

Public Key Cryptography

Key Exchange

All the ciphers mentioned previously require keys known **a-priori** to all the users, before they can encrypt and decrypt.

To communicate securely, they need to have a **common key, known only to them**.

Possible key exchanges:

1. An a-priori meeting to exchange keys.
2. Sending the keys by a special courier.
3. Using an already existing common key, to encrypt additional keys.

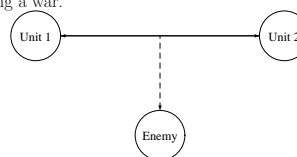
Key Exchange (cont.)

The problem: A meeting is required between the users (or their couriers), in order to be able to communicate securely.

Conclusion: Two users who have never met cannot communicate securely!

Example

Two armies during a war.



The enemy wins, since it found all the keys that our army use for communication.

Our army observes that the enemy found the keys. Our army must choose new keys, immediately, but it is impossible to send couriers through the enemies lines.

If our army does not agree on new common secret keys, we will certainly loose.

Public Key Cryptography - Background

The model: A network of N users.

In order to let any user to communicate securely to any other user, $\binom{N}{2} = O(N^2)$ keys should be distributed **in advance** in a **secure way**.

Possible solution: Trusted center.

Each user sets in advance a secret key with the trusted center. When user A wishes to communicate with user B, he chooses a new common key and sends it (encrypted under A's key) to the center, who forwards it (encrypted under B's key) to B.

Public Key Cryptography - Background (cont.)

Drawbacks:

1. There should be somebody that all the users trust.
2. All the users should have a common key with the trusted center **in advance**.
3. The center can always understand all the users' messages (and can fake messages).

Requirements for Key Exchange

We prefer a solution that allows two users who

- have **never** met, and
- do not have any a-priori common information,

to decide on a common key

- known only to them, and
- unknown to anybody else, even to passive eavesdroppers who listen to their communication (but cannot modify it).