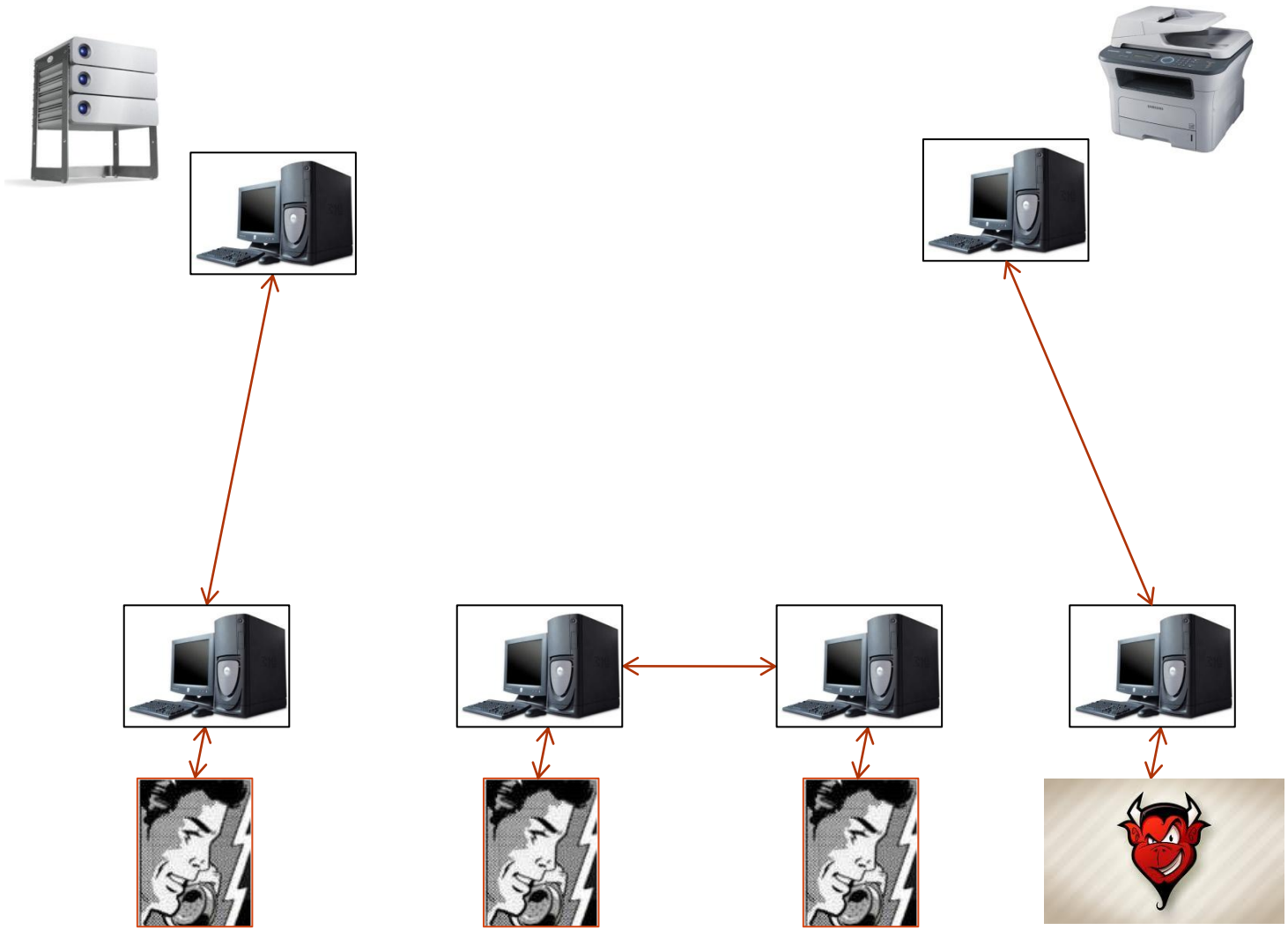
Kerberos: Scene I



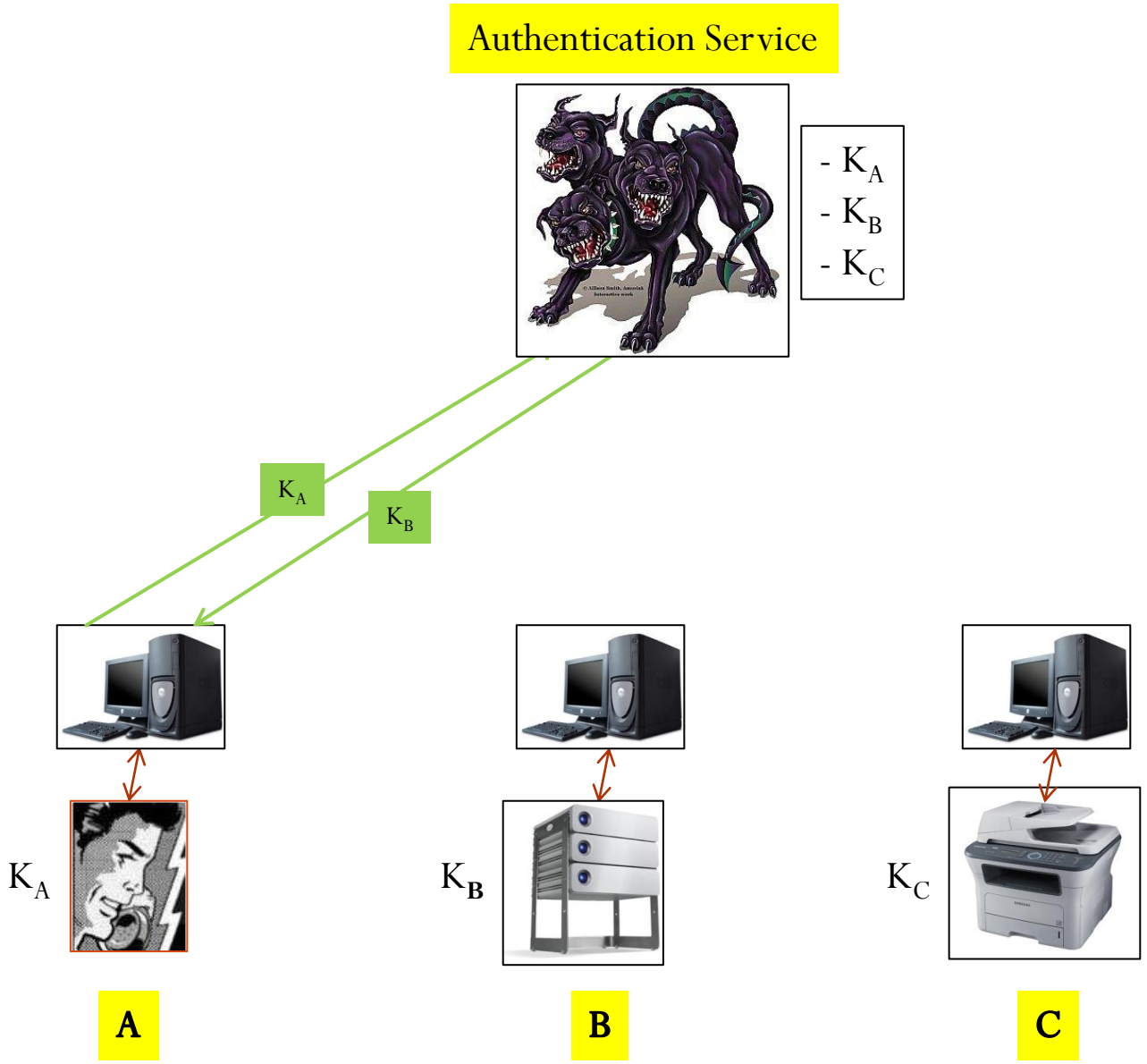
Kerberos: Scene I



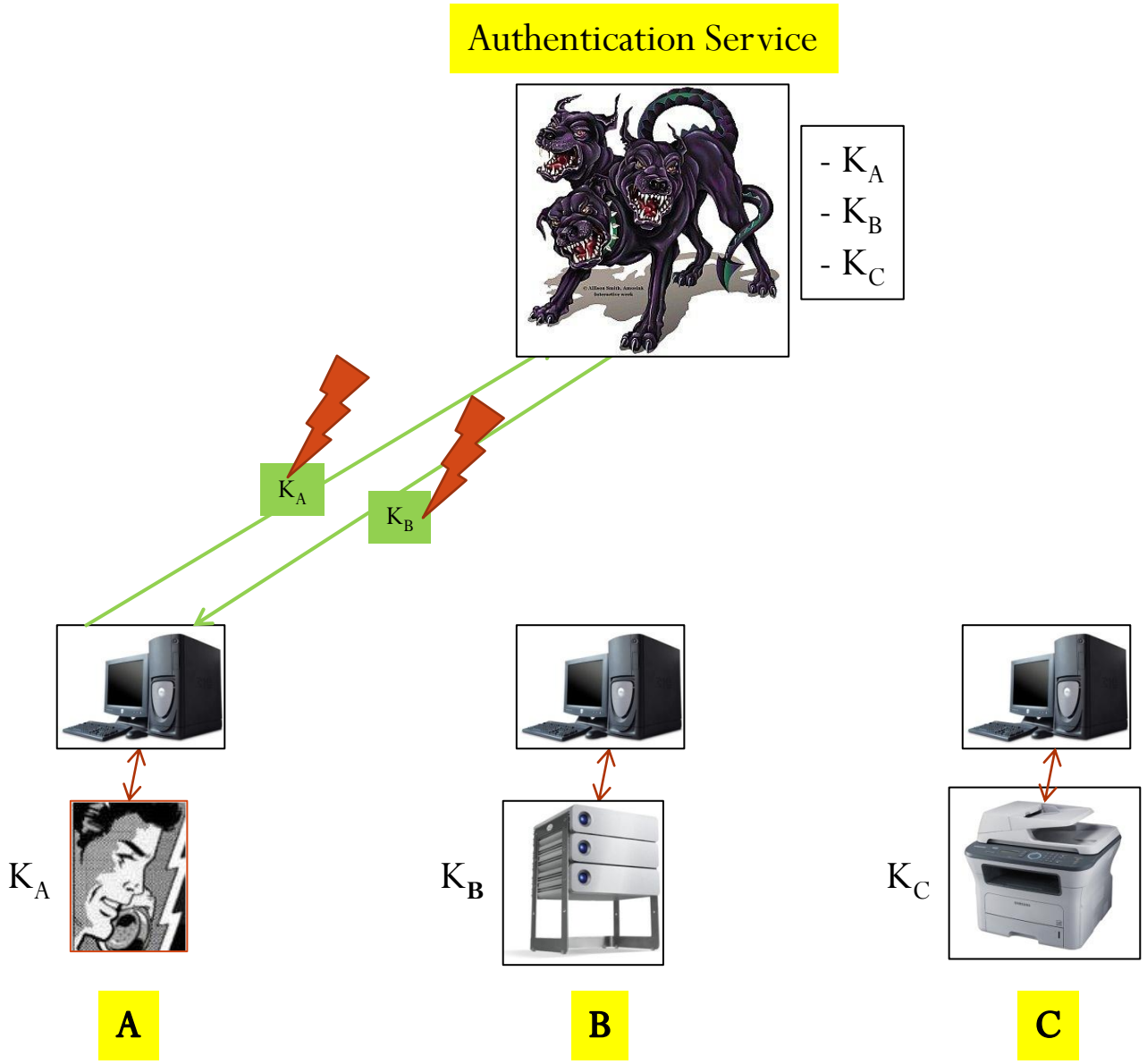
Kerberos: Scene I



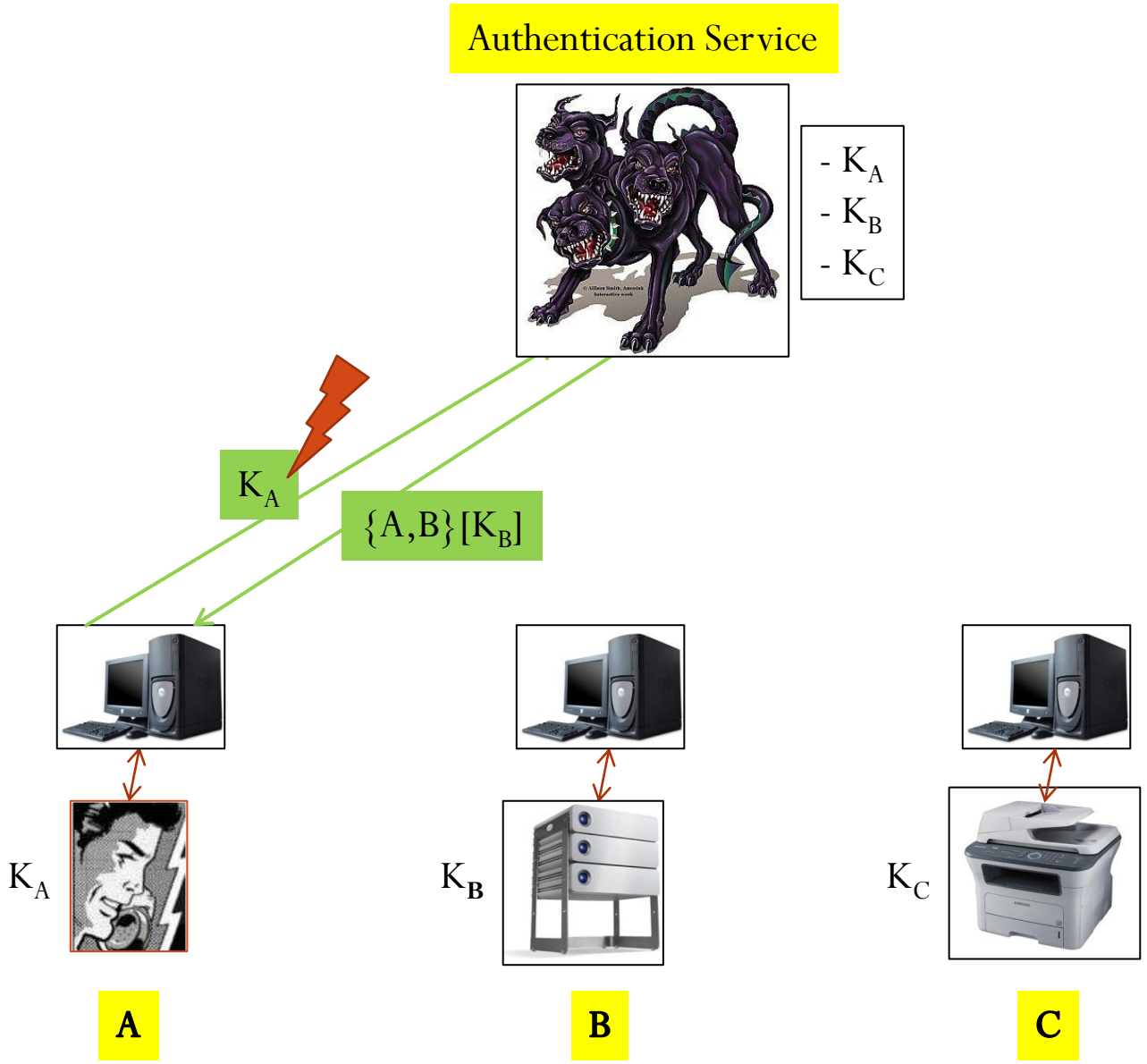
Kerberos: Scene II



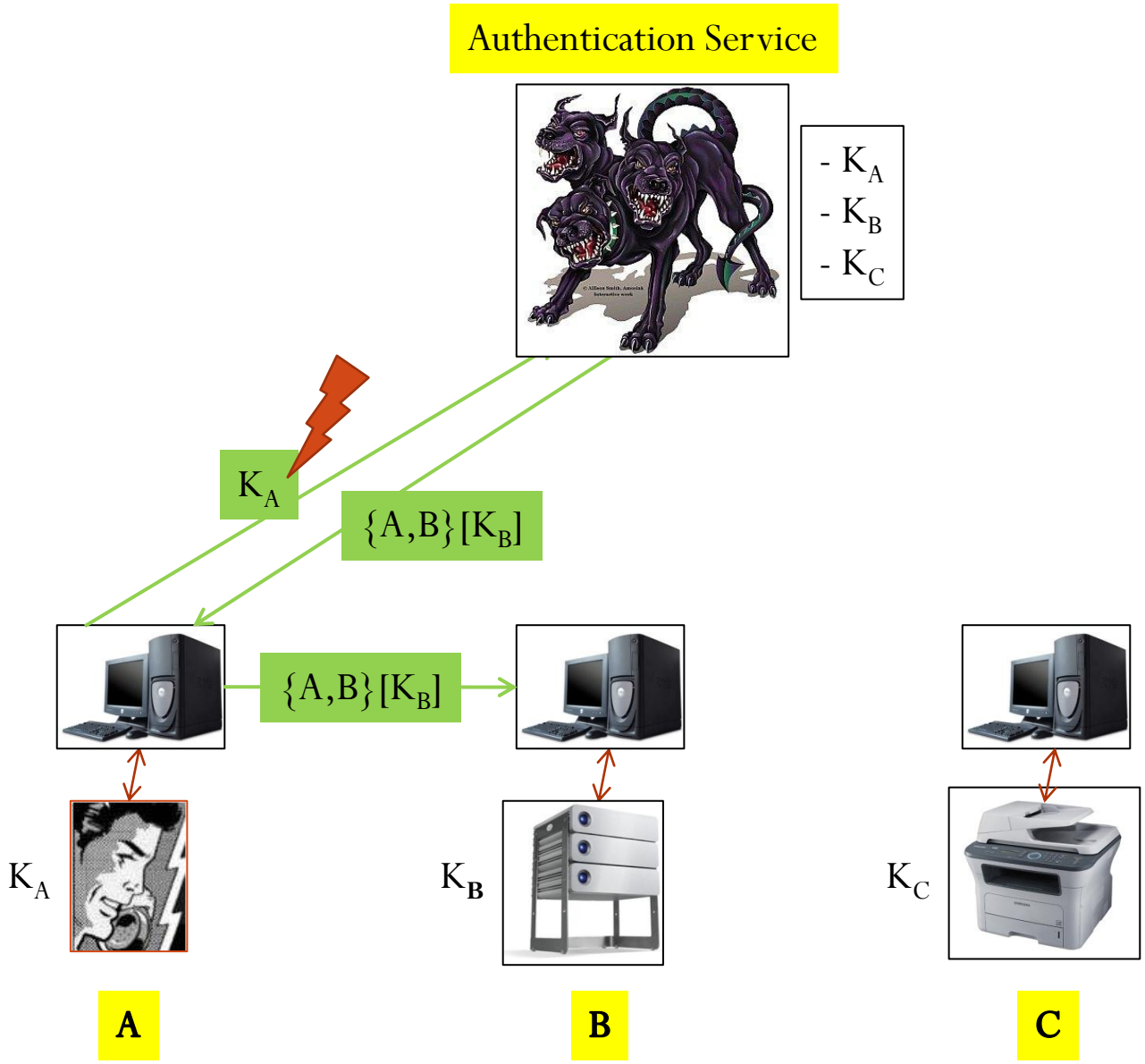
