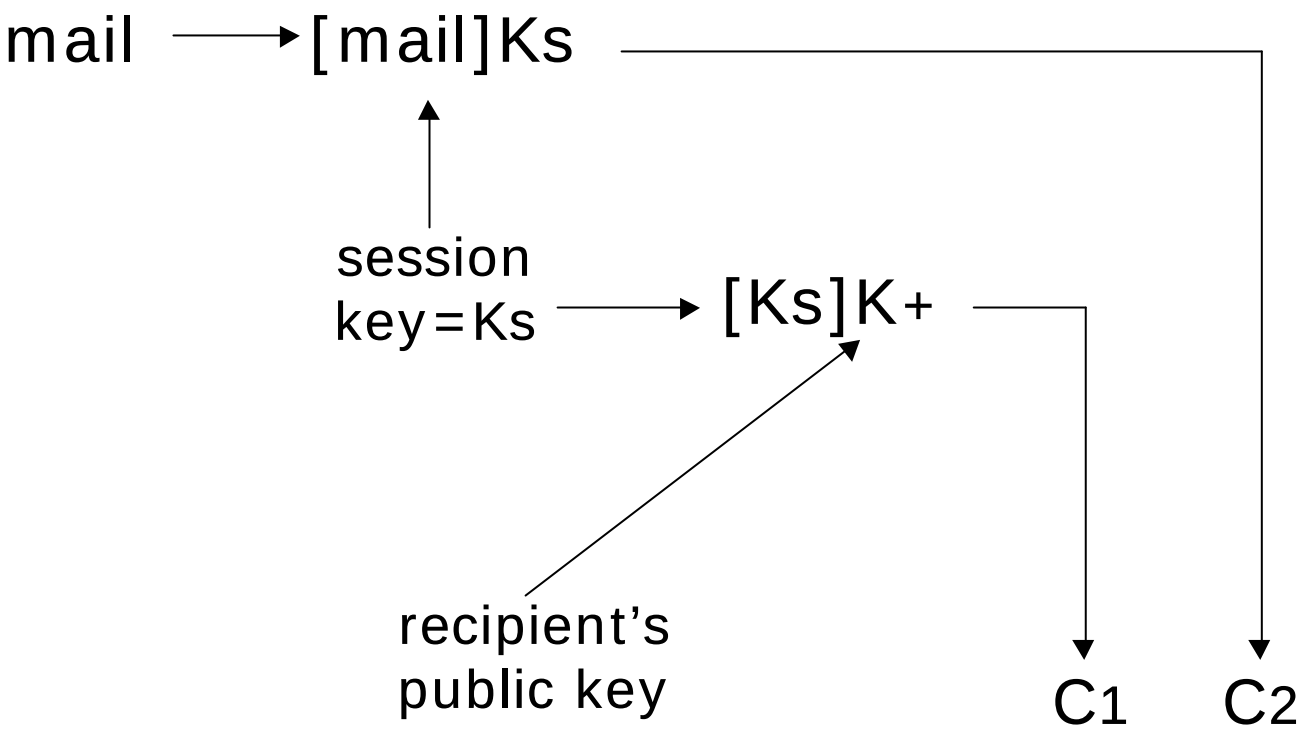
PGP: Pretty Good Privacy

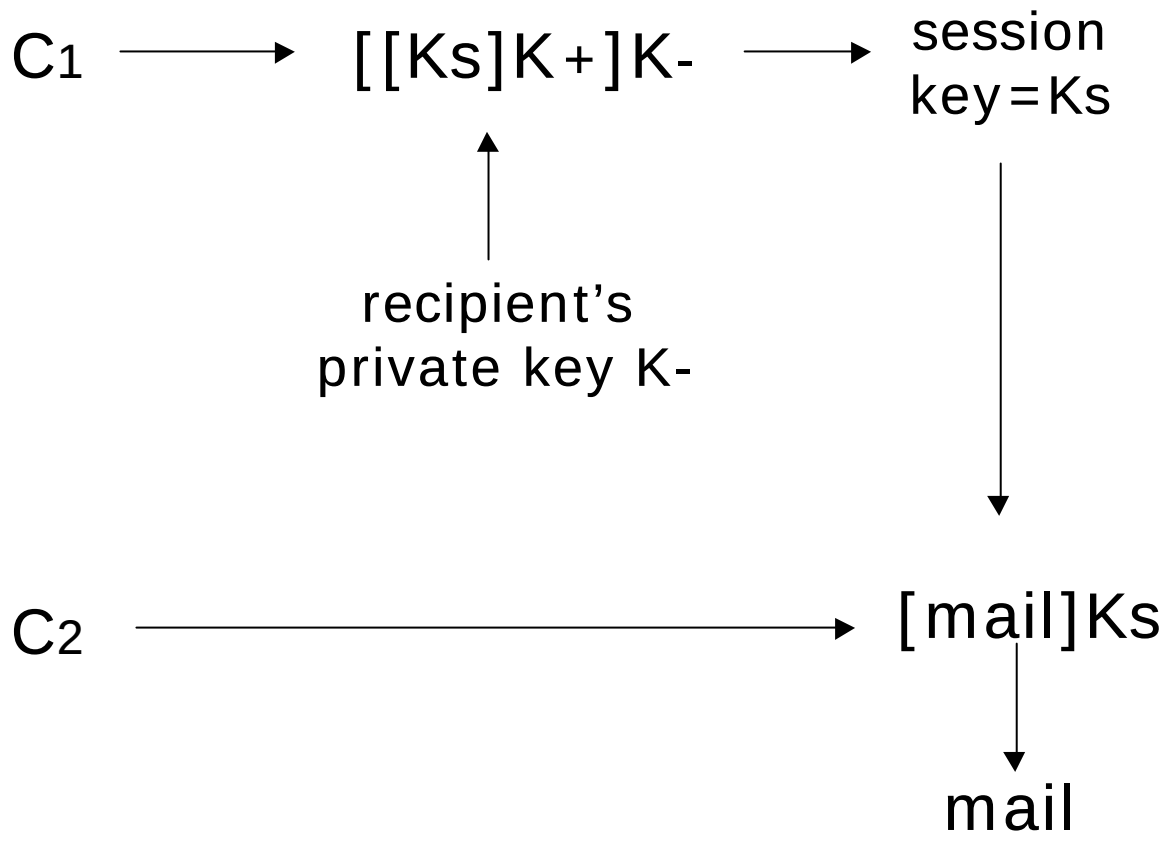
PGP

- Introduced by Zimmermann, first example of crypto for masses $\rightarrow$ legal troubles with US crypto export regulators
- Mainl application secure e-mail
- Trust model alternative to hierarchical ones (PKI based on ISO X.509 and IETF IPKI standards)
- Crypto algorithms used IDEA as SK, RSA and DH/DSA as PK, SHA-1 as hash function

