

Computer security: authentication of principals and cryptographic protocols

6.033 Spring 2007

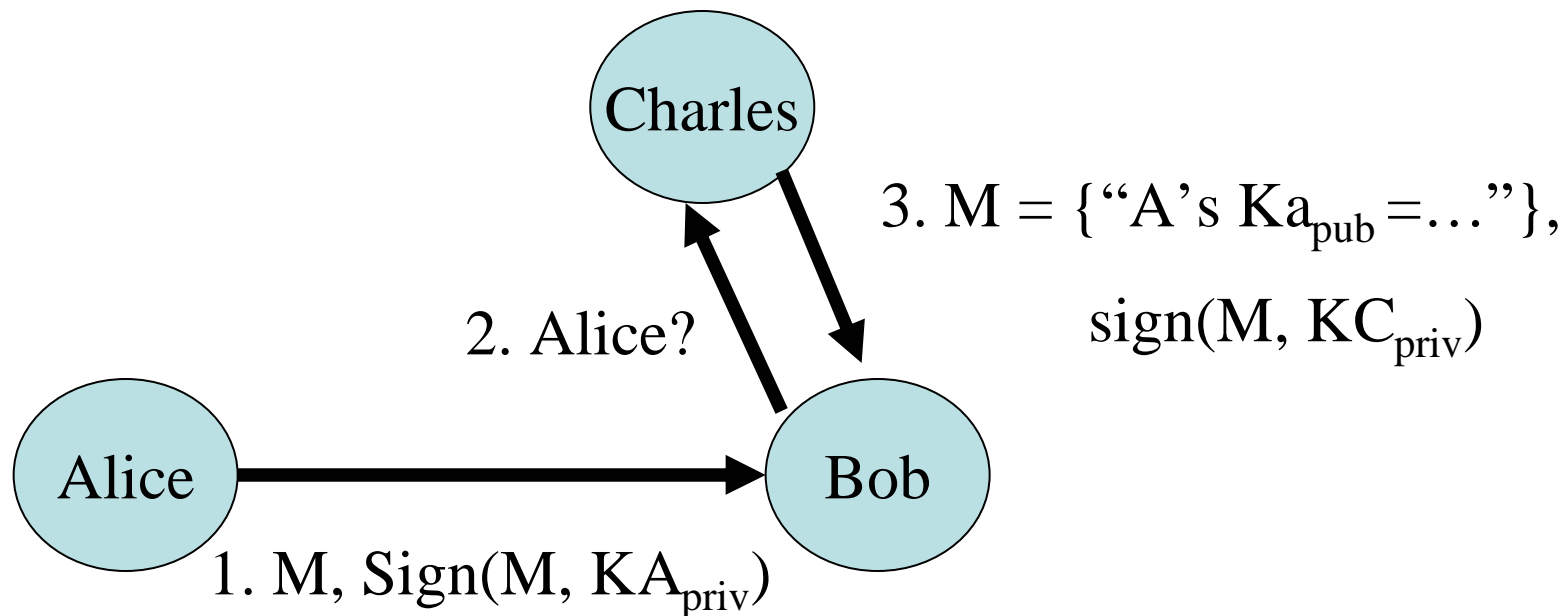
HKN Underground Guide

<https://sixweb.mit.edu/student/evaluate/6.033-s2007>

Link posted on 6.033 home page