Kerberos: Scene II



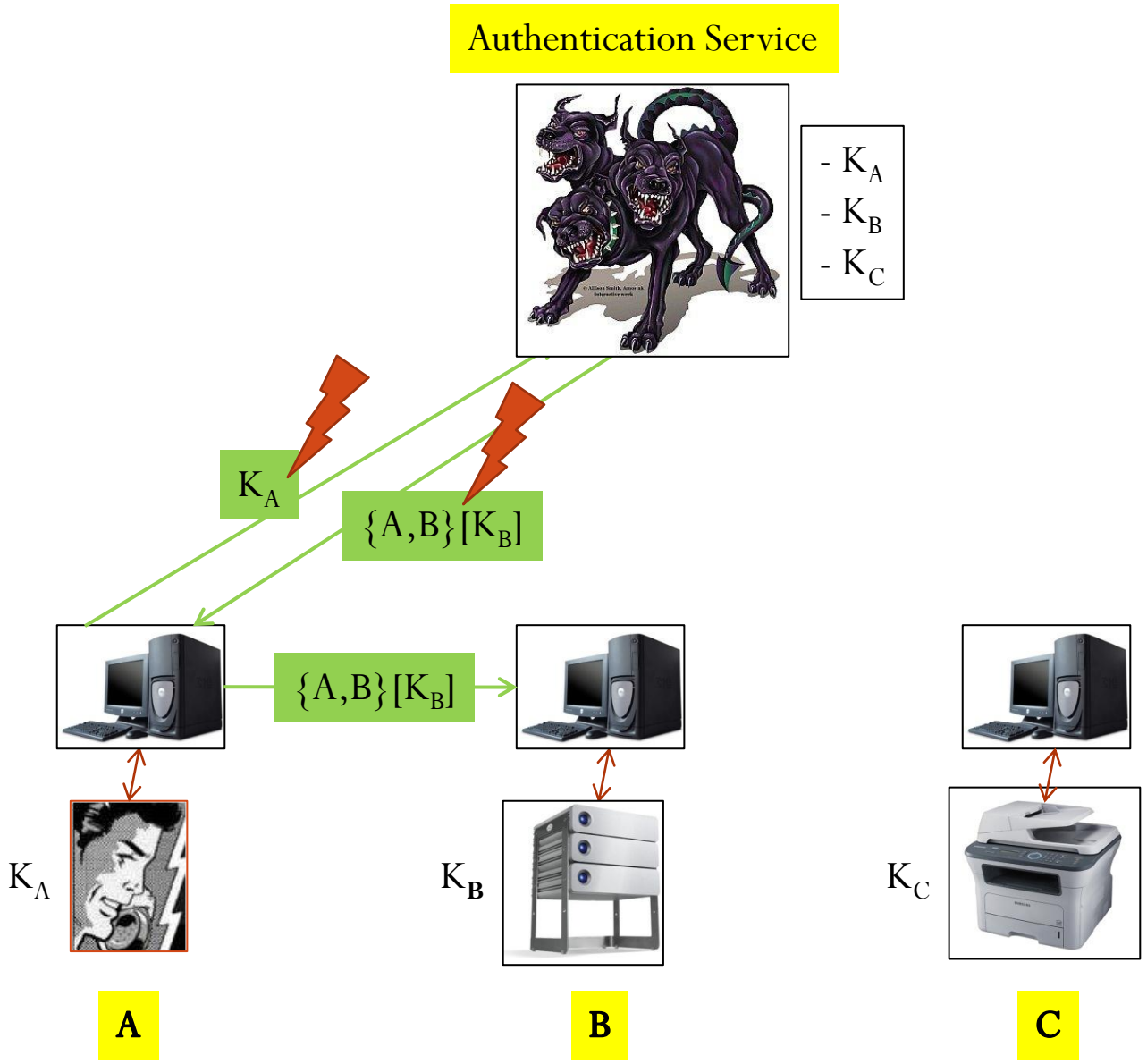
Kerberos: Scene II



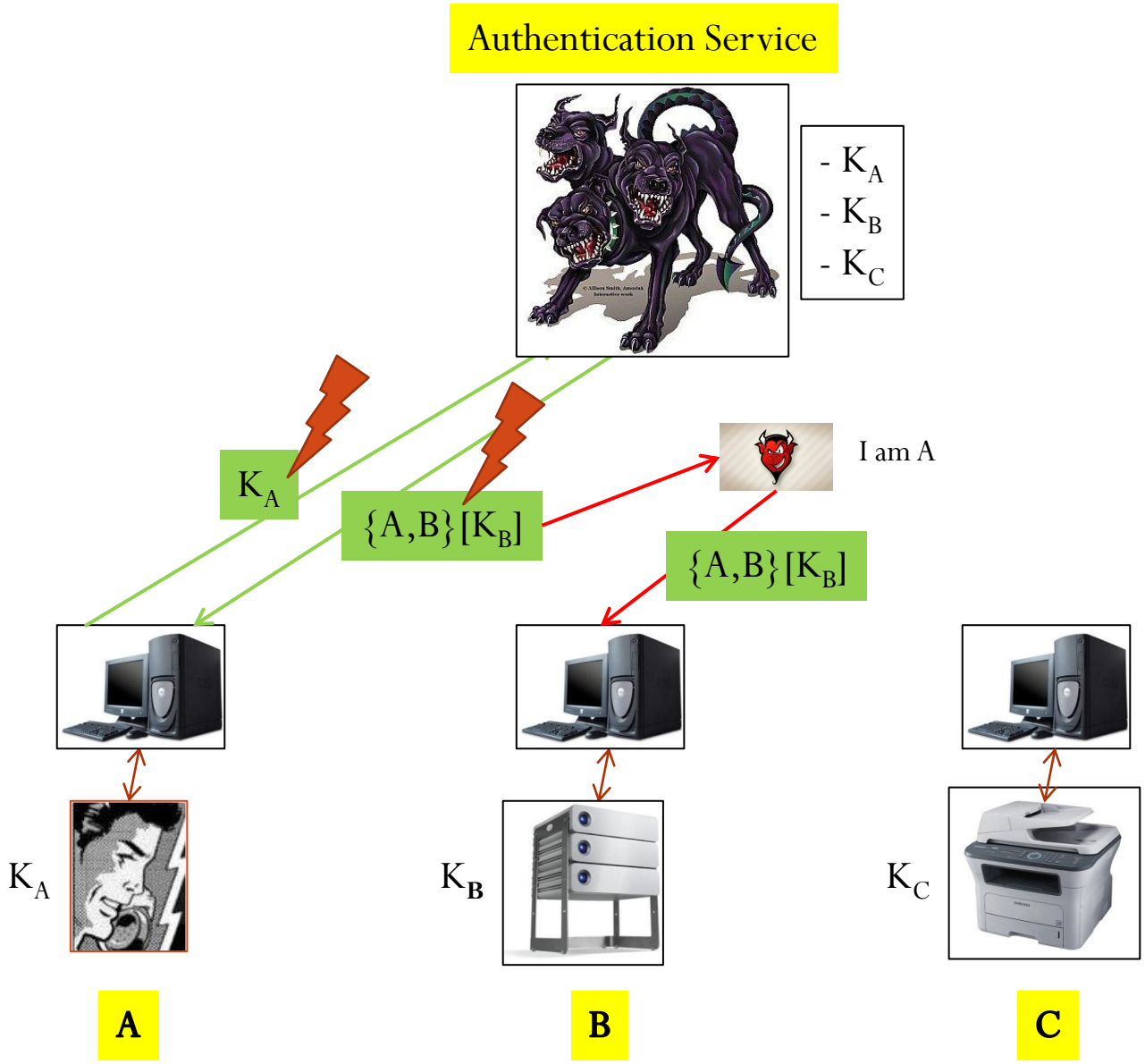
Kerberos: Scene II



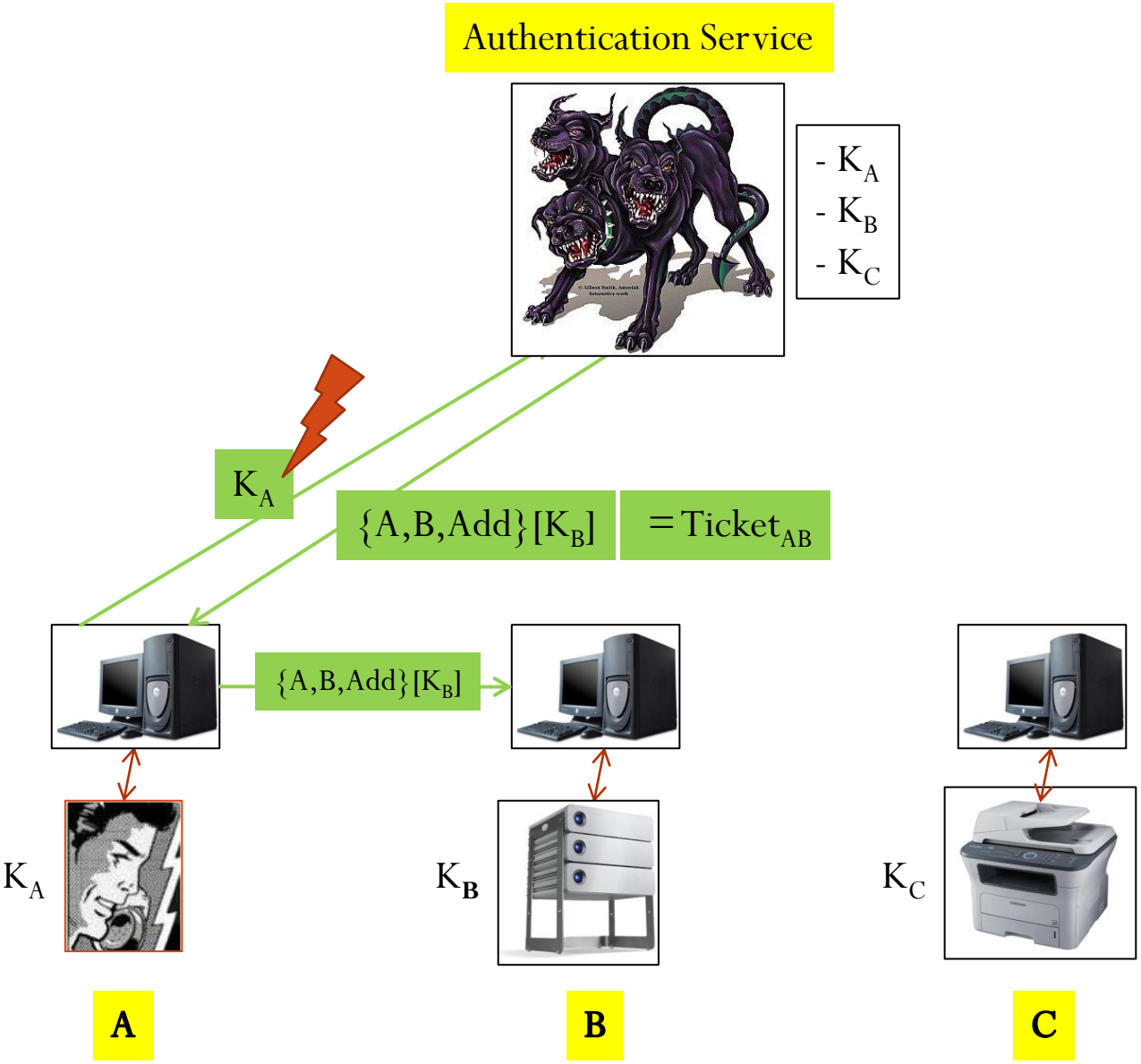
Kerberos: Scene II



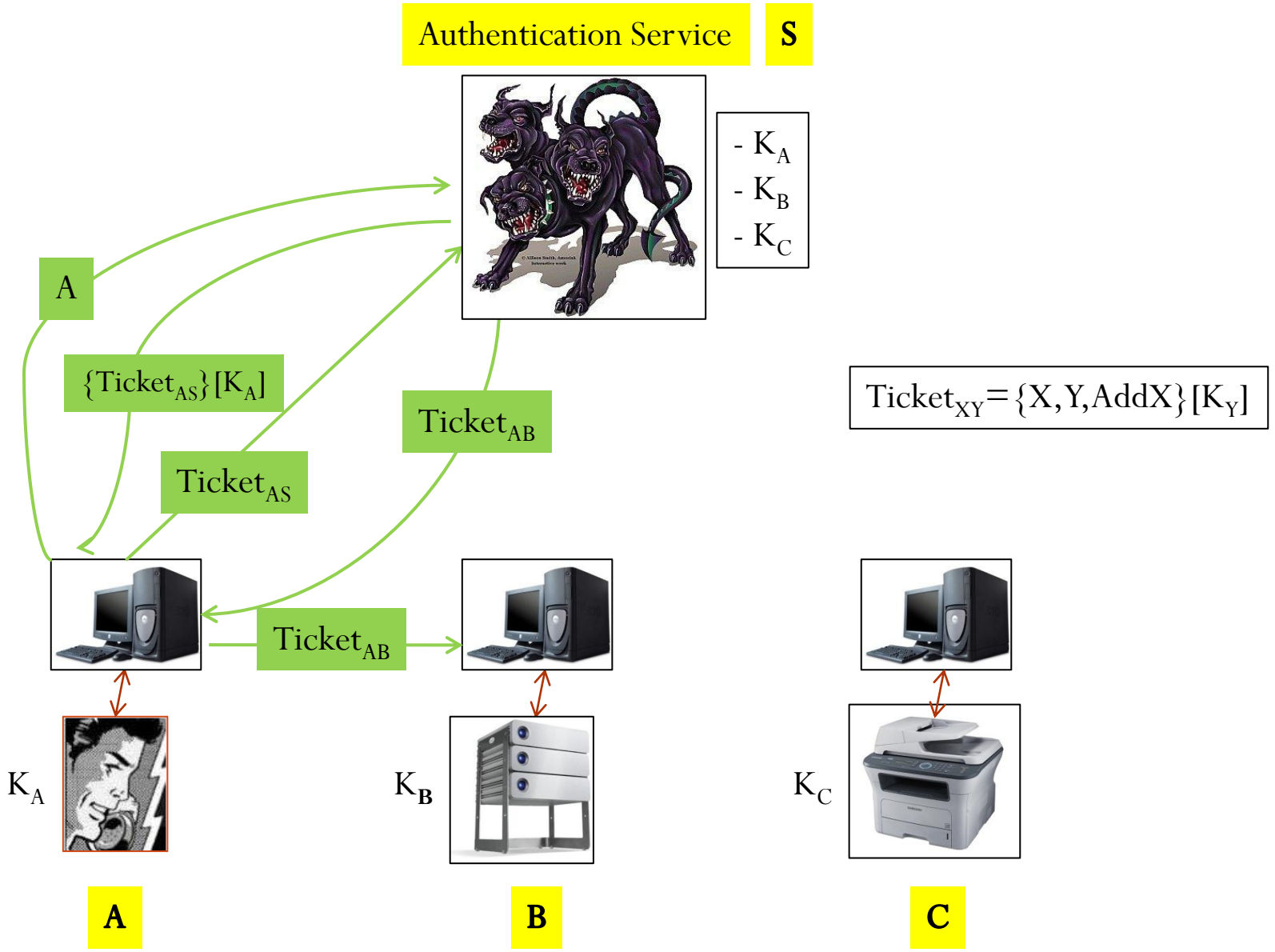
Kerberos: Scene II



