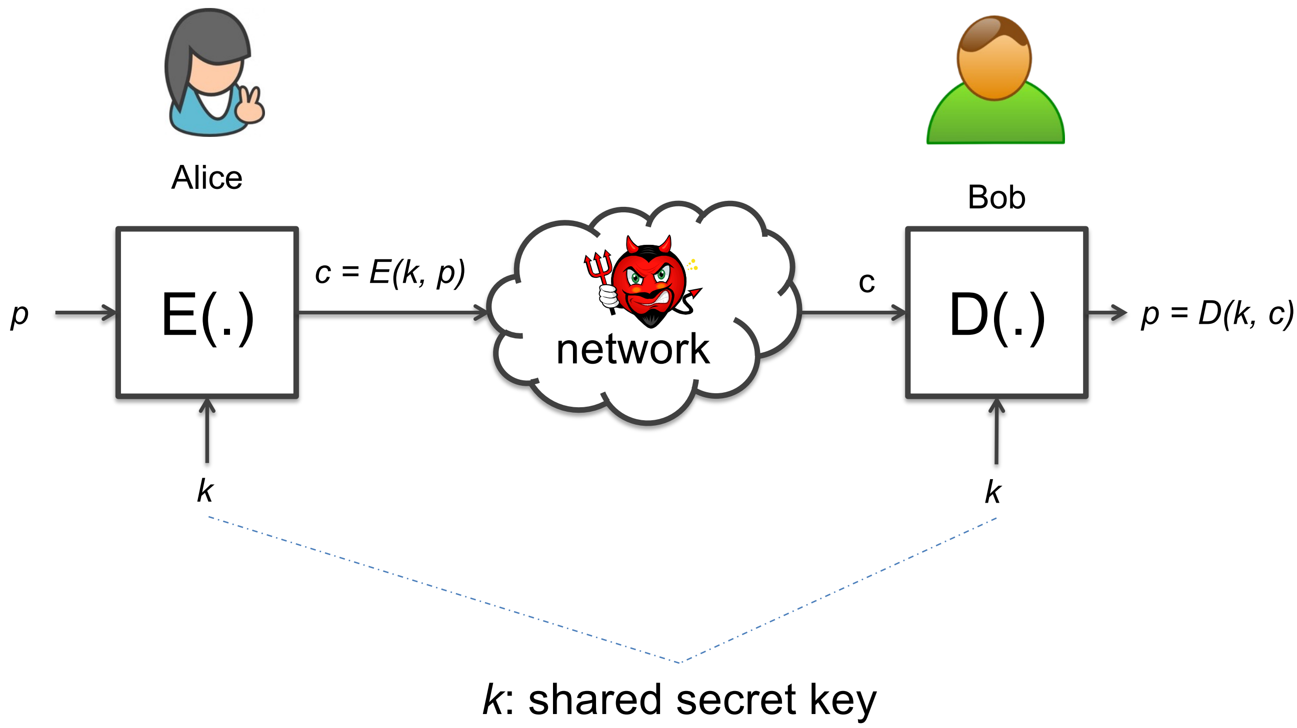
Key Establishment

Gianluca Dini
Dept. of Ingegneria dell'Informazione
University of Pisa
Email: gianluca.dini@.unipi.it
Version: 2024-04-22

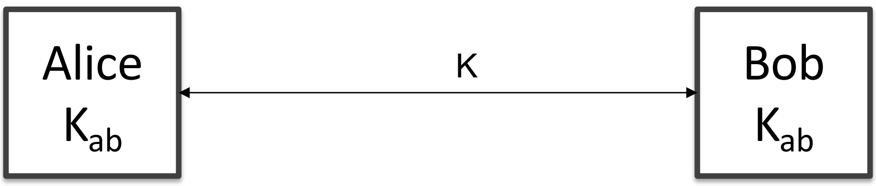
Key Establishment

INTRODUCTION

On establishing a secret shared key



Session key [→]



- K_{ab} is a long-term secret shared key
- K is temporary session (ephemeral) key