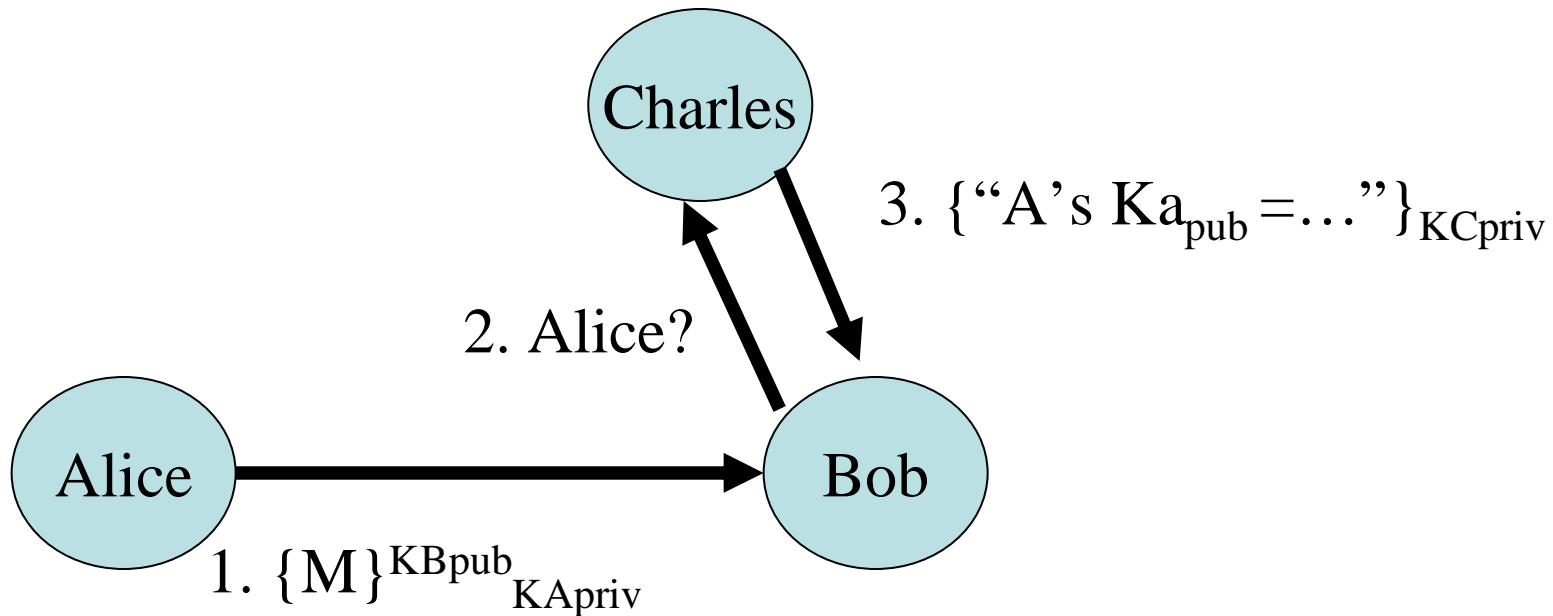
Deadline: May 20

▪ key distribution



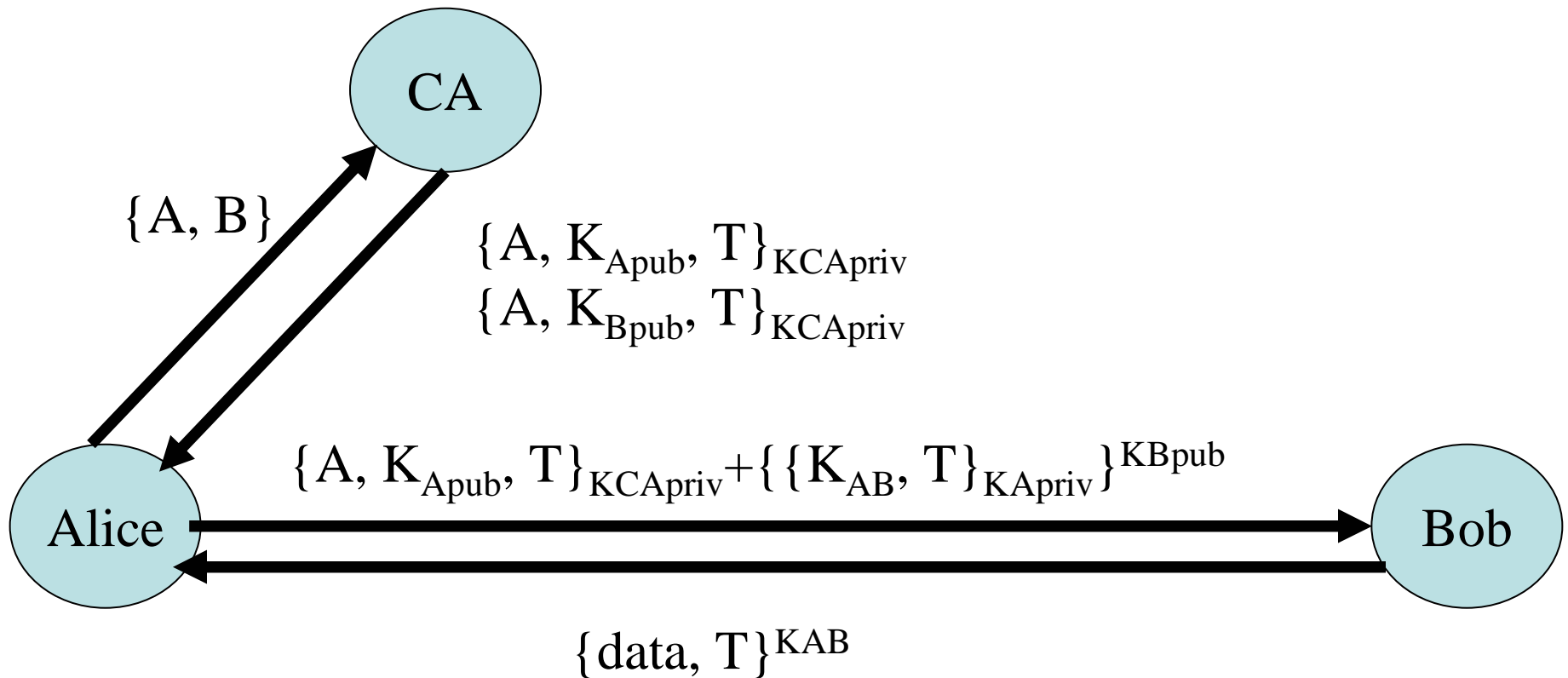
- 3 is a *certificate* for Alice's public key
- Charles is called a *certificate authority*
- The interaction is an example of a *cryptographic protocol*