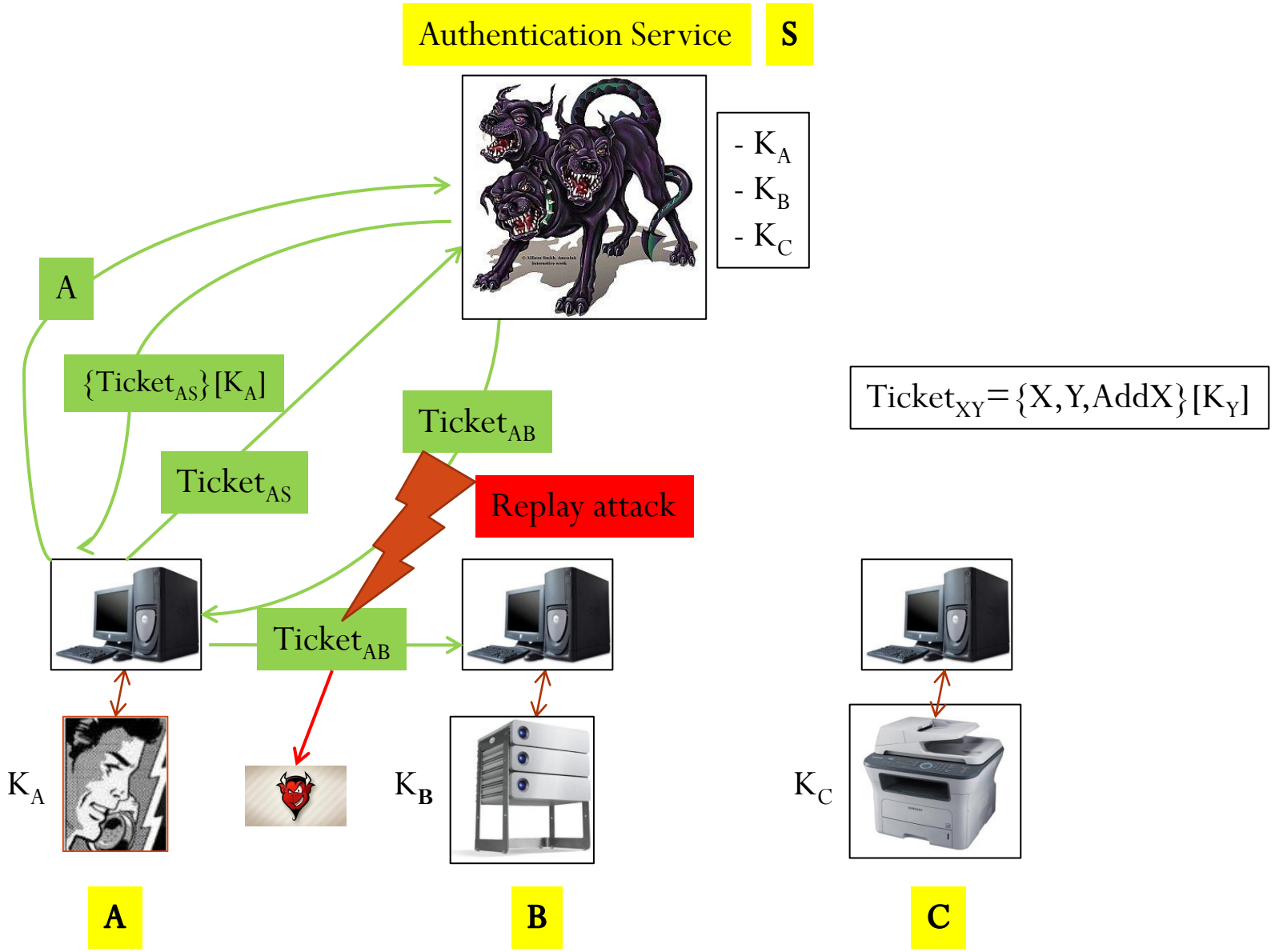
Kerberos: Scene II



Kerberos: Scene III



Kerberos: Scene III



Kerberos: Scene III

Authentication Service **S**

- K_A
- K_B
- K_C

$Ticket_{XY} = \{X, Y, AddX\}[K_Y]$

K_A

A

$Ticket_{AB}$

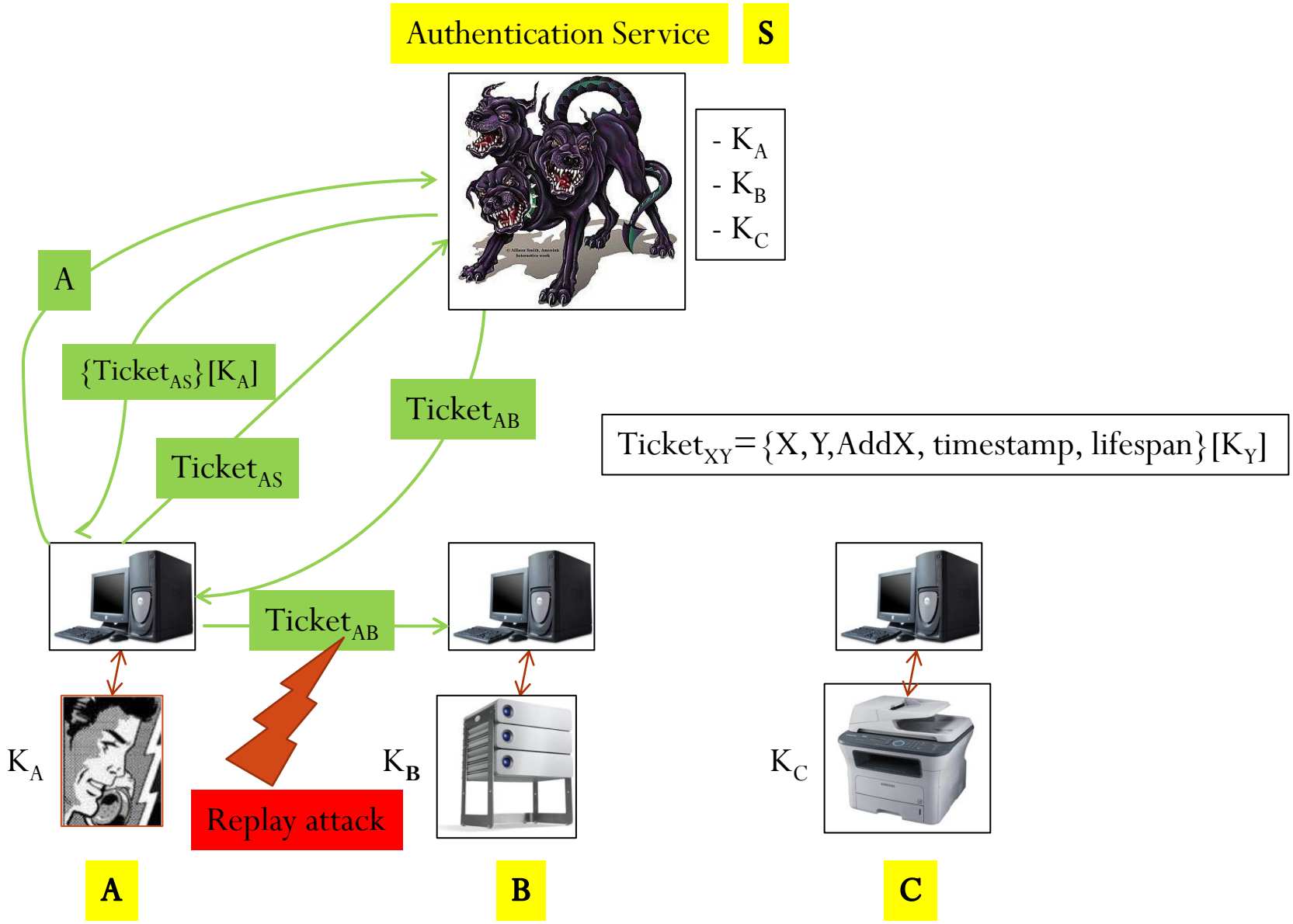
