Cryptographic Protocols: Making the Network Secured

Debdeep Mukhopadhyay
IIT Kharagpur

Protocols

- **Key Agreement**
- Authentication: Group Authentication
- Key Agreement and Authentication
- Key Agreement and authentication with key confirmation.
- Secret Sharing Schemes
- Zero Knowledge Protocols

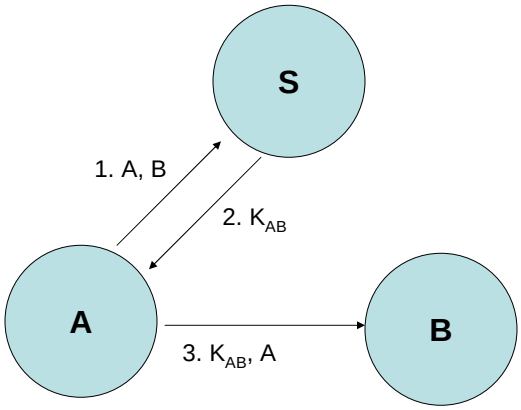
Keys in a Protocol

- **Long Term Keys:** Generated by a more costly process, like D-H. Stored in protected places (tamper-proof). Used to generate the session key, which is also known as the ephemeral or short-lived key.
- **Session-Key:** Changed per session. Used in future encryptions. So, they are more prone to cryptanalysis and attacks. Thus, they must be changed on a more regular basis.

Establishing the session Key

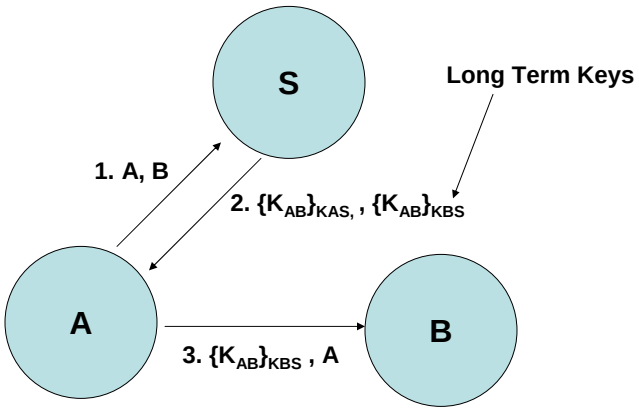
- Set Up:
  - Three legitimate entities
    - Alice (A)
    - Bob (B)
    - Trusted Server (S)
- Purpose: Establish new session key K_{AB}
- **Objectives of the Key Establishment Protocol:**
  - At the end K_{AB} should be known to only A, B and of course S
  - A and B should know that K_{AB} is newly generated

First Attempt



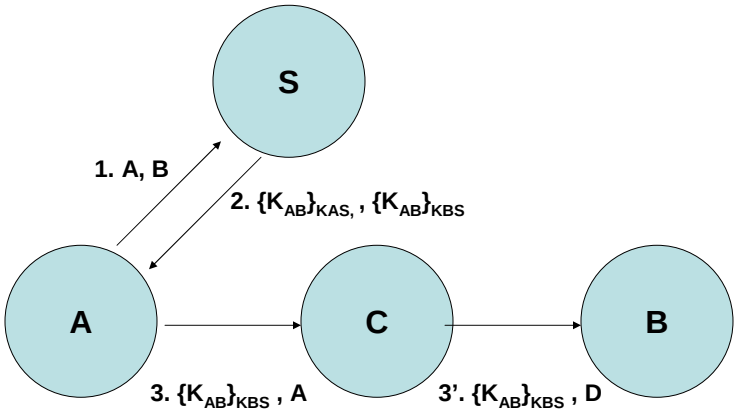
Security Assumption 1: *The adversary is able to eavesdrop on all messages*

Second Attempt



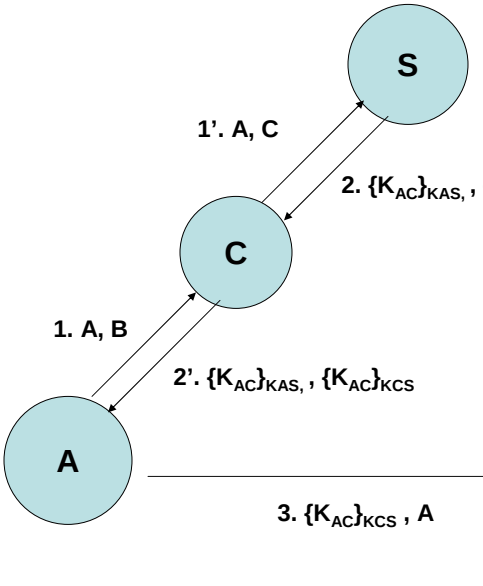
Security Assumption 2: *Attacker is able to alter messages using any information available, reroute messages, generate and insert completely new message*

Attack on Protocol-2



B thinks he is sharing with D, while he is actually doing it with A. So, B may leak some information meant only for D to A! So, we have the condition that all users should know with whom they are sharing keys.

Another Attack on Protocol-2



Security Assumption 3:

Insiders can be attackers or combine with outsiders to pose attacks

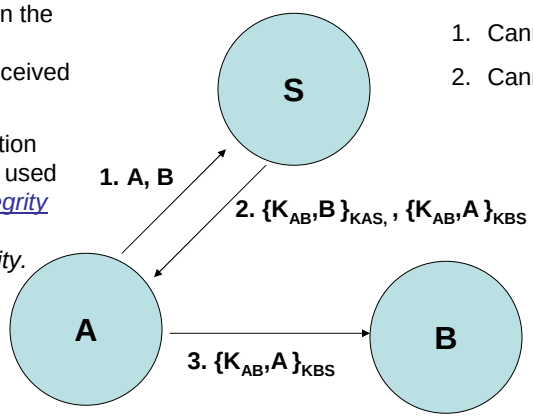
A thinks he is communicating with B, while he is actually communicating with C. C knows K_{AC}, and thus can masquerade as B to A, and obtain all information which A sends for B.

