CSE 5306
Distributed Systems

Security

Jia Rao

http://ranger.uta.edu/~jrao/

Security Threats

- Interception
  - Access by unauthorized users
- Interruption
  - Service or data becomes unavailable
- Modification
  - Unauthorized tampering of data or service
- Fabrication
  - Additional data or info is fabricated

Security Objectives

- Confidentiality
  - ✓ Prevent/detect/deter improper disclosure of information
- Integrity
  - ✓ Prevent/detect/deter improper modification of information
- Availability
  - ✓ Prevent/detect/deter improper denial of services offered by the system
- Other goals
  - ✓ Accountability, non-repudiation, anonymity

Security Mechanisms

- Implement functions that help prevent, detect, and respond to security attacks
  - ✓ Three layers of defense
    - Prevention, detection, and tolerance
- Some basic mechanisms
  - ✓ Encryption, authentication, authorization, auditing

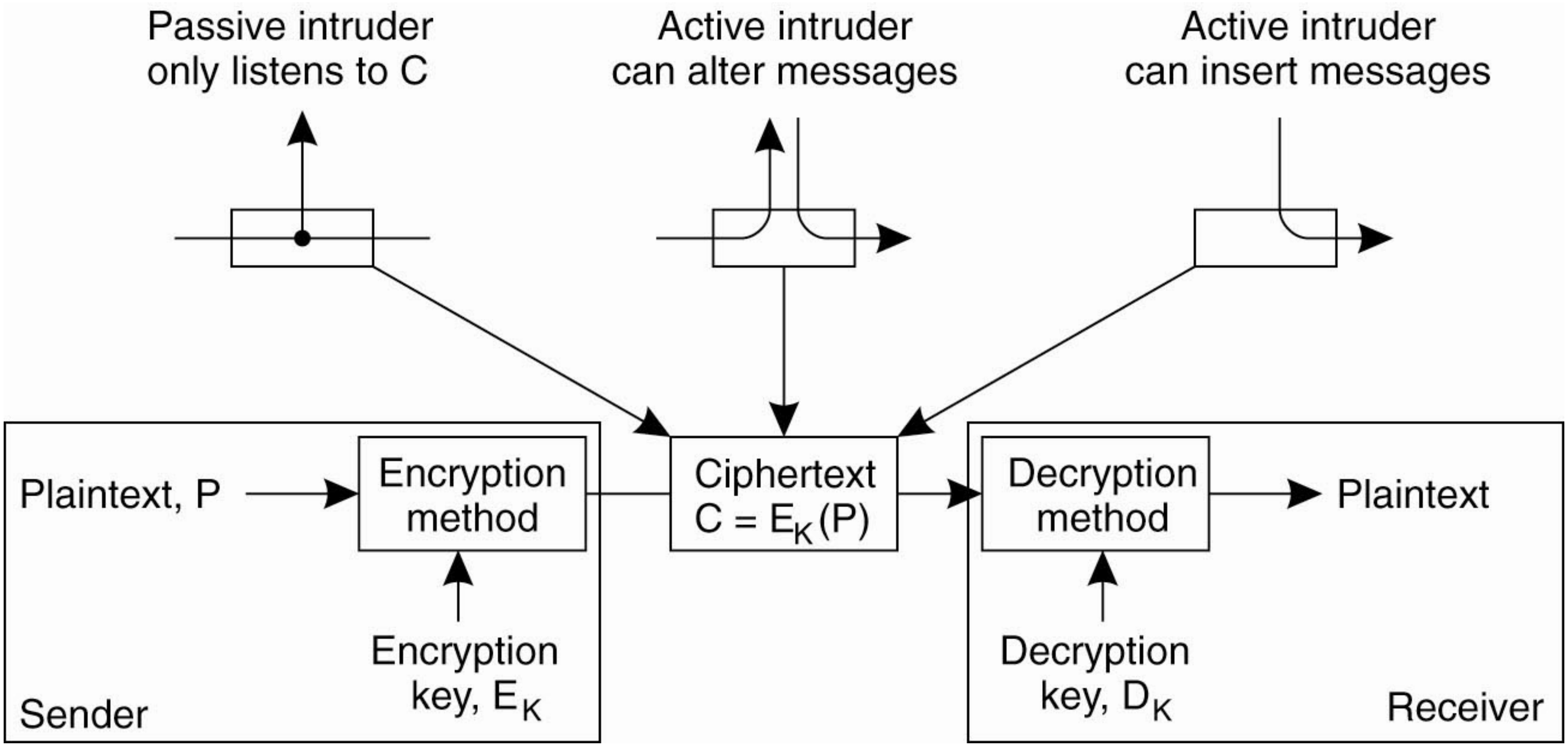
Cryptography and Security

- Cryptography
  - ✓ Study of fundamental algorithms such as encryption/decryption, hash, and digital signatures, to protect data
- Security
  - ✓ Study of protocols to protect a system
  - ✓ Often build upon cryptographic techniques