K_B

B

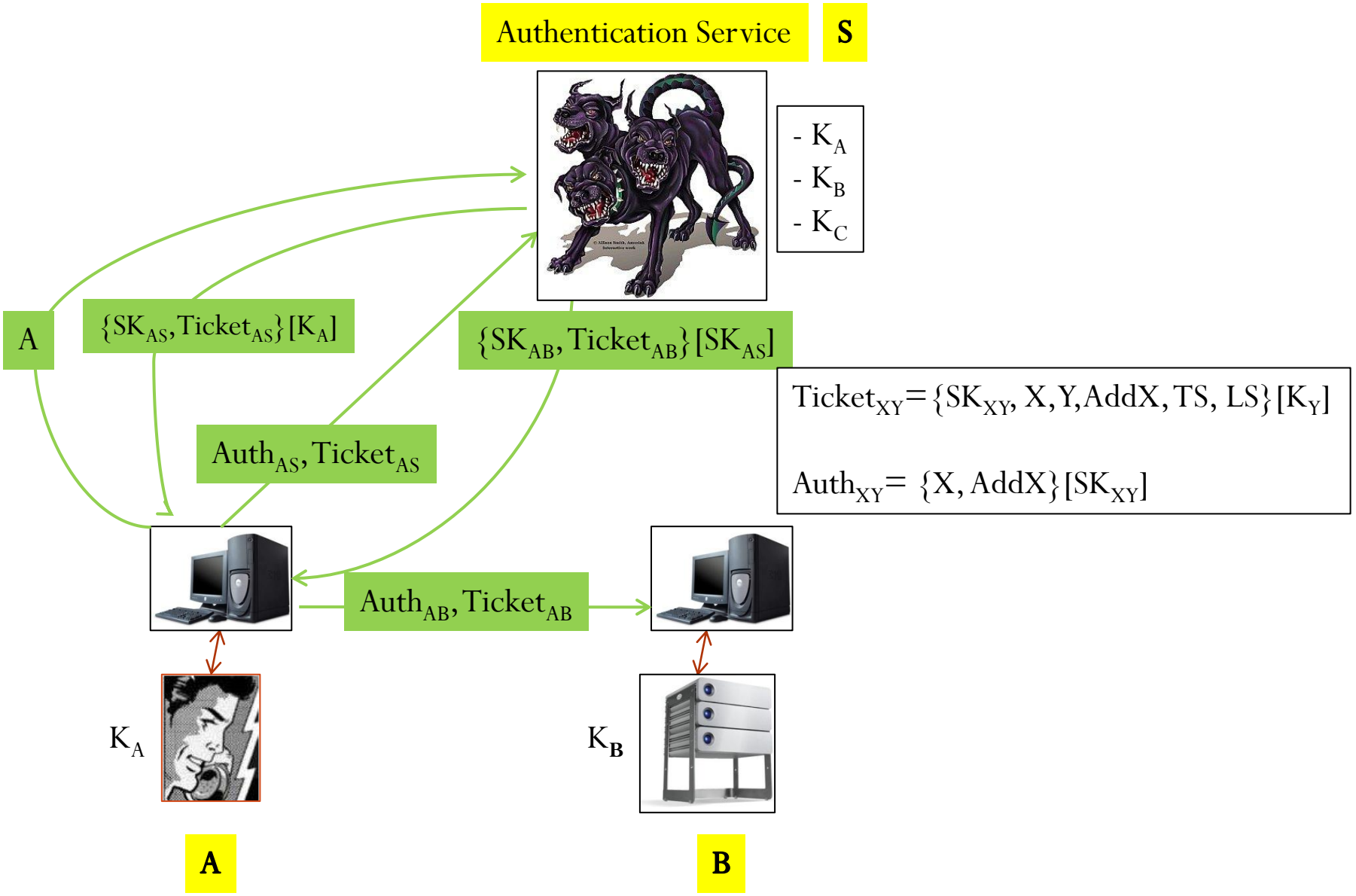
K_C

C

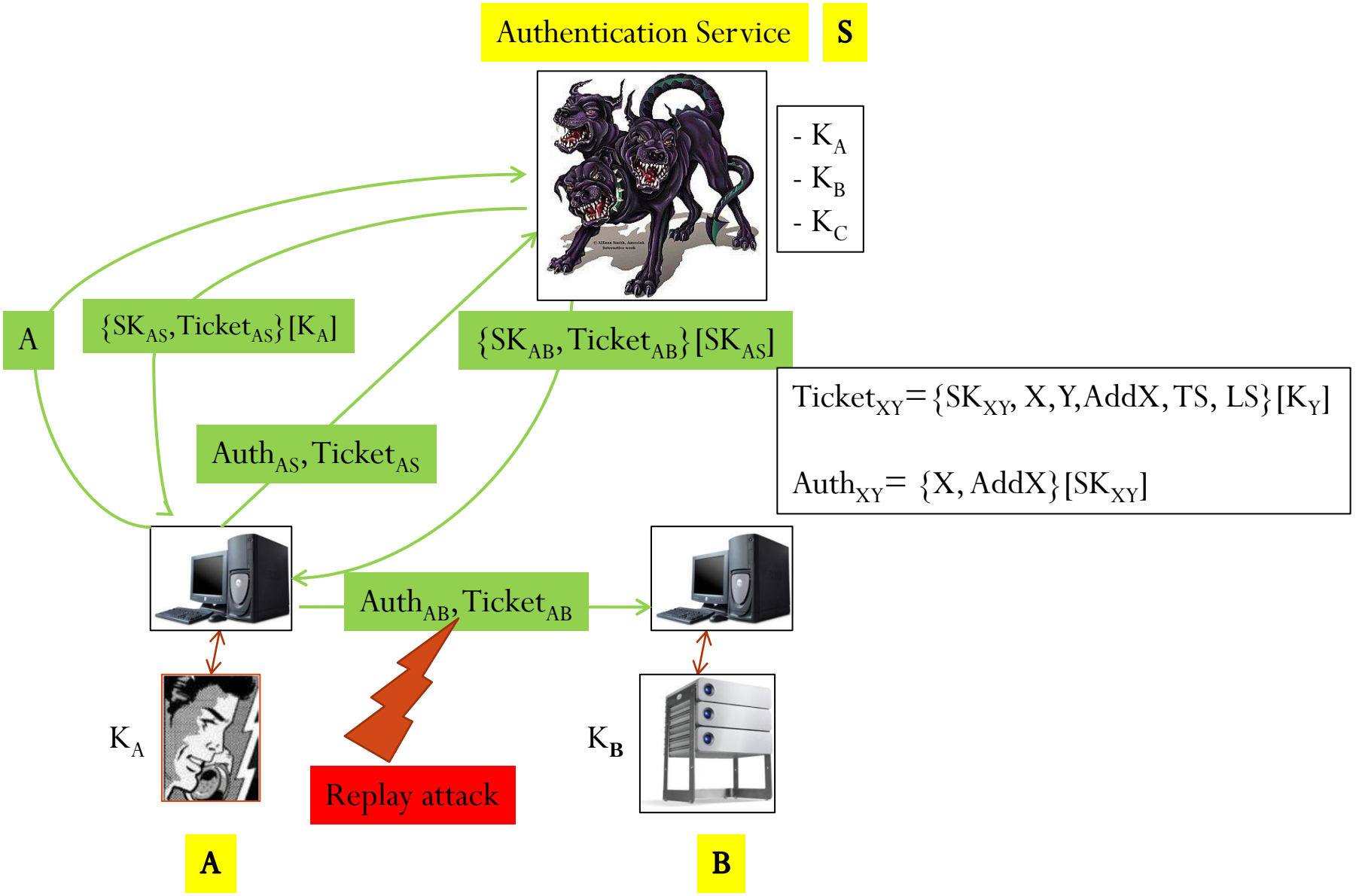
Kerberos: Scene III



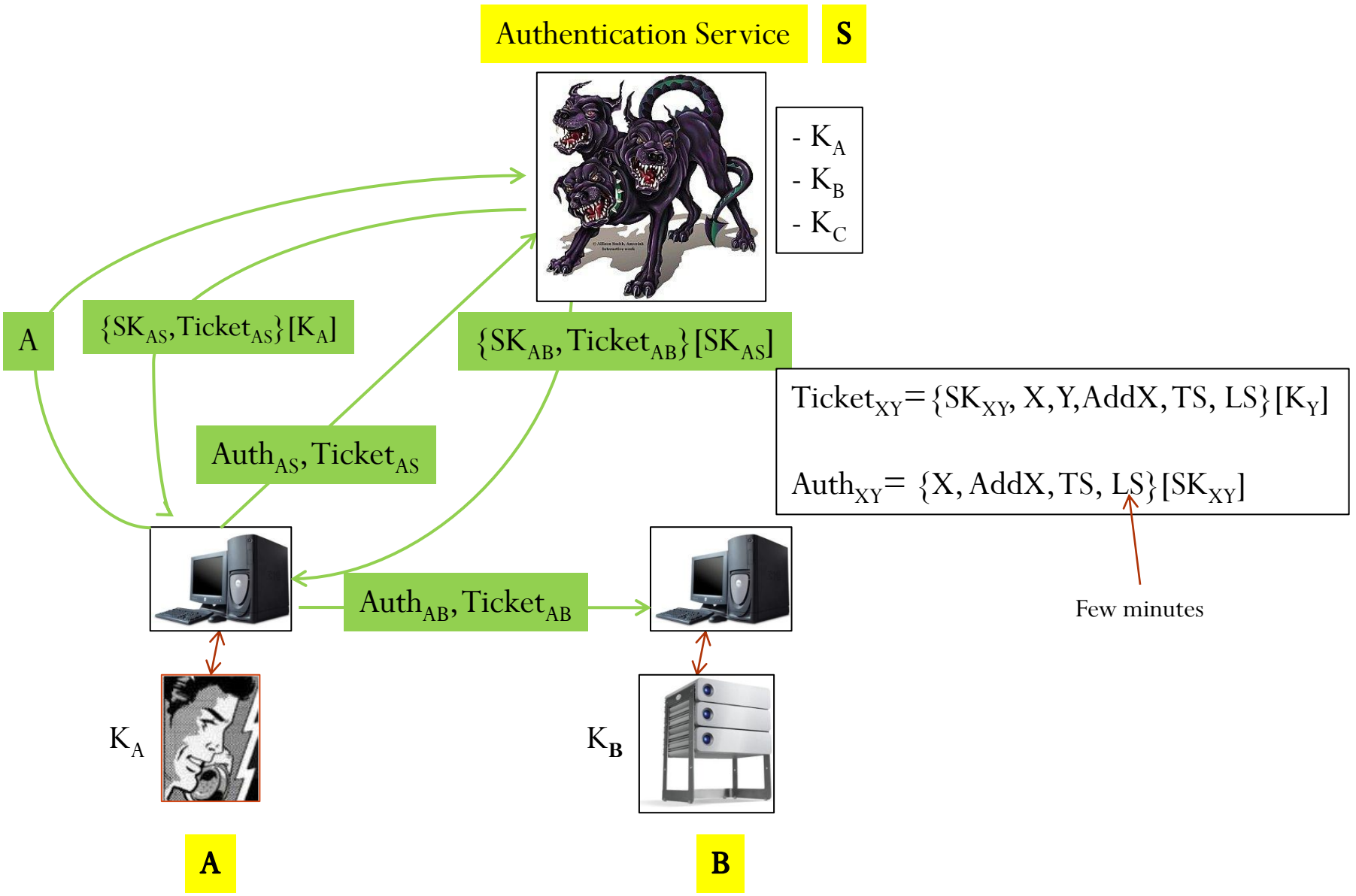
Kerberos: Scene IV



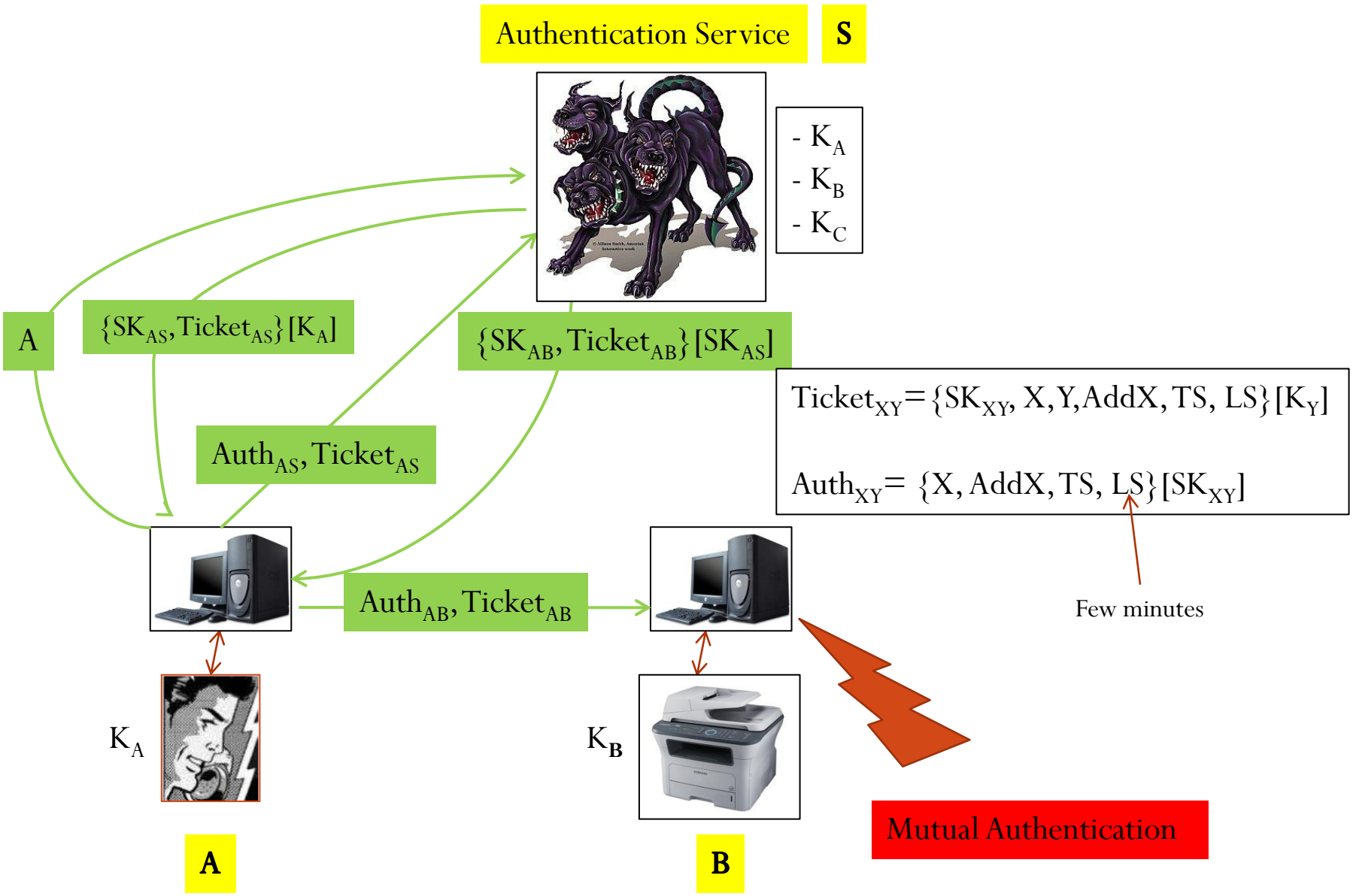
Kerberos: Scene IV



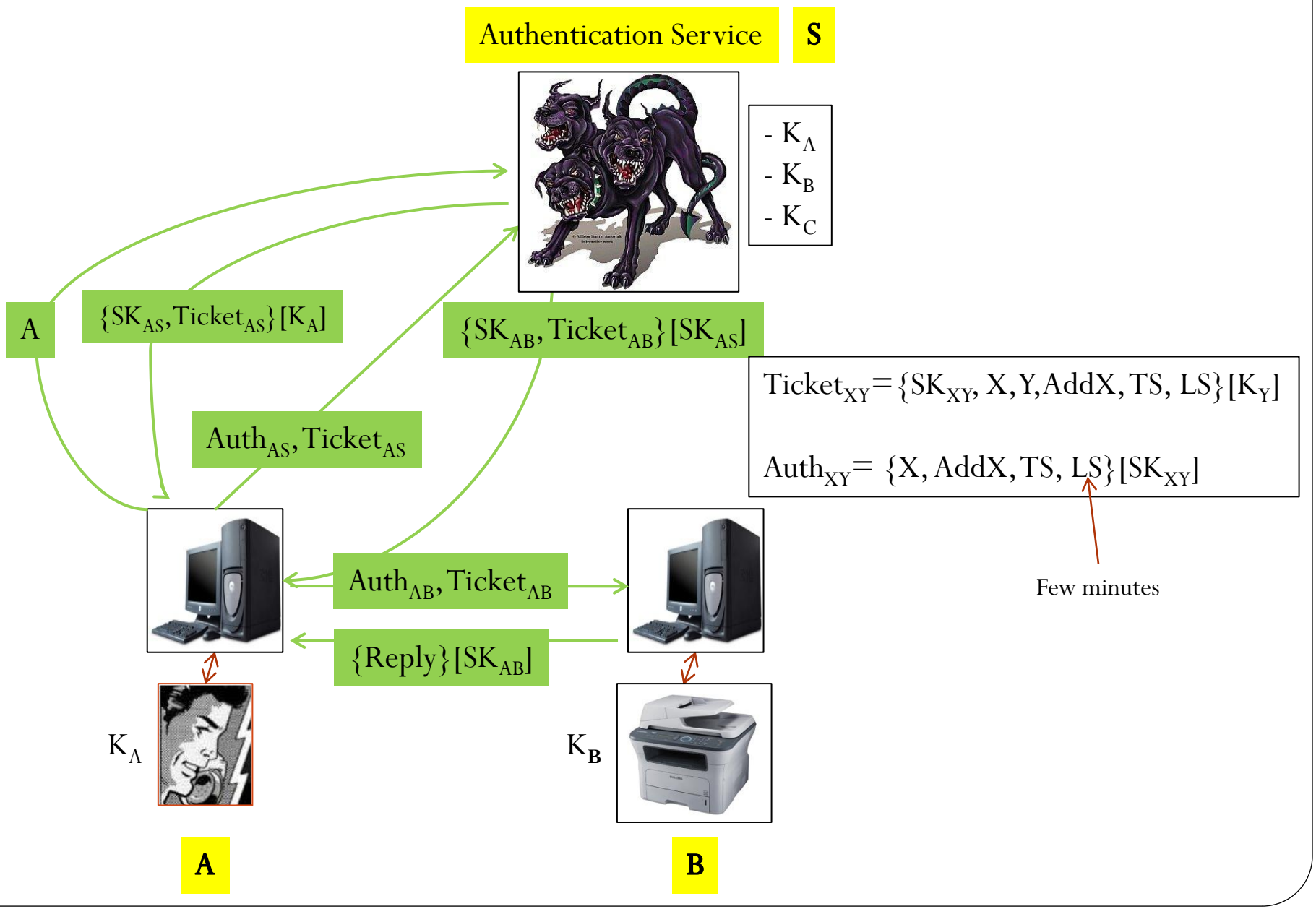