▪ Shorter notation



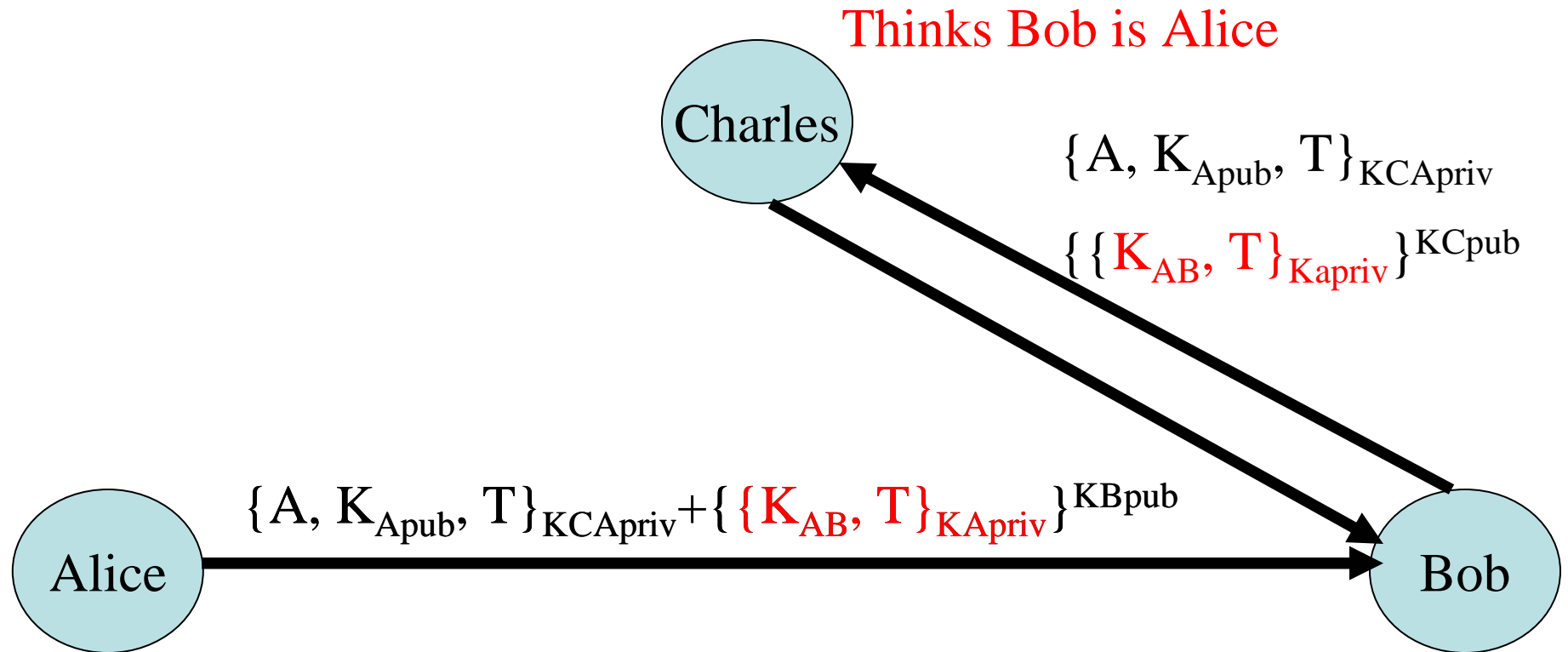
- Subscript for signing
- Superscript for encrypting