Cryptography

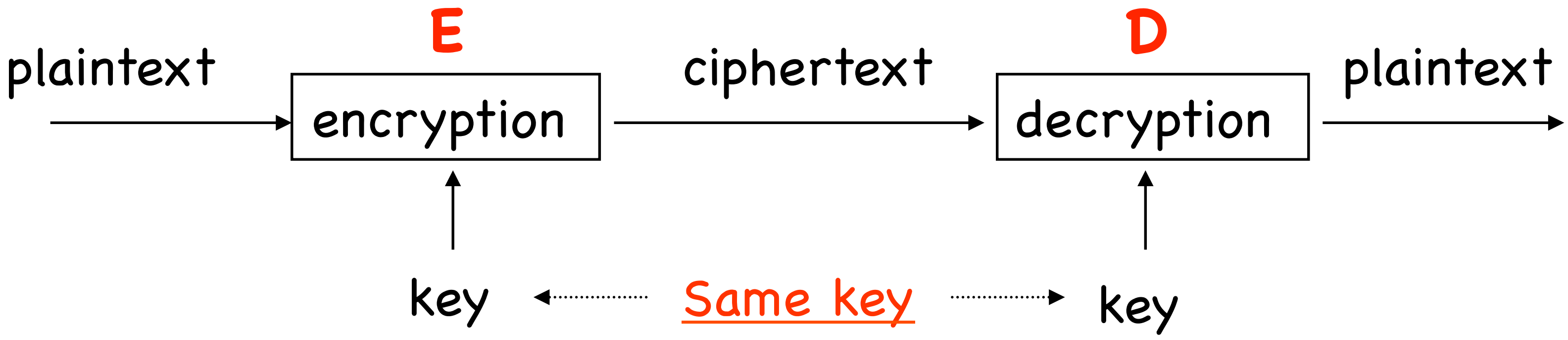
- Convert data into unintelligible form
- Types:
  - ✓ Secret key (symmetric) cryptography
    - A secret key is involved in the converting process
    - Reversible only when the secret key is known
  - ✓ Public key (asymmetric) cryptography
    - Two keys – public and private
  - ✓ Hash functions: no key

Communication and Attack Model



Intruders and eavesdroppers in communication.

Symmetric Cryptography

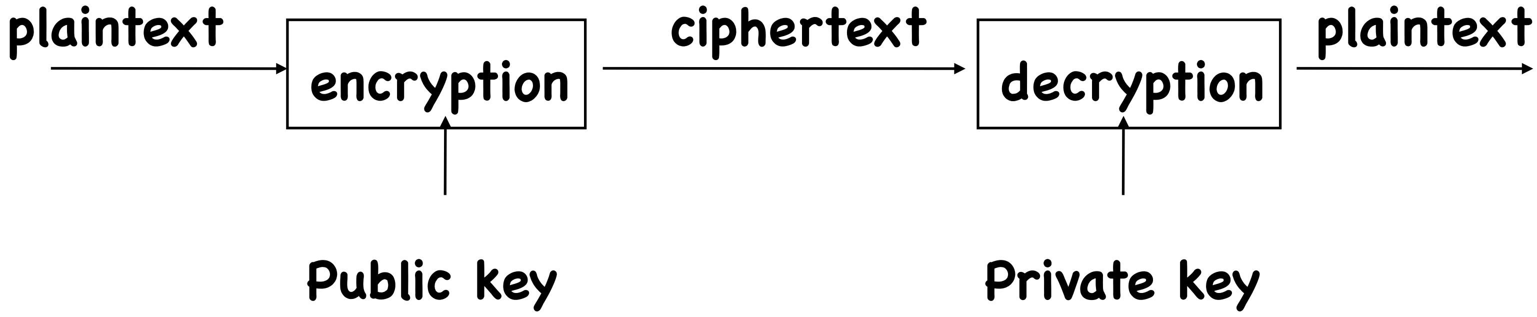


- Same key is used for encryption and decryption
- Ciphertext approximately the same length as plaintext
- Examples:
  - ✓ RC4, DES, IDEA, AES

