Authentication, Key Exchange, and Certificates

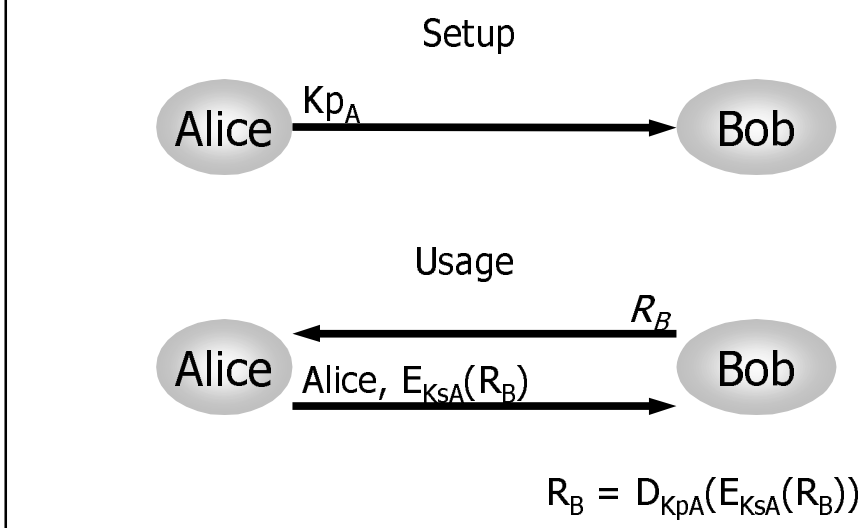
csci 7000-001 f01-07

Antonio Carzaniga

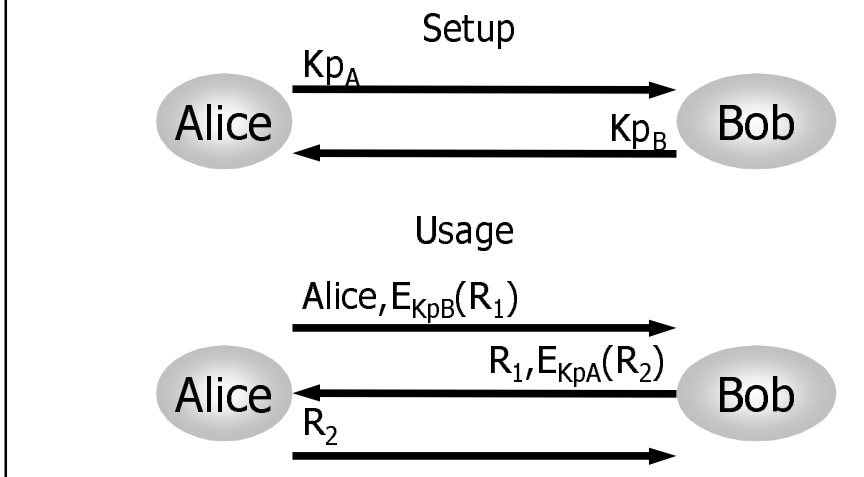
Outline

- Public-key authentication
- Message authentication
- Key exchange
- Key exchange and authentication
- Certificates

Public-key Authentication



Mutual Public-key Authentication



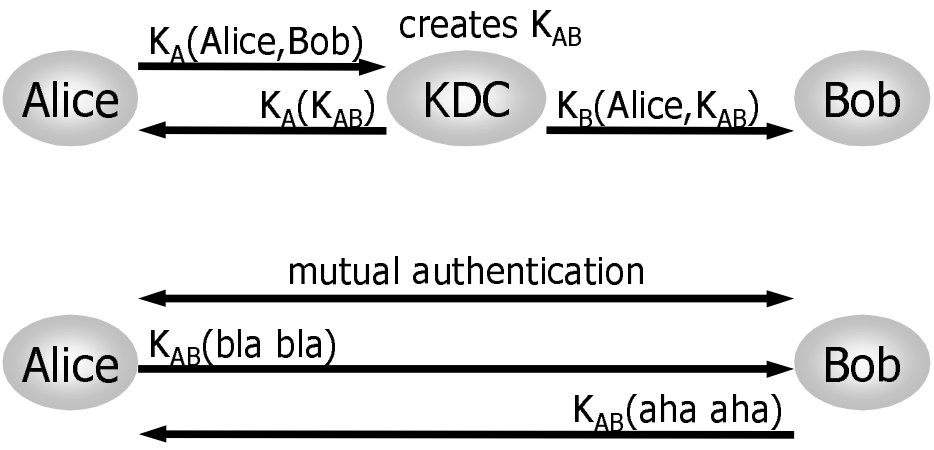
Mediated Authentication

- Key distribution center (KDC)
  - shares secret key with every node

+ single trusted node
+ only KDC needs to know about new/old nodes
+ N nodes: N^2 vs. N