PGP: Encryption



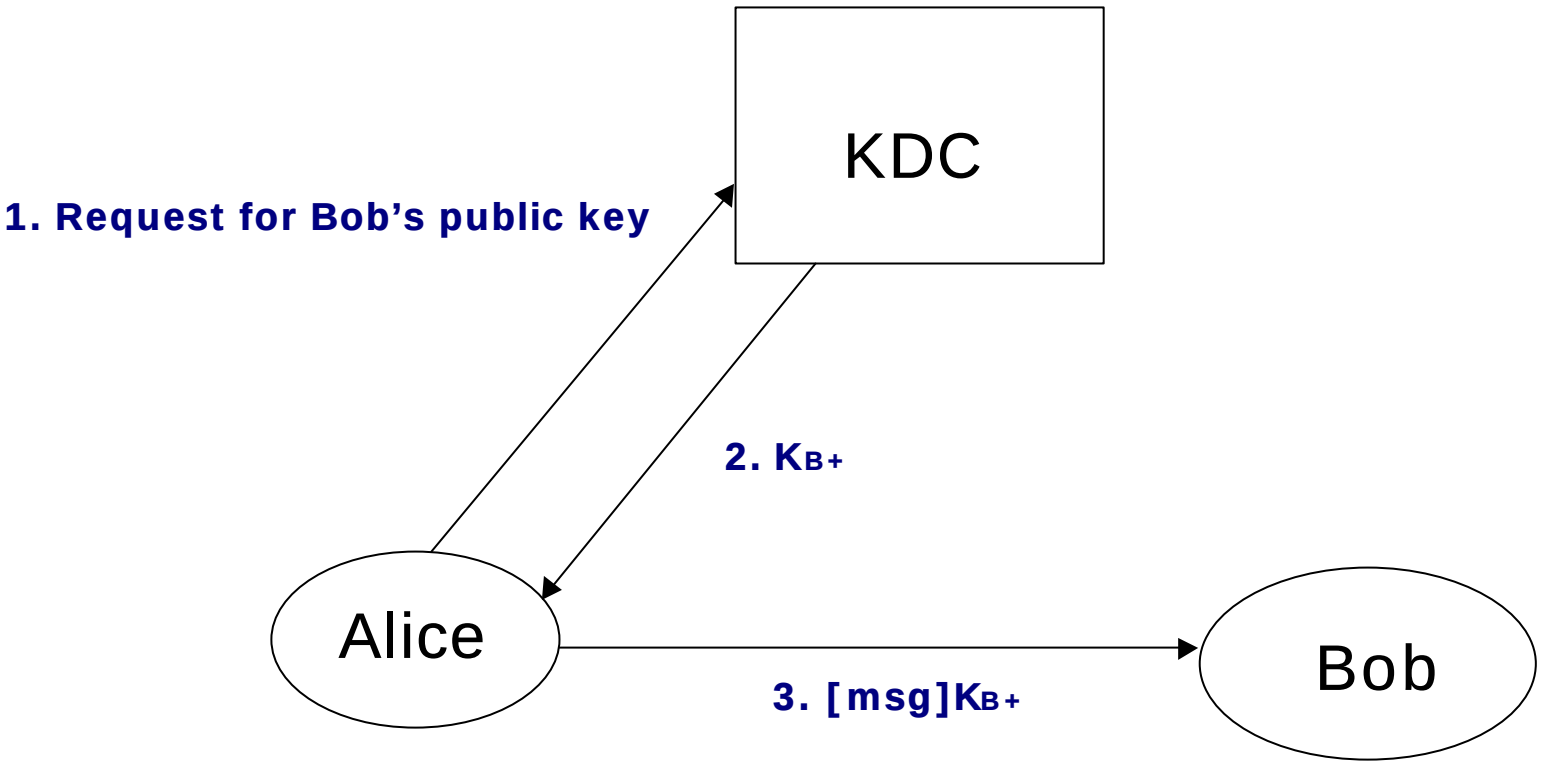
PGP: Decryption



PGP: Key storage

- Encryption key are generated when needed (session keys)
- Public keys and private keys are stored in special key stores called *pubring* and *secring,* encrypted with a key generated from a passprhase.
- PGP use a passphrase instead of a password

Trusted binding



PGP: digital certificate

- To securely bound a user id (e-mail address) to his public key, PGP use digital certificate

- PGP's digital certificate are consist of:

{

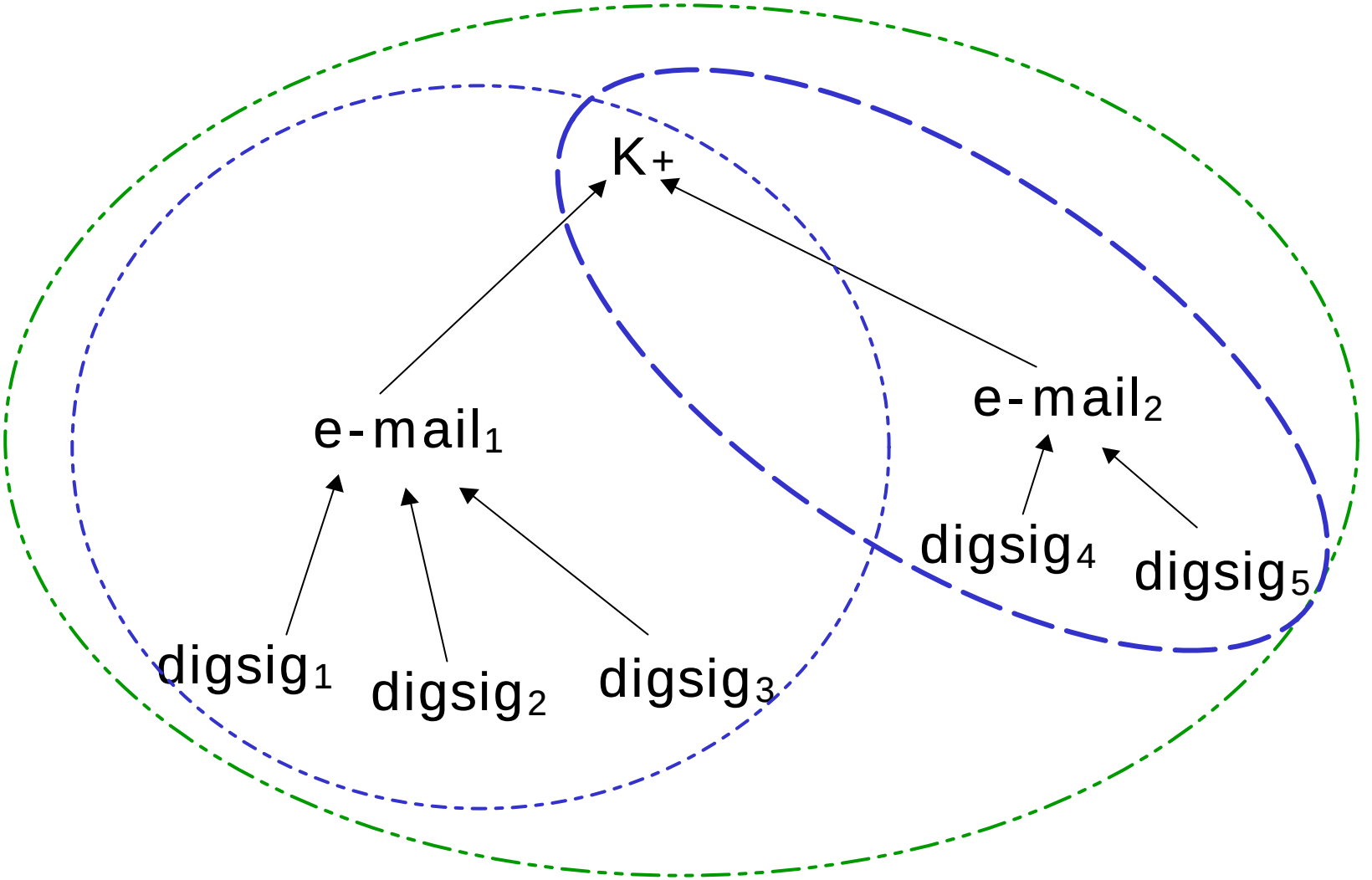
public key

user ID

one or more digital signatures

}

PGP: certificate and certification



PGP: Key servers

- PGP’s certificates can be published in many database as user wishes.
- He has simply to send his certificate to these databases (*key server*)
- Key servers can also be imported and used locally

PGP: trust model

- Important to consider which trust model is used to bind a public key to a user (or better to his e-mail address)

- PGP is different compared to other model (e.g. PKI) for the trust model adopted.

PGP: trust model

- PGP use a *democratic* approach completely distributed in order to manage the assignment and the distribution of trust
- PGP does not use third parties to register user's public keys or to issue the related certificate. Any user can execute those two functions
- Doing so PGP creates a *web of trust*

PGP: trust model

- PGP defines
  - Certifier: the user that generates the certificate
  - Certified: the user requiring his public key to be certified
  - The certifier by issuing a certificate asserts two things:
    - Authenticity of the binding key-certified
    - His level of trust of the certified acting as a certifier

PGP: trust model

- Each user can adopt his own criteria to reach his level of trust in the certified acting as certifier. So criteria may be very heterogeneous and difficult to represent in an objective way

- Level of trusts of different users cannot be compared

PGP: trust model

- On the contrary, PGP adopts two *trust levels* schemes
- A trust level to qualify the quality of certified users to act as certifiers

- A trust level to qualify the quality of the binding key-certified

Trust Levels for Certifiers

- A certifier can associate 4 different levels of trust to a certified acting as a certifier.
  - Implicit Trust
  - Complete Trust
  - Marginal Trust
  - Untrusted

Trust Levels for Certifiers

- *Implicit Trust*: Highest. It's the level associated by the certifier to his own key.