Two-party Communication Problem

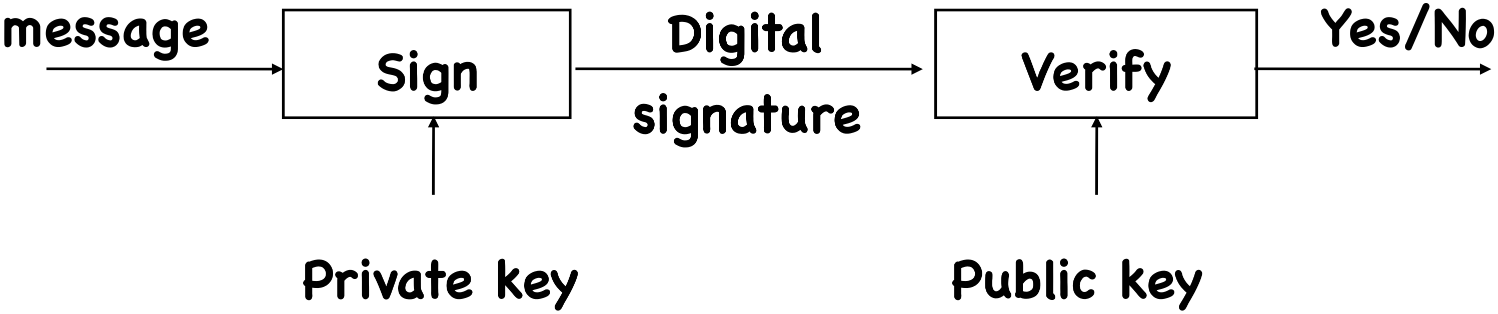
- Problem:
  - ✓ Alice (A) and Bob (B) want to securely communicate with each other
- Solution:
  - ✓ Establish a shared key (K)
  - ✓ Encrypt message (M) with the shared key
    - A→B: $E_k(M)$
  - ✓ Problem: no guarantee of integrity

Asymmetric Cryptography



- A public/private key pair is used
  - ✓ Public key can be publicly known
  - ✓ Private key is kept secret by the owner of the key
- Much slower than secret key cryptography
- Avoid the exchange of secret key between communicating parties

Digital Signature



- Sign
  - ✓ Only the one with the private key can sign a message (i.e., create a digital signature)
- Verify
  - ✓ Anyone who has the public key can verify a digital signature
- The signer cannot deny that he/she has done so

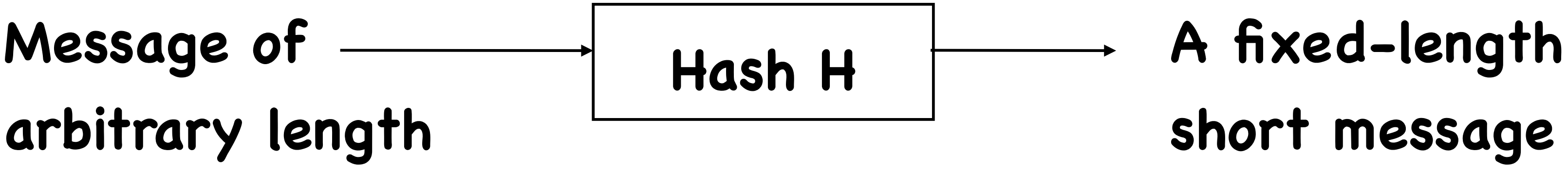
Applications of Asymmetric Cryptography (1/2)

- Secure data transmission
  - ✓ Alice encrypts m using Bob’s public key and Bob decrypts m using his private key
- Secure storage in public media
  - ✓ Can create a safety copy: using public key of trusted person
- Authentication
  - ✓ No need to store secrets, only need public keys
  - ✓ Secret key cryptography: need to share secret key for every person to communicate with

Applications of Asymmetric Cryptography (2/2)

- Digital signatures
  - ✓ Sign message M with the private key
- Key exchange
  - ✓ Establish a common session key between two parties

