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*

1. $M, \text{Sign}(M, KA_{\text{priv}})$
2. Alice?
3. $M = \{”A’s \text{ Ka}_{\text{pub}} = …”\}$,
   $\text{sign}(M, KC_{\text{priv}})$
Shorter notation

• Subscript for signing
• Superscript for encrypting

1. \( \{M\}_\text{KBpub}_{\text{KApriv}} \)

2. Alice?

3. \( \{“A’s \text{ Ka}_{\text{pub}} =…”\}_\text{KCpriv} \)

Alice → Bob → Charles

Diagram:

- Charles
- Alice
- Bob
- Arrows indicate communication flow.

- 1. Bob encrypts message \( M \) with Alice's public key and sends it to Charles.
- 2. Alice queries Charles about the encrypted message.
- 3. Charles decrypts the message using Alice's private key and sends the decrypted message back to Alice.
1. Authenticate Alice to Bob and Bob to Alice
2. Set up a shared-secret key
Impersonation Attack

Bob sends Alice a message: 

\[ \{A, K_{A_{pub}}, T\}_{K_{CA_{priv}}} + \{\{K_{AB}, T\}_{K_{A_{priv}}}\}_{K_{C_{pub}}} \]
Denning-Sacco (fixed)

Be explicit!
Web (SSL simplified)

- **U**: [https://www.amazon.com](https://www.amazon.com)
- **B → W**: \{random_c, session-id, ciphersuites\}
- **B ← W**: \{random_s, session-id, \{amazon.com, K_{pub-amazon}\}_{Kversign}\}
- **B**: verify(\{amazon.com, K_{pub-amazon}\}_{Kversign}, K_{pub-verisign})?
- **B → W**: \{pre-master-secret\}_{K_{pub-amazon}}
- ......