Protocols and Authentication

Protocols

- Every party knows every step of the protocol in advance
- Every party must agree to follow the protocol
- A protocol must be unambiguous
- A protocol must be complete

Classes of Protocols

- Arbitrated
- Adjudicated
- Self-enforcing

Classes of Attacks

- Passive attacks
  - attacker does not take part in the protocol
  - attacker can only observe
- Active attacks
- Cheaters: attacker is a legitimate player
  - passive
  - active

Cryptographic Protocols

- Authentication
- Key exchange
- Authentication and key exchange
- Secret splitting and sharing
- Undeniable digital signatures
- Certification
- Subliminal channel
- Proxy signature
- Group signature

More Cryptographic Protocols

- Computing on encrypted data
- Prediction commitment
- Fair coin flip
- Mental poker
- Key escrow
- Zero-knowledge proof
- Simultaneous contract signing
- Digital certified mail
- Simultaneous exchange of secrets

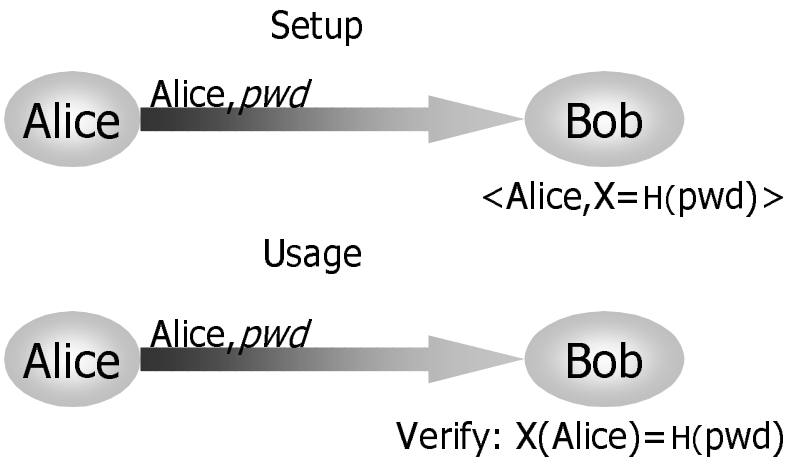
Esoteric Protocols

- Secure elections
- Secure multiparty computations
- Anonymous message broadcast
- Digital cash (or anonymous digital cash)

Authentication

- It's not who you are
- It's what you know
  - it's what you can compute
  - it's how you can respond to a challenge

Plaintext Authentication



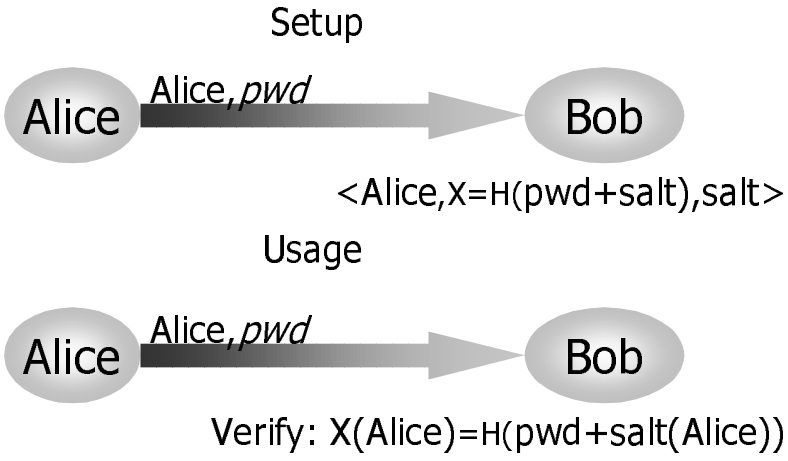
Plaintext Authentication

- Setup:
  - Alice stores *pwd*
  - Bob stores *<Alice, X=H(pwd)>*
- Usage:
  - Alice sends: *{Alice, pwd}*
  - Bob verifies: *H(pwd)=X(Alice)*