Session key

- Key freshness
  - Use a key for a limited amount of time and then update it
  - Session key or ephemeral key
- Advantages
  - Less damage if a key is exposed
  - Less cyphertext available for analytical attacks
  - An adversary must recover several keys if (s)he is interested in decrypting larger parts of plaintext

Session key transport and agreement

- **One-pass Key transport**
  - M1 A → B: $E(K_{ab}, K||t_a)$
    - where t_a is a timestamp
    - Requires clock synchronization
- **Key transport with challenge-response**
  - M1 B → A: n_b
  - M2 A → B: $E(K_{ab}, K||n_b)$
    - where n_b is a nonce, i.e., a fresh quantity never used before

Session key

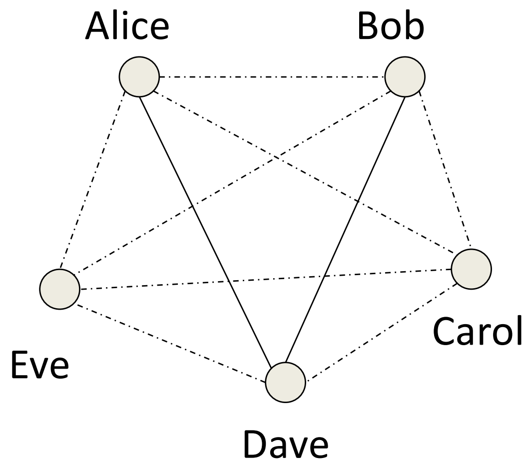
- **Key agreement**
  - M1 B → A: n_b
  - M2 A → B: $E(K_{ab}, K'||n_a||n_b)$
  - M3 B → A: $E(K_{ab}, K''||n_a)$
    - Where n_a and n_b are nonces and $K = kdf(K', K'')$
    - Examples of kdf():
      - $K = K' \oplus K''$
      - $K = H(K' || K'')$, with $H(\cdot)$ secure hash function

The n^2 Key Distribution Problem

- Consider a system
  - Composed of *n* users where each party securely communicates with everyone
  - Where each pair of users shares a long-term secret pairwise key
    - Key pre-distribution
    - Out-of-band transmission

The n^2 Key Distribution Problem

- Every user stores (n -1) keys
- There are $\binom{n}{2} = \frac{n \cdot (n-1)}{2}$ symmetric key pairs in the system which is in the order of n^2.



The n^2 Key Distribution Problem

- Pros: Security
  - If a subject is compromised only its communications are compromised;
  - communications between two other subjects are not compromised
  - We cannot do any better!
- Cons: Poor scalability
  - The number of keys is quadratic in the number of subjects
  - A new member's joining/leaving affect all current members

The n^2 Key Distribution Problem

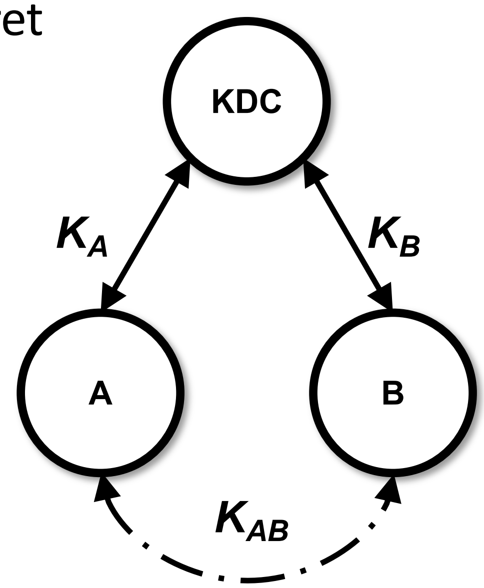
- Pre-distribution does not work for large dynamic networks
- Pre-distribution works for small networks where the number of users does not change frequently
  - E.g., branches of a company

Key Establishment

KEY ESTABLISHMENT USING SYMMETRIC-KEY TECHNIQUES

Key Distribution Center

- Each user shares a long-term secret key with KDC
  – Key Encryption Key (KEK)
- Each KEK constitutes a secure channel
- KEKs are pre-distributed