Hash Functions



Message of arbitrary length

Hash H

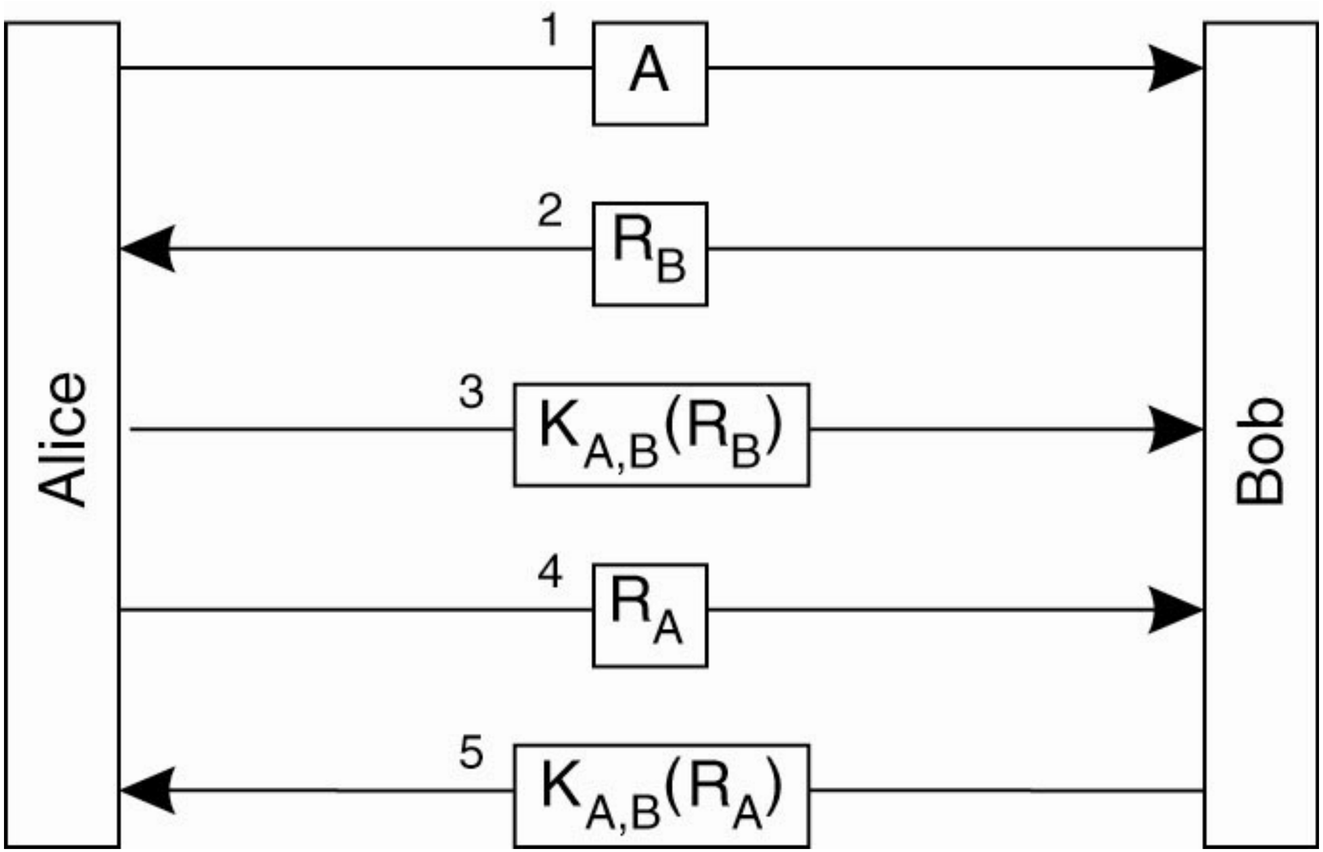
A fixed-length short message

- Length of H(m) is much shorter than the length of the original message m
  - ✓ Usually fixed lengths: 128 or 160 bits
- Also known as
  - ✓ Message digests
  - ✓ One-way transformations
  - ✓ One-way functions