- *Complete Trust*: Certificates generated by users classified with this level are equivalent (trustwise) to certificates issue by the certifier himself

Trust Levels for Certifiers

- *Marginal Trust*: certificates generated by at least two certified classified with this level are equivalent to certificates generated by the certifier

- *Untrusted*: certificates generated by certifieds with this level are considered untrusted thus not reliable

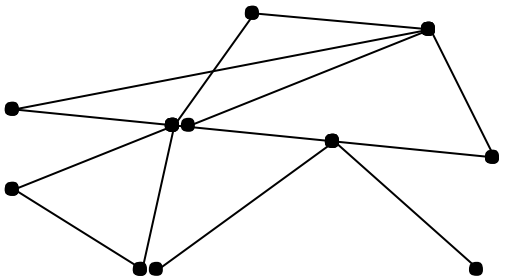
Trust Levels for Bindings

- A certifier can indicate three different levels of trust to the public key of a certified user.
  - Valid
  - Marginally valid $\rightarrow$ 2 make a valid one
  - Invalid

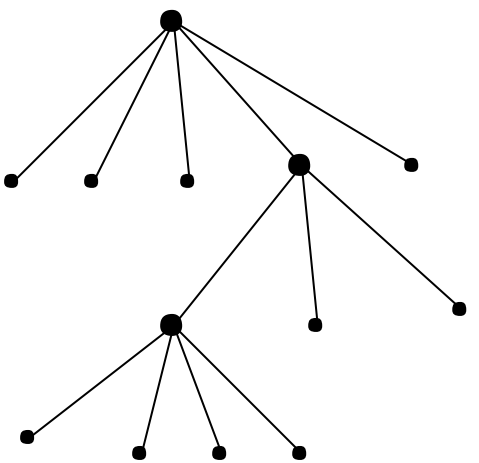
PGP: revocation

- Also with PGP is possible to revoke certificates. The problem is the distribution of the revocation information
- With PGP the user can revoke his key by sending the self-signed revocation msg to the keyserver. Other users have the duty to check this information
- There is no general mechanism but all is left to the good will and discipline of the user $\rightarrow$ usually bad assumption in security

Trust Models



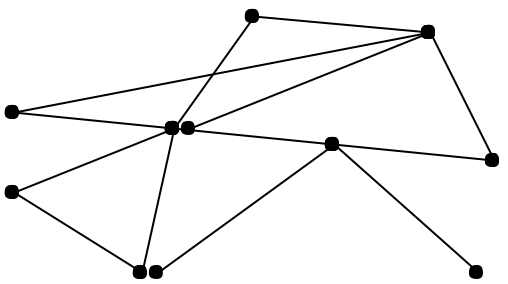
graph



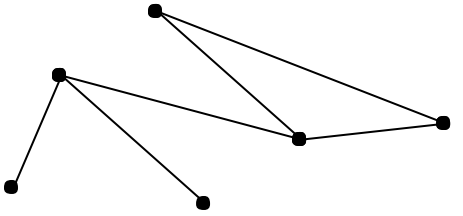
tree

Trust Models

Based on a “small world” observation called “*six degree of separation*” that says that representing users as nodes of a graph, given any two nodes is always possible to find a path between traversing at most 6 nodes



The model cannot exclude the Possibility of having disconnected islands.



PGP: trust model

- PGP associates public keys to e-mail addresses not to users
- PGP aim to offer a global system with no global policy to define and evaluate how to set the trust in the binding

public key « e-mail address

PGP: limitations

- Model of trust maps quite well many of our private communications but not the more formal ones (work,commercial, etc.)

- Web-of-trust does not reflect the trust model of many organisations which often adopt a hierarchical model

PGP: limitations

- PGP assumes trust transitive $\rightarrow$
  two marginal trust $\Rightarrow$ complete trust

In general trust is not transitive!