Plaintext Authentication

- Eavesdropping
- Dictionary attack
- Brute force attack

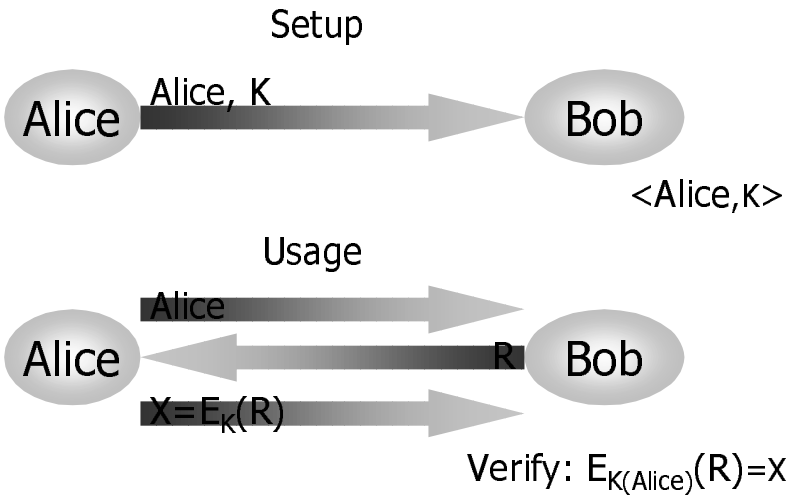
Defeat Dictionary Attack with Salt



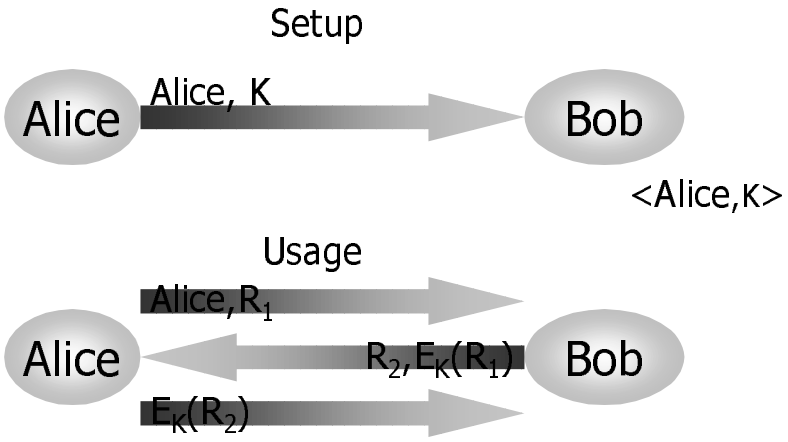
How to Defeat Eavesdropping?

- Alice and Bob share a secret K_{AB}
- Alice must be able to convince Bob that she knows K_{AB} without sending K_{AB} to Bob
- Alice might use K_{AB} to encrypt a random challenge presented by Bob
- Alice might authenticate Bob the same way

Symmetric-cipher Authentication



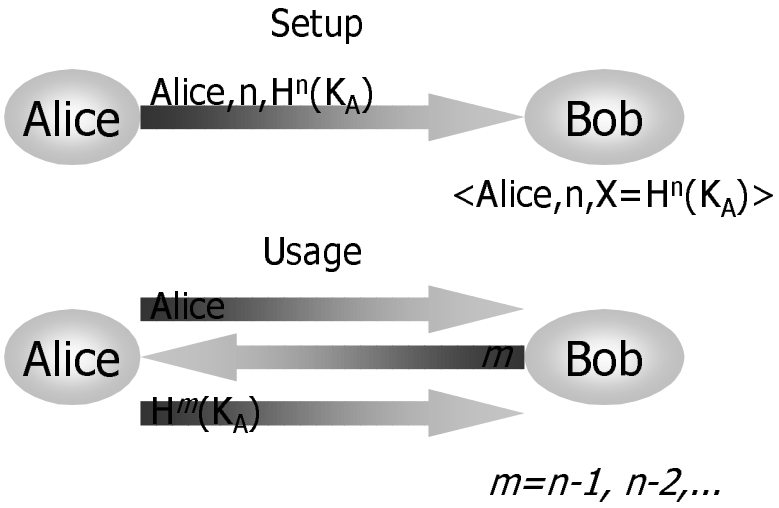
Symmetric-cipher Authentication



Symmetric-cipher Authentication

- Reflection attack
- Chosen plaintext attack
  - off-line password guessing

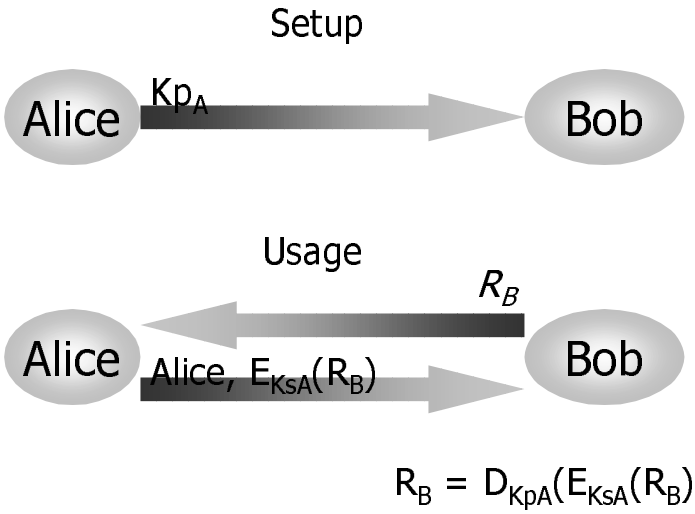
Hash-based Authentication (SKey)



Analysis of SKey

- Man-in-the-middle
- Periodic setup

Public-key Authentication

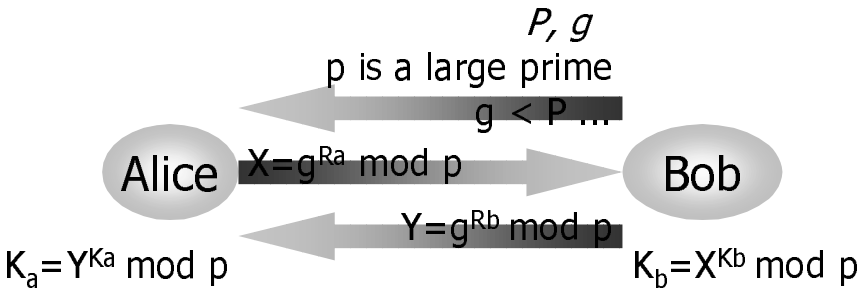


$R_B = D_{KpA}(E_{KsA}(R_B))$

Integrity and Confidentiality

- Alice and Bob encrypt their communications
- What encryption key?
- Shared secret
  - same key: massive ciphertext attack
- Byproduct of authentication: e.g., R_1 and R_2
  - attacker can spoof Bob in the future and uncover previous conversations

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

Formal Analysis of Protocols

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