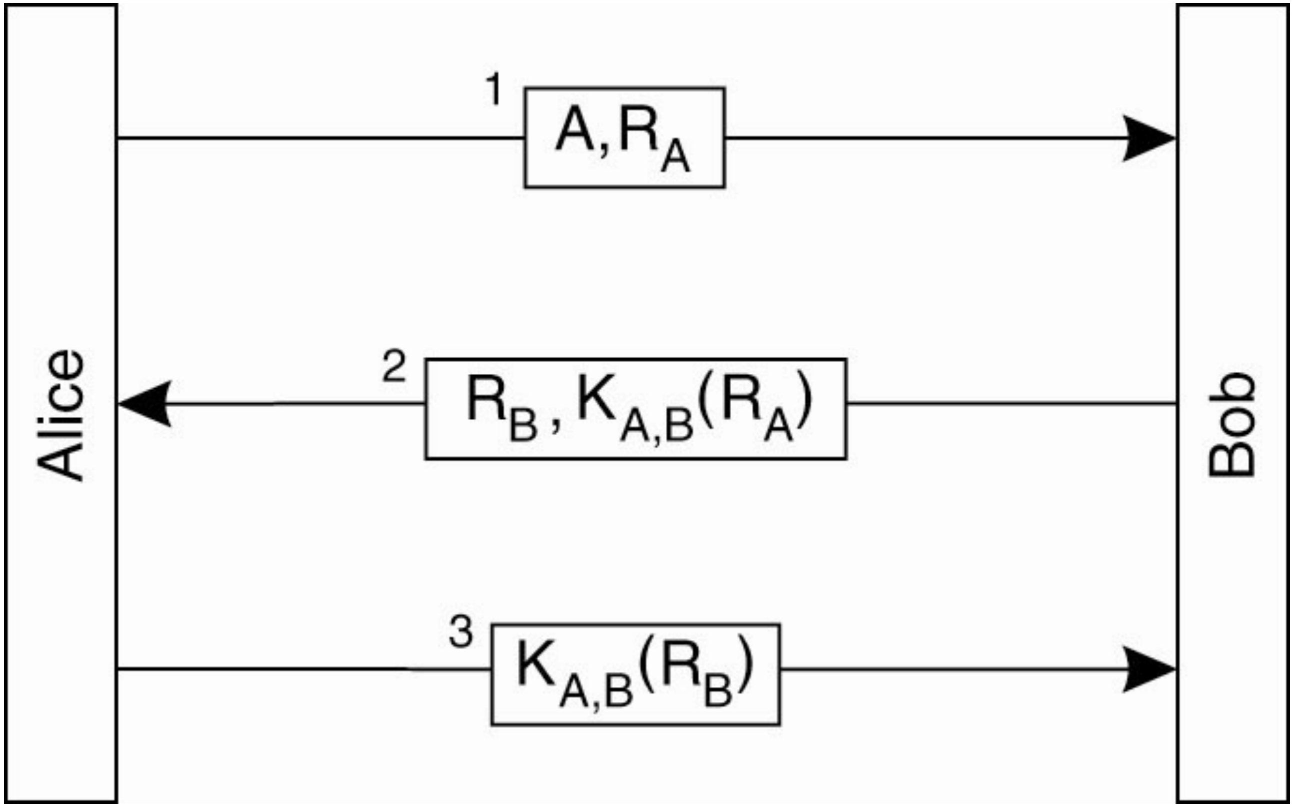
Properties of Hash Functions

- Flexibility
  - ✓ Can be applied to a block of data of any size
- Convenience
  - ✓ Produce a fixed-length short output
- Performance: easy to compute
- One-way property:
  - ✓ Given H(m) but not m, it is difficult to find m
- Weak collision free:
  - ✓ Given H(m), it is difficult to find m’ such that H(m’) = H(m)
- Strong collision free:
  - ✓ It is difficult to find m_1, m_2 such that $H(m_1) = H(m_2)$