Kerberos: Scene IV



Kerberos: Scene IV



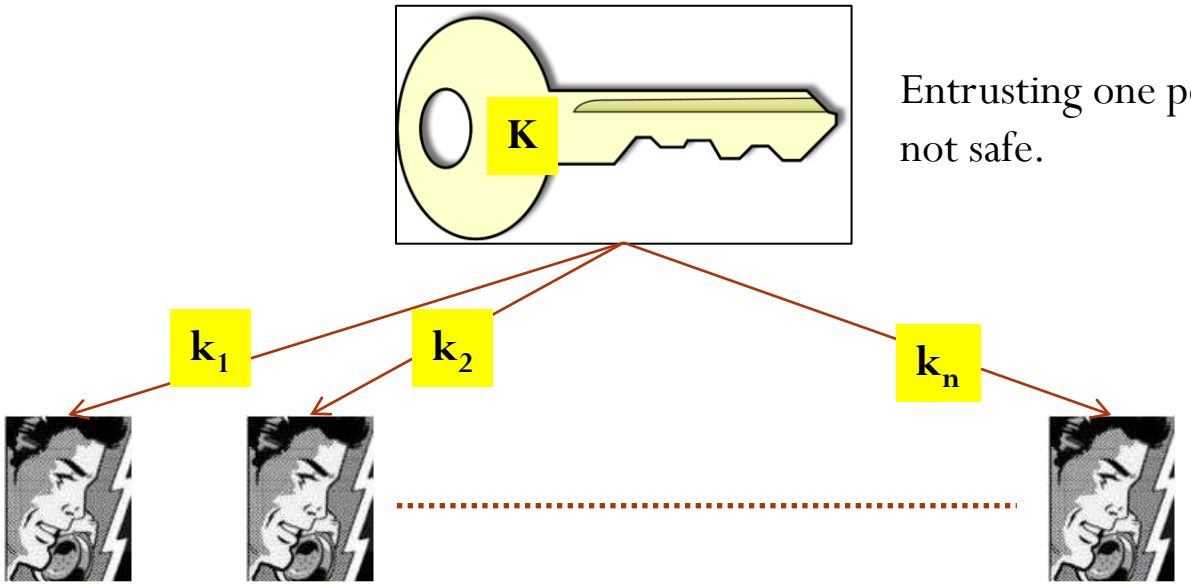
Kerberos: Scene IV



Other Cryptographic Protocols

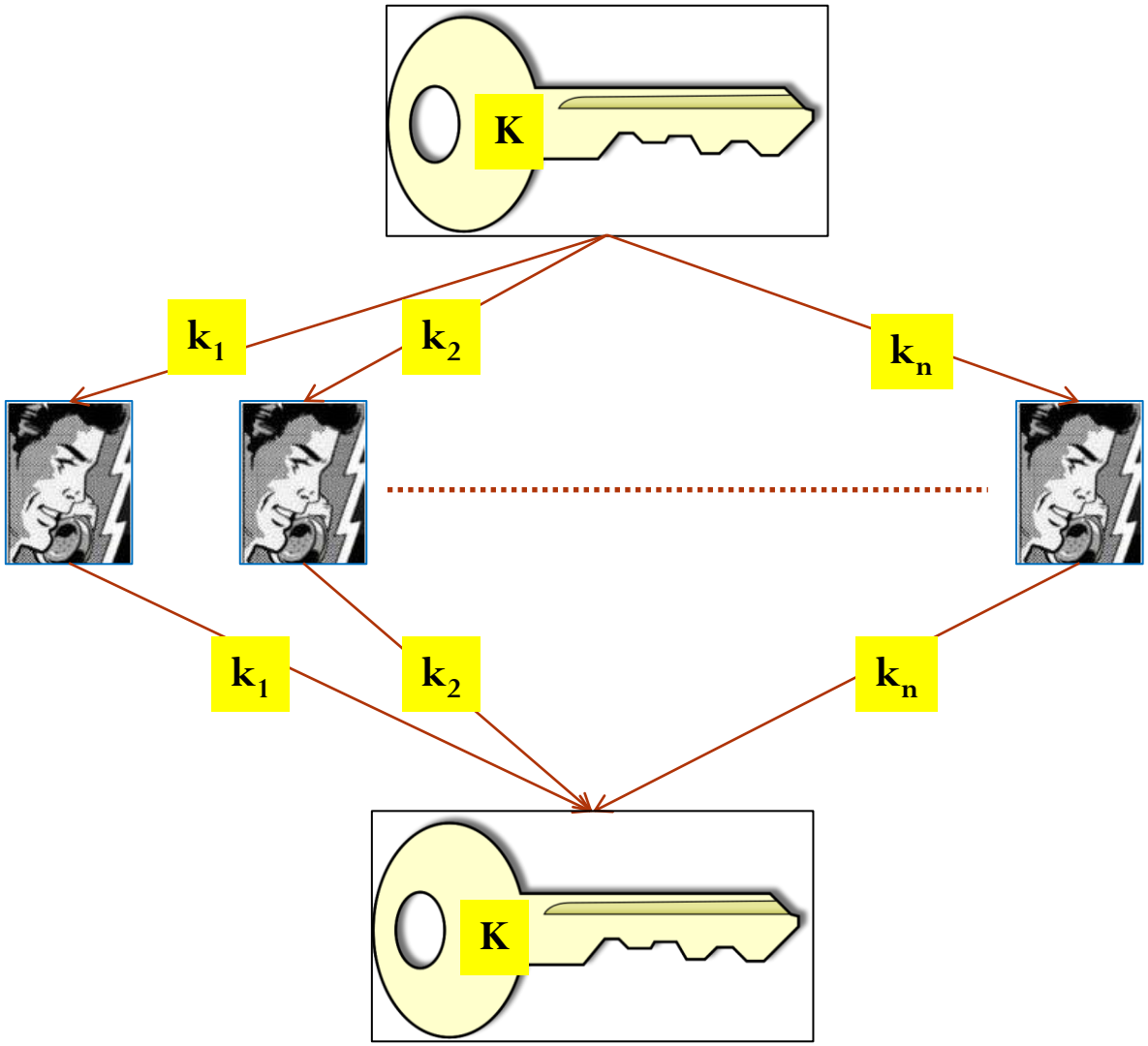
- Secret sharing
- Coin flipping over phone
- Oblivious transfer

Secret Sharing

