# Computer security: authentication of principals and cryptographic protocols

6.033 Spring 2007

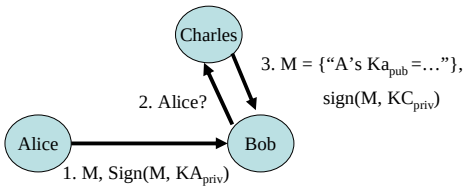
## HKN Underground Guide

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

Link posted on 6.033 home page

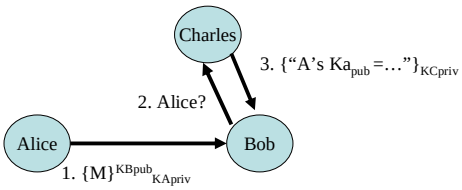
Deadline: May 20

## key distribution



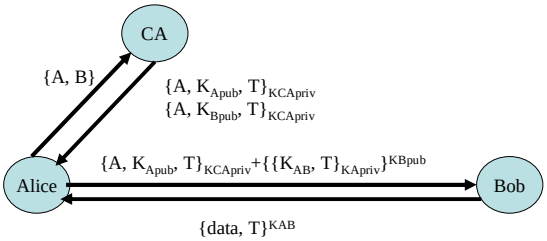

- 3 is a *certificate* for Alice's public key
- Charles is called a *certificate authority*
- The interaction is an example of a *cryptographic protocol*

## Shorter notation



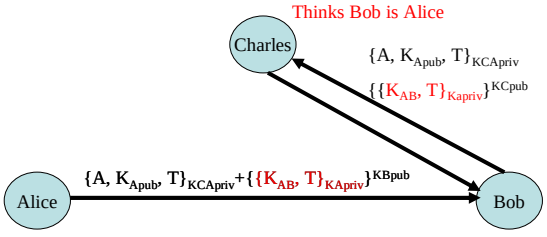

- Subscript for signing
- Superscript for encrypting

## Denning-Sacco

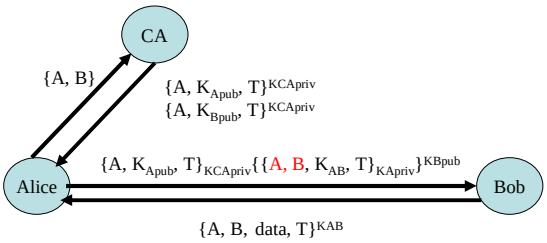



1. Authenticate Alice to Bob and Bob to Alice
2. Set up a shared-secret key

## Impersonation Attack



## Denning-Sacco (fixed)




Be explicit!

## Example: Web (SSL simplified)

- U: https://www.amazon.com
- B →W: {random$_c$, session-id, ciphersuites}
- B ← W: {random$_s$, session-id, {amazon.com, $K_{pub\text{-}amazon}$}$_{Kversign}$}
- B: verify({amazon.com, $K_{pub\text{-}amazon}$}$_{Kversign}$, $K_{pub\text{-}verisign}$)?
- B →W: {pre-master-secret}$^{Kpub\text{-}amazon}$
- .....

## 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;
  };