Third Protocol Attempt

Include the names of A and B in the encrypted message received from S.

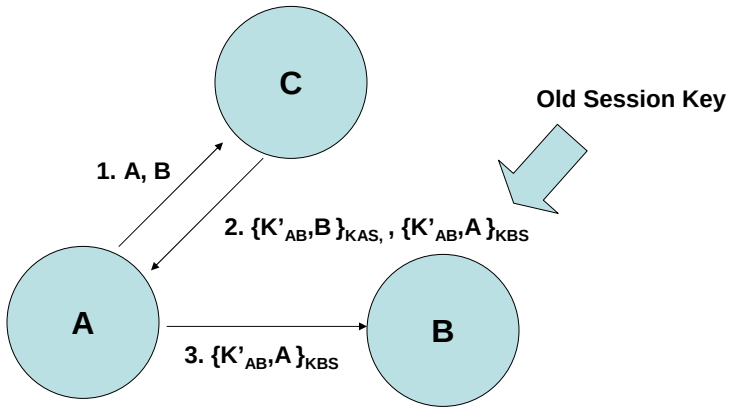
The Encryption algorithm is used for *data integrity* and not for *confidentiality*.

1. Cannot Eavesdrop
2. Cannot Alter message



Security Assumption 4: *Attacker is able to obtain any previous session key*

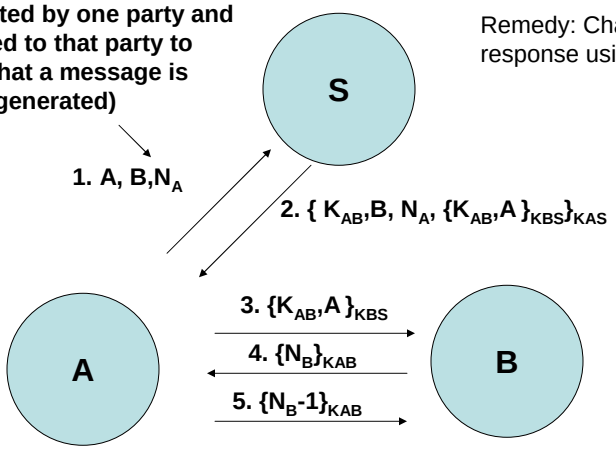
Attack on Protocol 3
---- replay attack



Fourth Protocol Attempt

Nonce (random value generated by one party and returned to that party to show that a message is newly generated)

Remedy: Challenge-response using Nonces.



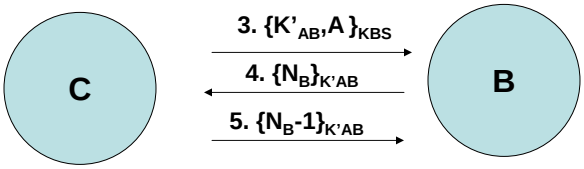
Essentially known as Needham and Schroeder's Protocol

Attack on Protocol-4

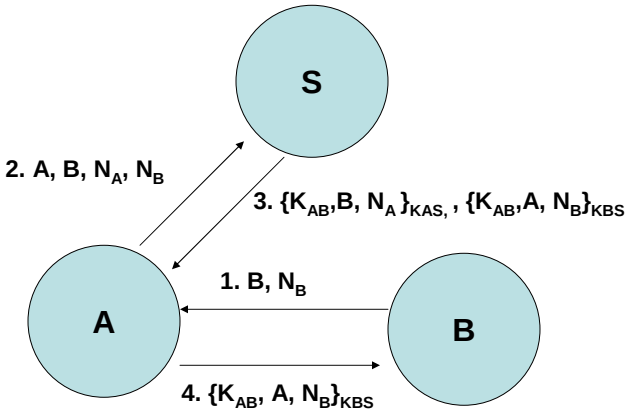
Assumption of Previous Protocol:

--- Only A can correctly answer 4th challenge of B

---- But C may know an old key K'$_{AB}$



Fifth Protocol Attempt



Protocol Architectures

- It is not possible to establish an authenticated session key without existing secure channels already being available.
- Off-line servers: Certified public keys are available to the principals.
- On-line servers: Each principal shares a key with a trusted server.

Methods of session key generation

- **Key Transport:** one principal generates the key, which is transferred to the others.
- **Key Agreement:** session key is a function of inputs by all parties.
- **Hybrid Protocols** also exist, which are key transport to a party, but agreement to the other.

Number of Users

- Two party
- Multi-party (conference key protocols) complicate the matter a great deal.

Hybrid Protocol

- $A \rightarrow B$: A, N_A
- $B \rightarrow S$: $\{N_B,A,B\}_{KBS},N_A$
- $S \rightarrow A$: $\{K_{AB},A,B,N_A\}_{KAS},N_S$
- $A \rightarrow B$: $N_S,\{A,B\}_{KAB}$
- $B \rightarrow A$: $\{B,A\}_{KAB}$

Observe that B is not being given K_{AB} explicitly. He can compute using a function f, $K_{AB}=f(N_B,N_S)$.

To B this is an example of agreement, while for A it is a key transport.