– single point of failure
– single point of attack
– performance bottleneck

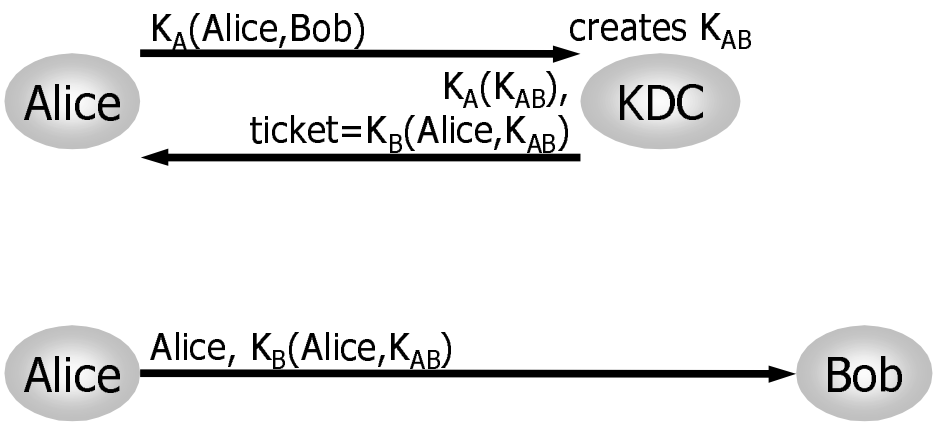
Simple Authentication with KDC



Simple Authentication with KDC

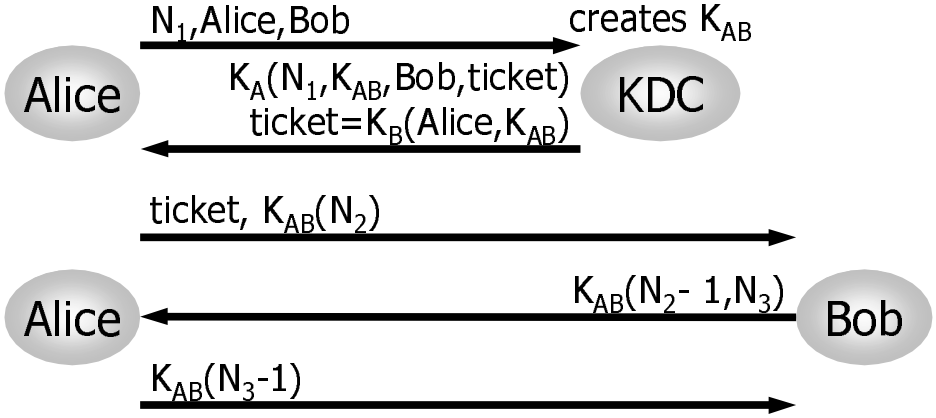
- Practical problems
  - network latency: Bob may receive $K_B(Alice,K_{AB})$ only after Alice starts authenticating herself or sending messages
  - KDC must initiate a communication with Bob

Tickets



Needham-Schroeder

- Tickets+mutual authentication



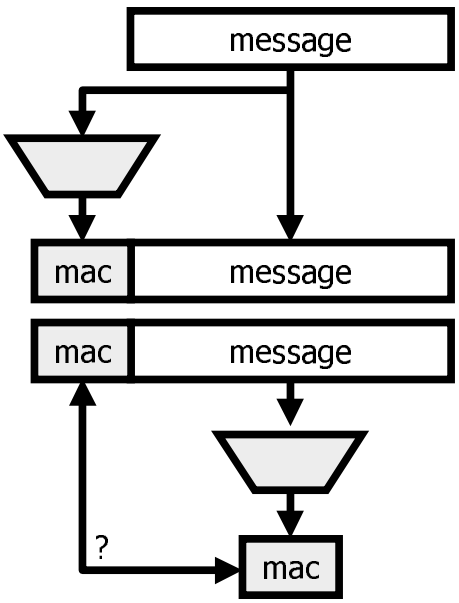
Message Authentication

- Plaintext authentication
- Message authentication code (MAC)
  - conventional cryptography
  - public-key cryptography
  - one-way hash

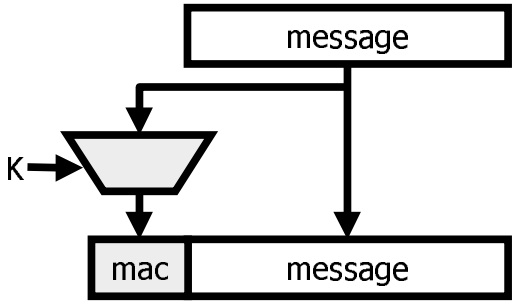
Why Plaintext Authentication?