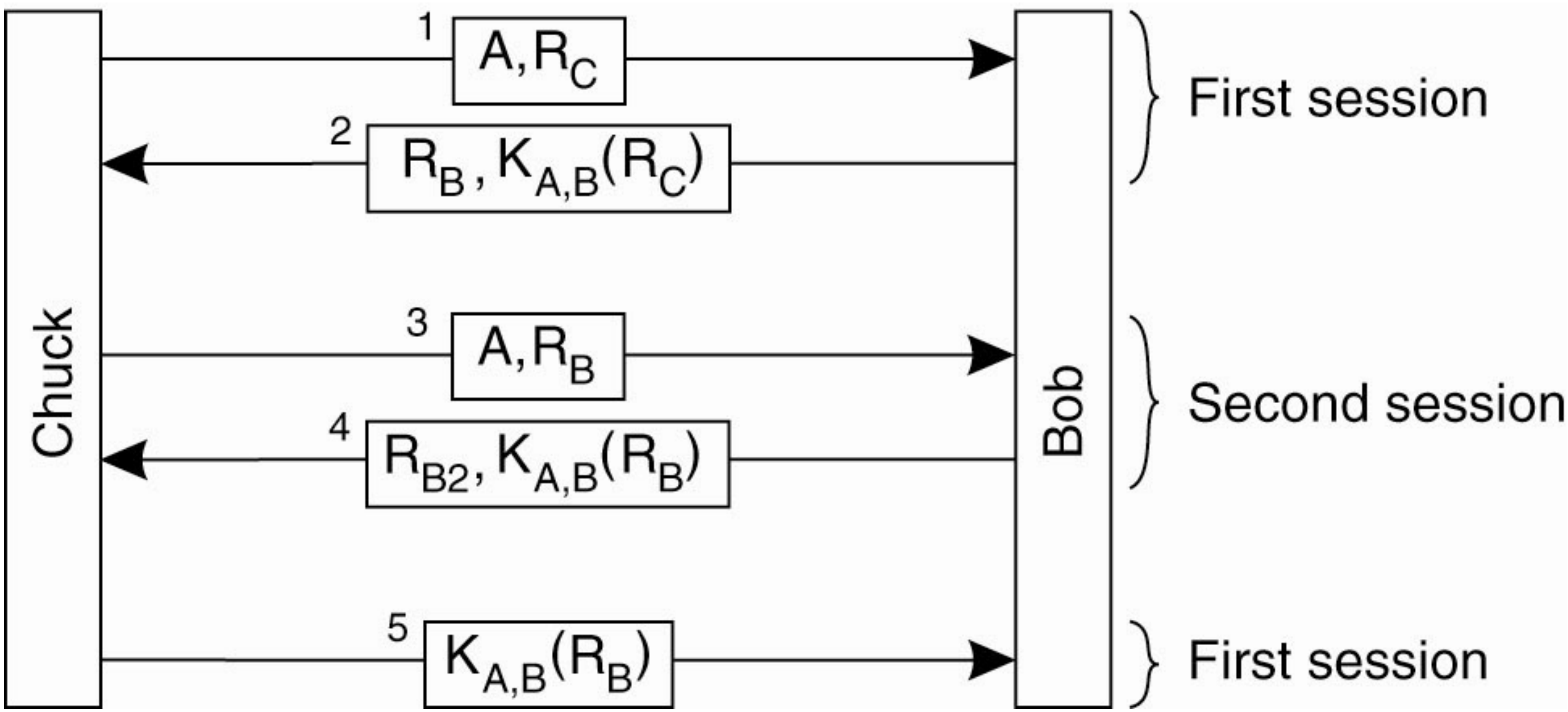
Authentication Based on a Shared Secret Key



