Contents

1 Key Distribution and PKIs

1.1 The Problem of key distribution

Simple when people can meet beforehand.

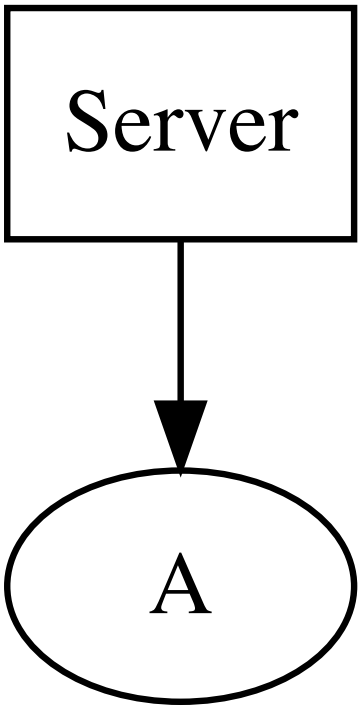
1.1.1 Key Distribution Centers

Some trusted server gives keys on the fly. Good if users are e.g. working in a company. Bad on internet, relies on honesty, needs permanent availability.

Notation for authenticated encryption: $i\{M\}_K$ with $K = (K_C, K_M)$.

A and B both trust server S, each having a shared key K_{AS}, K_{BS} with the server.

Idea1: Server chooses random K_{AB}, sends $\{K_{AB}\}_{K_{AS}}$ and $\{K_{AB}\}_{K_{BS}}$ to A.



Symmetric crphtography **does not** allow forward secrecy (when a session key is compromized, all future session keys are also compremized).

Idea 3: Needham-Schroeder (had an attack)

Final Idea: Fixed Needham-Schroeder

1.2 Idea of Merkle, Diffie and Hellman

Solution without KDC: Public-Key Cryptography. Using separate keys for encryption and decryption. public key sk used for verifying the correctness of the tag generated by the private key sk. A public register of public keys is still needed. Only this key distribution center needs to be known.

Advantages of digital signatures

- publicly verifiable
- transferable
- provide non-repudiation

Problems:

- Who maintains the register?
- How to contact in securely
- How to revoke the key if it is lost?