- Broadcast channels
  - all listeners would have to share encryption key
  - instead, only one receiver could be responsible for verifying authenticity
- Encryption does have a cost
  - a party may verify authenticity of a few randomly chosen packets
- Verification only when needed

MAC

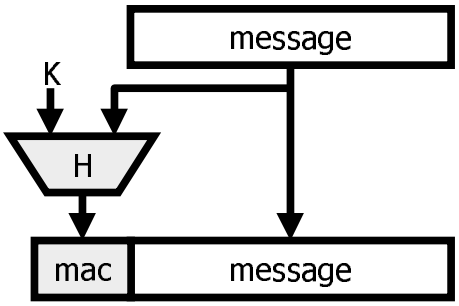


Secret-key MAC



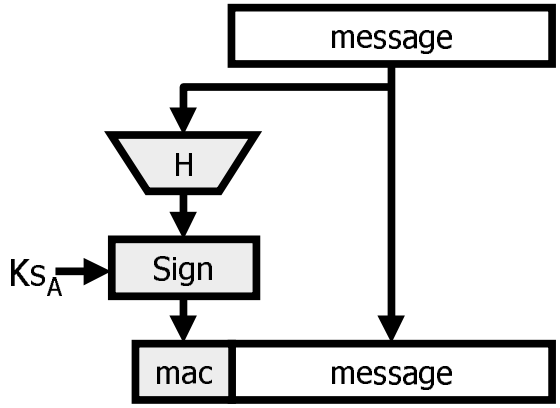
- E.g., perform CBC and use the last block as a MAC

One-Way Hash MAC



- MAC=H(message+K)

Public-key MAC

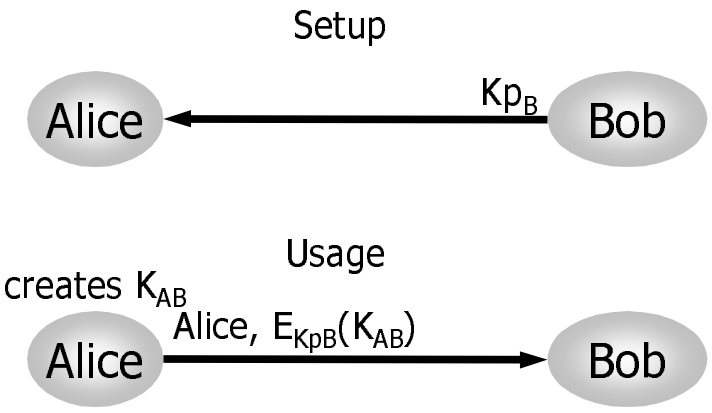


- MAC=S(H(m))

(Encrypted) Key Exchange

- With KDC
  - with authentication
- Public-key
  - with authentication
- Diffie-Hellman
  - no authentication

Simple Public-Key EKE



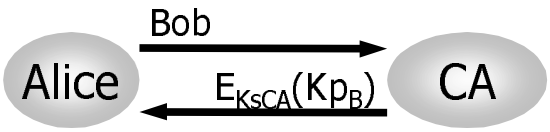
Simple Public-Key EKE

- Vulnerable to man-in-the-middle attack

Certificates

- Trusted certification authority
- Certificate=signed public key

$C_B = E_{KsCA}(Kp_B)$



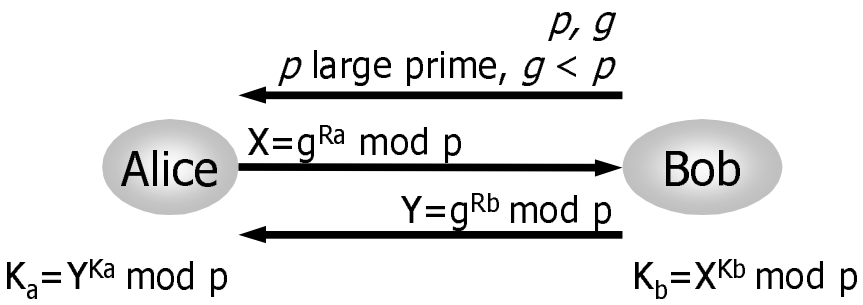
Certificates

- Certification authority
  - has well-known public key
  - signs other party's public-key

+ doesn't need to be on-line, can be easily secured
+ doesn't participate in protocols
+ certificates are not security-sensitive
+ compromised CA doesn't affect previous (or even future conversations

– revocation of certificates

Key-Exchange: Diffie-Hellman



- $K_{session}=K_a=K_b=g^{Ra \cdot Rb} \bmod p$
- Attacker can't compute K from X and Y without computing discrete logs
- No authentication!

Formal Analysis of Protocols

- Traditional software verification
- Expert system
- Logic of beliefs and knowledge
- Algebraic methods