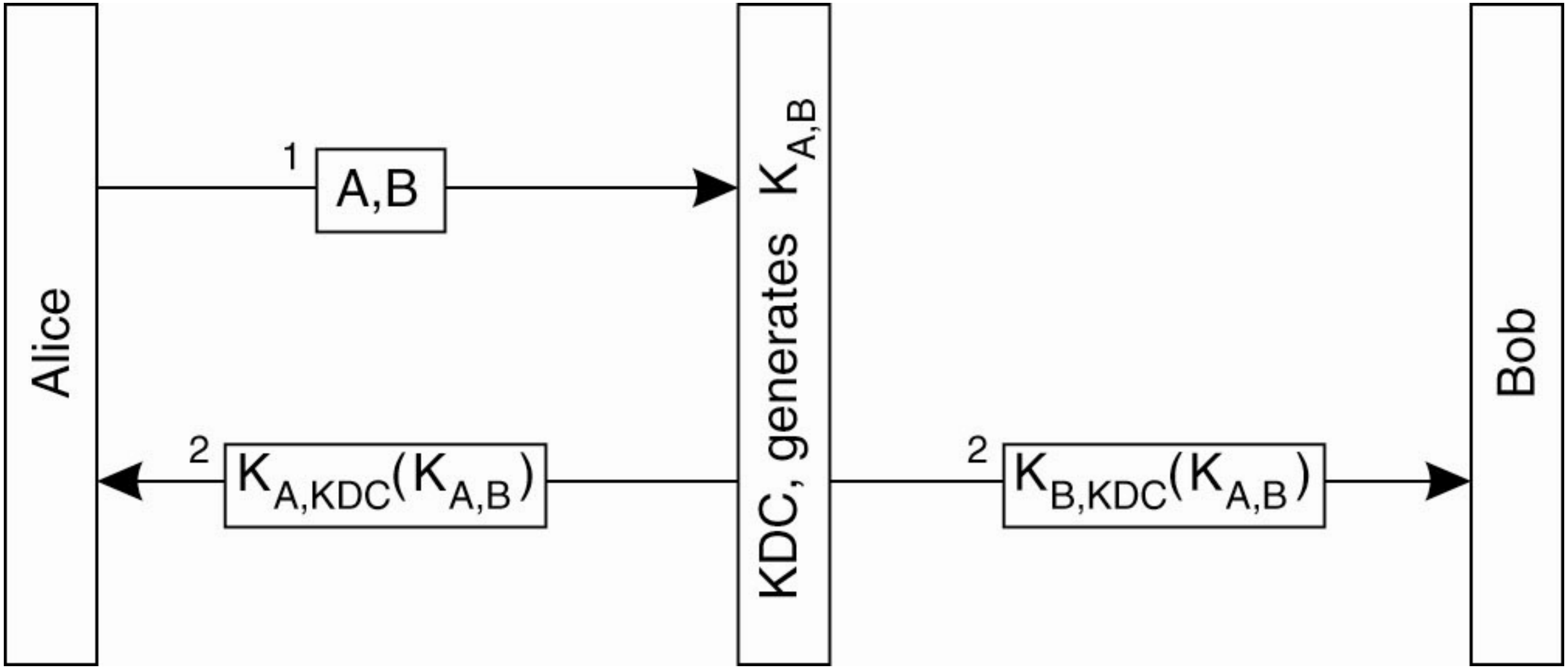
A Simplified but Unsecure Protocol



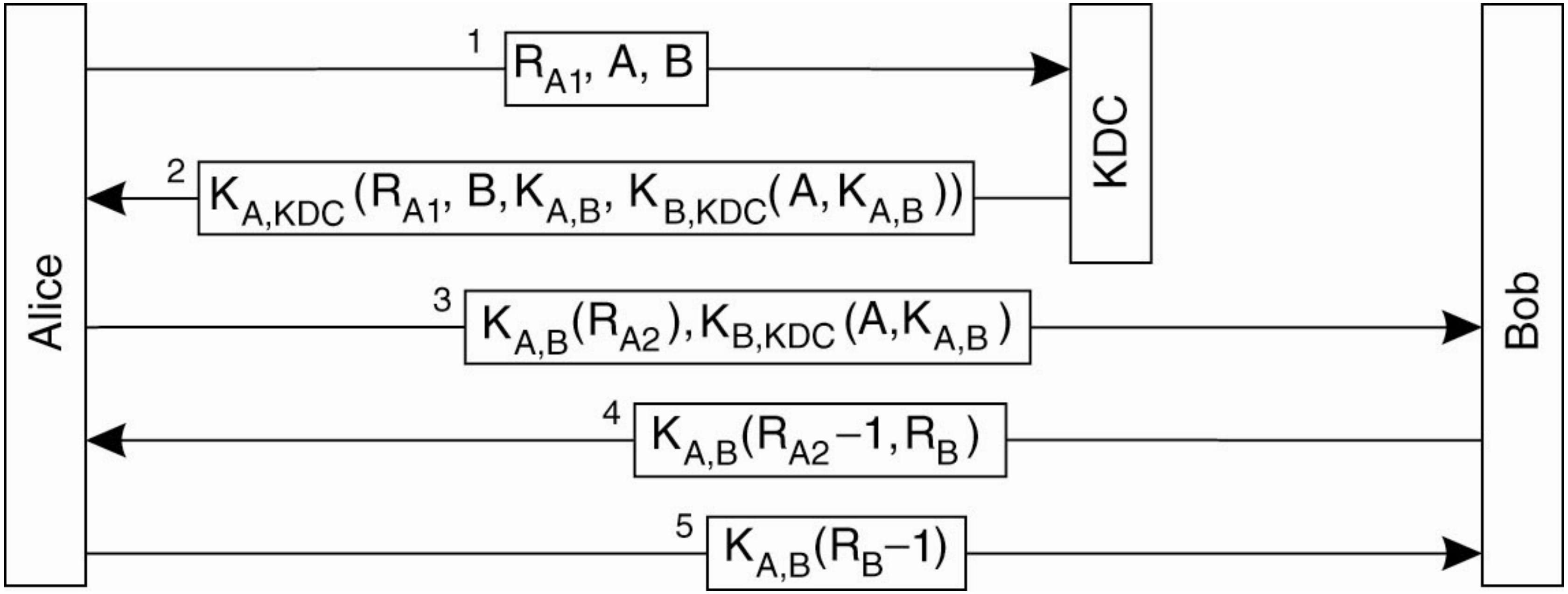
The Reflection Attack



Key Distribution Center



The Needham-Schroeder authentication protocol.