Performance and security issues

- Performance
  – Better scalability than pairwise scheme
  – Each user stores 1 KEK; the overall number of KEKs is *n*
  – Upon member's joining/leaving ➔ only 1 KEK must be established/removed
- Security
  – If a user is compromised, its communications are compromised
  – If KDC is compromised, all communications are compromised

Key Distribution Center

- KDC is a single point of failure
  - Performance
    - KDC must be available
    - KDC must be efficient
  - Security
    - KDC knows all the keys
    - KDC can read all msg between Alice and Bob
    - KDC can impersonate any party
    - KDC must a trusted third party

Basic KE using KDC (1/2)

Alice	**KDC**	**Bob**
KEK: K_A	KEK: K_A, K_B	KEK: K_B

----------- REQ(A, B) -- >

K_{AB} < -- RNG()

$y_A = E_{KA}(K_{AB})$; $y_B = E_{KB}(K_{AB})$

< ---- y_A ----------------- |-------------------- y_B ---- >

$k_{AB} = D_{KA}(y_A)$ $K_{AB} = D_{KB}(y_B)$

< ---- E_{KAB}(*session*) --- >

Basic KE using KDC (2/2)

Alice **KDC** **Bob**

KEK: K_A KEK: K_A, K_B KEK: K_B

|------------ REQ(A, B) -- >

$K_{AB} \leftarrow RNG()$

$y_A = E_{KA}(K_{AB})$; $y_B = E_{KB}(K_{AB})$

< ---- y_A ,y_B ----------------|

$k_{AB} = D_{KA}(y_A)$

|---------------------------- y_B ----------------------- >

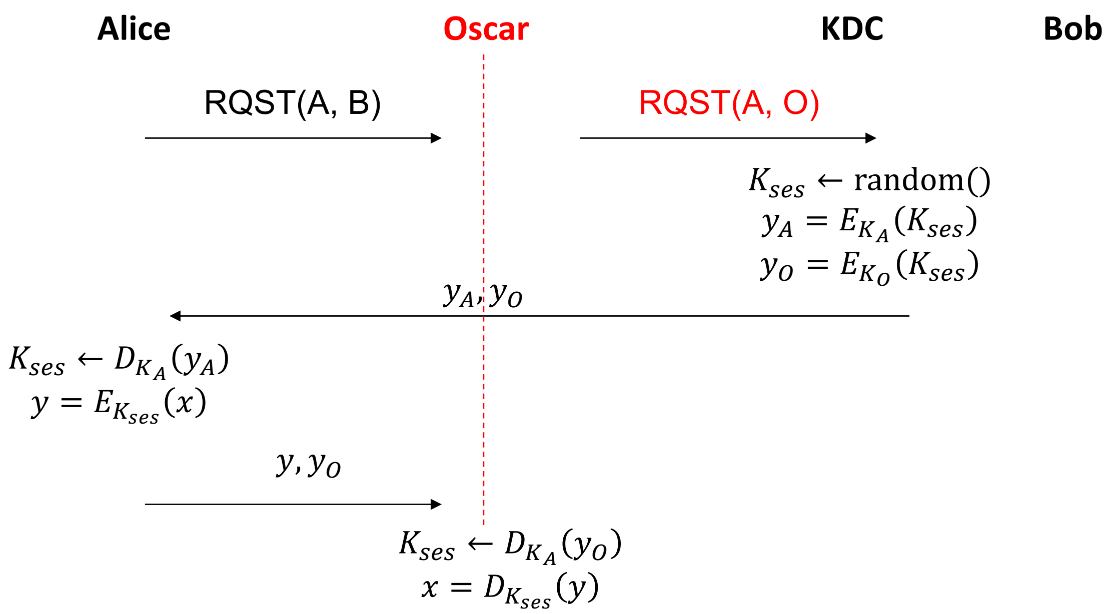
$K_{AB} = D_{KB}(y_B)$

< ------- E_{KAB}(*session*) ------ >

Security issues

- Replay Attack
  - The adversary records the key establishment protocol
  - The adversary replays y_A and/or y_B
  - The adversary make users to use an old session key
    - An old session can be replied (the session has to be recorded)
    - A compromised session key can be reused
  - We need a freshness proof.
- Key Confirmation attack (see next slide)
  - MIM attack performed by a legitimate but malicious user
  - Messages must be self-explainable/-contained