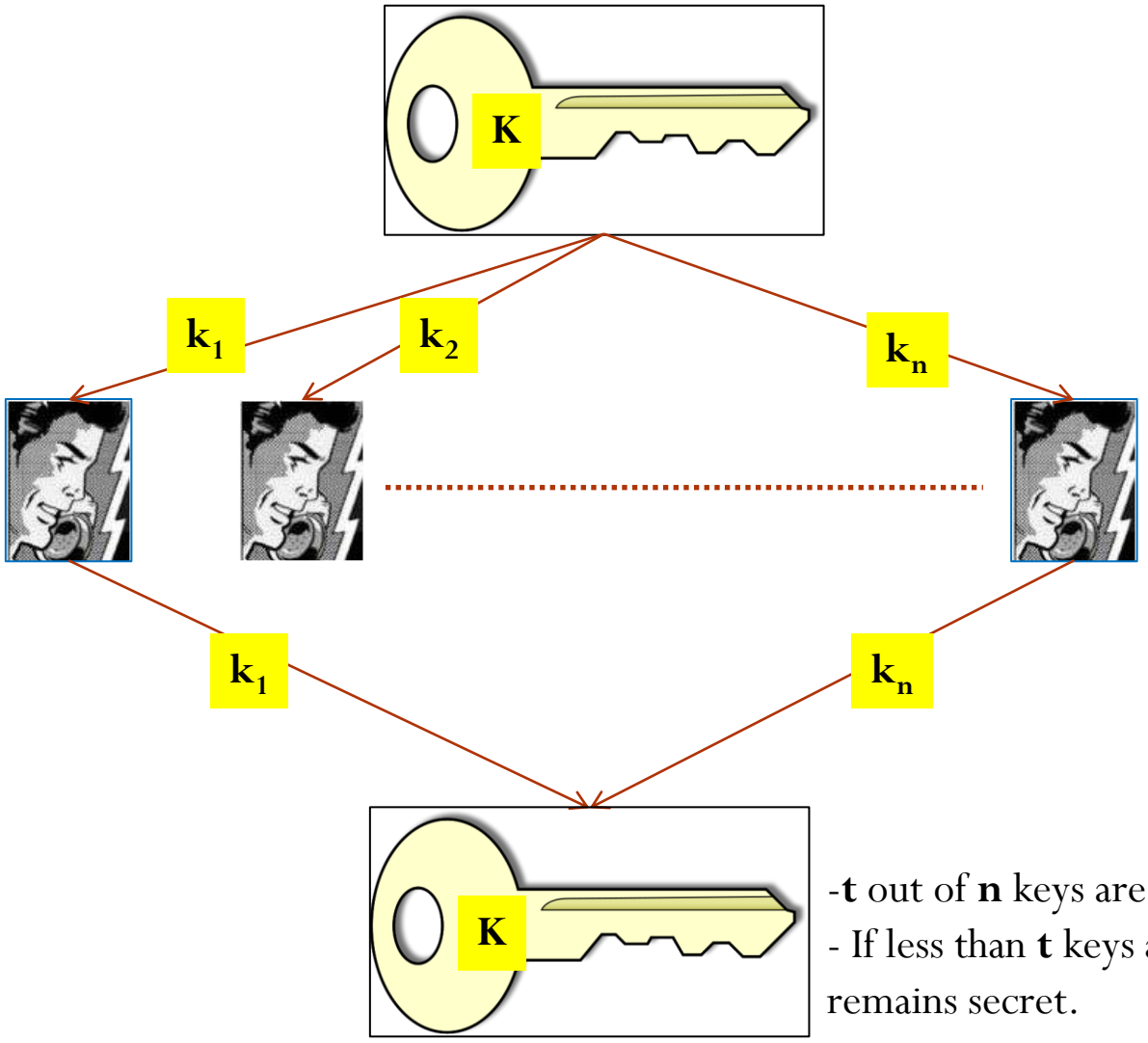


Entrusting one person with K is not safe.

Secret Sharing



Secret Sharing



-**t** out of **n** keys are sufficient to obtain **K**
- If less than **t** keys are available, then **K** remains secret.

Secret Sharing

- How do we construct such a protocol?
  - Ideas?

Secret Sharing

- How do we construct such a protocol?
  - Shamir's secret sharing protocol: A degree **d** polynomial is completely determined by **d** points evaluated on the polynomial.

Coin flipping

Alice and Bob want to agree on a secret bit.

Coin flipping

Alice and Bob want to agree on a secret bit.

Coin flipping

Alice and Bob want to agree on a secret bit.

Bit commitment protocol

Other protocols we did not talk about

- Oblivious transfer.
- Multi-party computation.
- Electronic voting.
- …

Thank you