Alice

KDC

Bob

1 R_{A1}, A, B

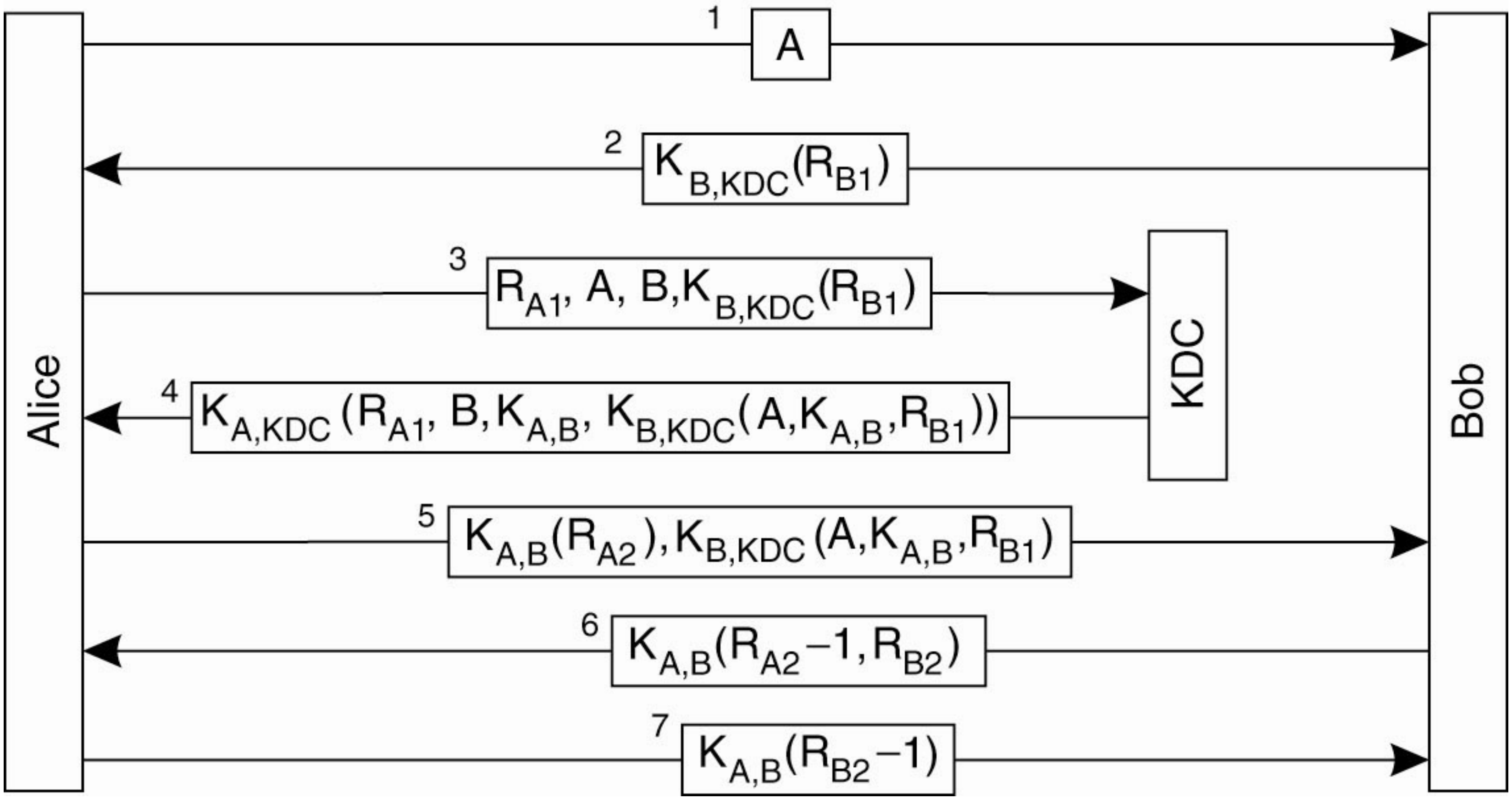
2 $K_{A,KDC}(R_{A1}, B, K_{A,B}, K_{B,KDC}(A, K_{A,B}))$

3 $K_{A,B}(R_{A2}), K_{B,KDC}(A, K_{A,B})$

4 $K_{A,B}(R_{A2}-1, R_B)$

5 $K_{A,B}(R_B-1)$

An Improved NS Protocol



Alice

KDC

Bob

1 A

2 $K_{B,KDC}(R_{B1})$

3 $R_{A1}, A, B, K_{B,KDC}(R_{B1})$

4 $K_{A,KDC}(R_{A1}, B, K_{A,B}, K_{B,KDC}(A, K_{A,B}, R_{B1}))$

5 $K_{A,B}(R_{A2}), K_{B,KDC}(A, K_{A,B}, R_{B1})$

6 $K_{A,B}(R_{A2}-1, R_{B2})$

7 $K_{A,B}(R_{B2}-1)$