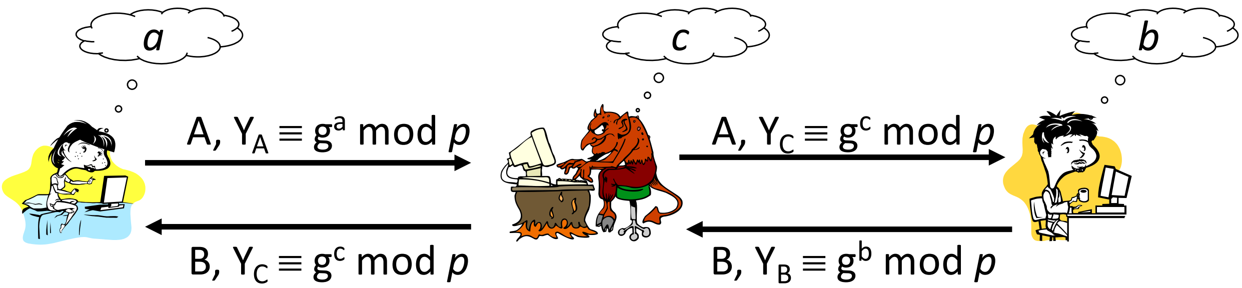
Key confirmation attack



Key establishment techniques

USING ASYMMETRIC TECHNIQUES

Man-in-the-middle Attack



$K_{AC} \equiv g^{a \cdot c} \bmod p$

$K_{AC} \equiv g^{a \cdot c} \bmod p$
$K_{BC} \equiv g^{b \cdot c} \bmod p$

$K_{BC} \equiv g^{a \cdot c} \bmod p$

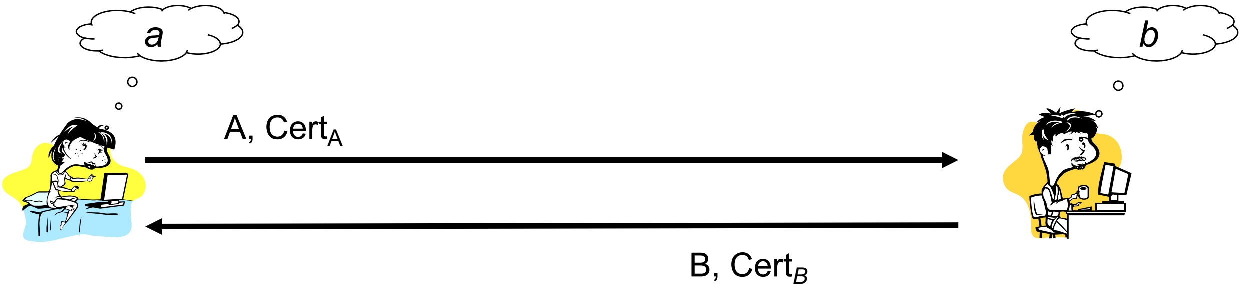
Certificate

- Certificate
  - Data structure that cryptographically links the identifier of a subject to the subject public key (and other stuff):

    $$Cert_A = A, pubK_A, L_A, S_{CA}(A \,||\, pubK_A \,||\, L_A)$$

    - A: identifier; $pubK_A$: public key; L_A: validity interval; || concatenation operator
  - Certification Authority (CA) is a TTP that attests the authenticity of a public key
  - CA's signature indissolubly links identifier and public key (and other parameters)

Man-in-the-middle Attack



$K_{AB} \equiv g^{a \cdot b} \bmod p$

$K_{AB} \equiv g^{a \cdot b} \bmod p$