Denning-Sacco

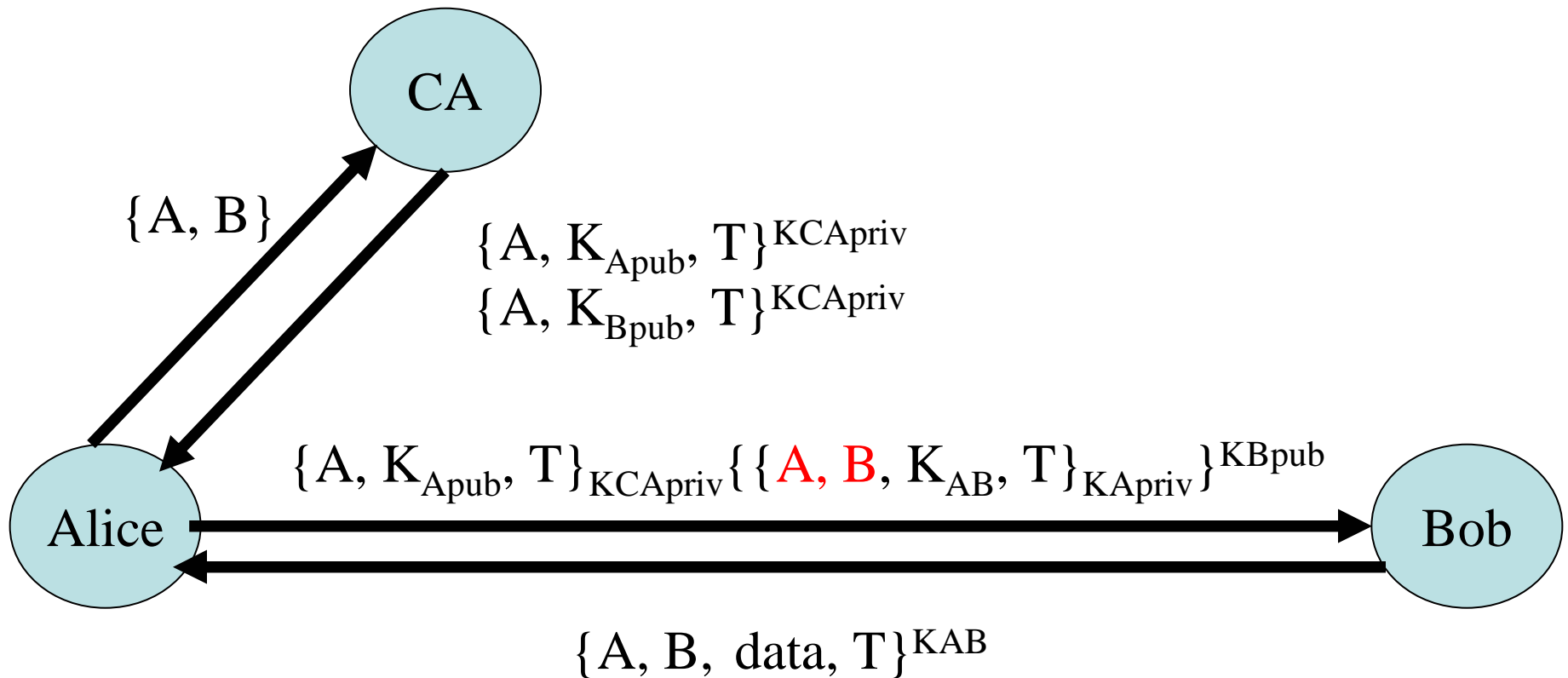


1. Authenticate Alice to Bob and Bob to Alice
2. Set up a shared-secret key

Impersonation Attack



Denning-Sacco (fixed)



Be explicit!

Example: Web (SSL simplified)

- U: <https://www.amazon.com>
- B \rightarrow W: {random_c, session-id, ciphersuites}
- B \leftarrow W: {random_s, session-id,
 {amazon.com, K_{pub-amazon}}_{K_{versign}}}
- B: verify({amazon.com, K_{pub-amazon}}_{K_{versign}},
 K_{pub-verisign})?
- B \rightarrow W: {pre-master-secret}_{K_{pub-amazon}}
-

X509 certificate

- ```
struct X509_certificate {
 unsigned version;
 unsigned serial;
 signature_cipher_identifier;
 issuer_signature;
 issuer_name;
 subject_name;
 subject_public_key_cipher_identifier;
 subject_public_key;
 validity_period;
};
```

QuickTime™ and a  
TIFF (Uncompressed) decompressor  
are needed to see this picture.

QuickTime™ and a  
TIFF (Uncompressed) decompressor  
are needed to see this picture.