PKI (and FEIDHE)

Nordunet, Copenhagen

16.4.2002

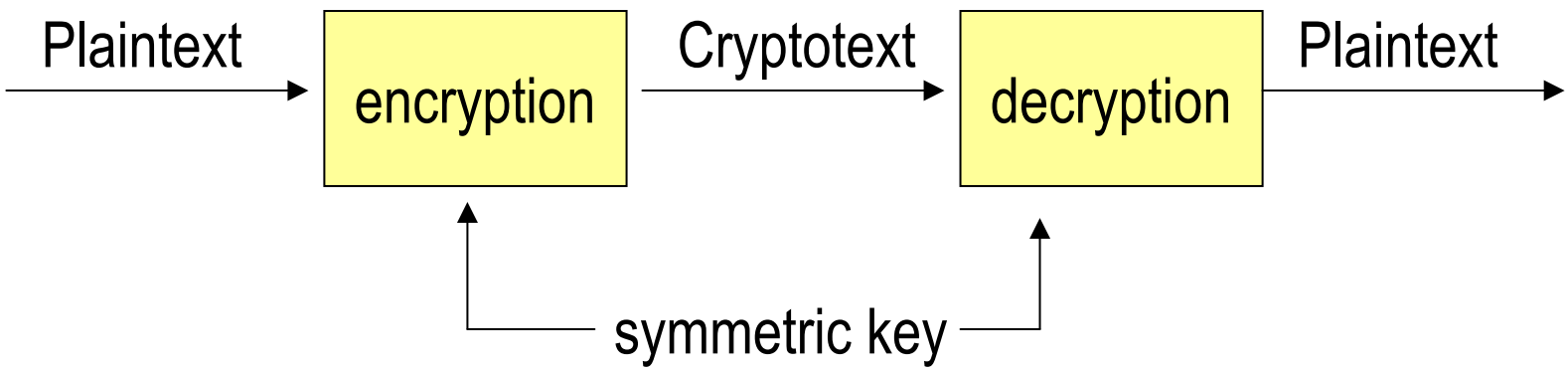
Pekka Linna

Contents

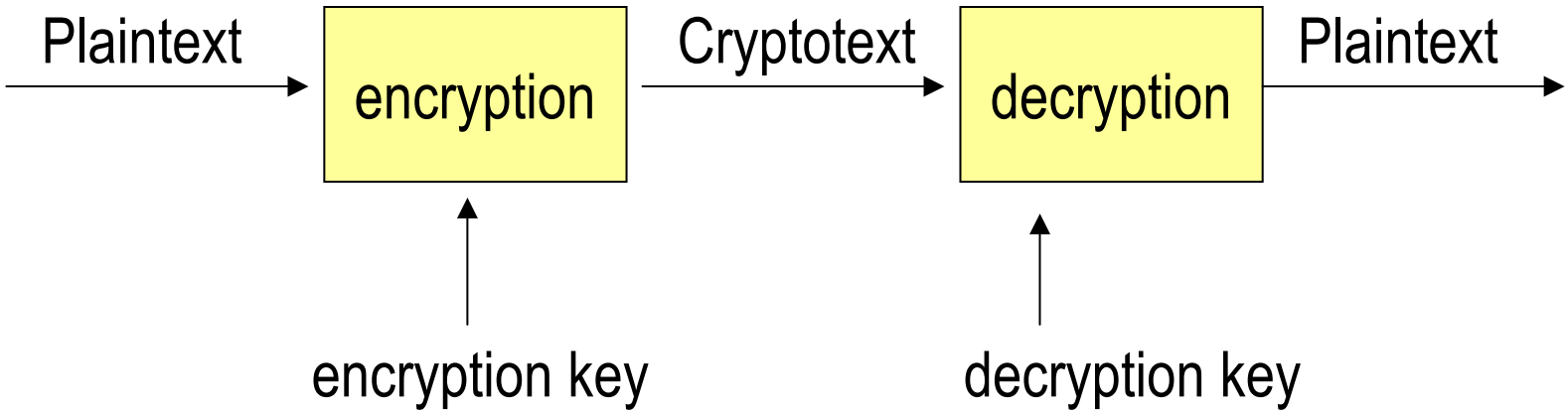
- Principles of public key infrastructure
  - No technological implementations
  - From the perspective of authentication
  - From the perspective of authentication of people
- Conclusions of the Finnish HE PKI initiative FEIDHE

Symmetric encryption

- Old invention
- Same key encrypts and decrypts



Asymmetric encryption



- In asymmetric encryption the encryption key and the decryption key are different from each other.

Public key

- Two separate keys for encryption and decryption
- Yet it is impossible to calculate one key from the other

Innovation

- One of the keys can be made publicly available.
- The interaction is safe if only the other key stays private.
- Hence ’public key’ and ’private key’.

Authentication

- These two keys are belong together
- Yet it is impossible to calculate one key from the other
- The private key is in possession of a certain person.

Innovation

- This can be used for strong authentication.
  - If I use your encryption key to encrypt a test-message, you are the only one that can decrypt that message!

Problems: key distribution

- How can I get my private key and be sure that no-one else knows it?
- How can you get my public key and be sure that it is mine (that I have the private key related to this public key)?

-> Private key infrastructure

Trusted third party

- We need a trusted third party.
  - An actor that both I and all potential interaction partners of mine can trust.
- This trusted third party will
  - be responsible for the private key being in the possession of the right person.
  - make the public key publicly available.
  - publish a connection between the public key and the person to whom the private key was given to.

Problems: connection

- How to publish a trustworthy connection between the public key and the person to whom the private key was given to?

->Certificate

Certificate

- The trusted third party signs a document that includes
  - my public key; and
  - the information that that public key relates to me.

- This document is called ’certificate’.
- The third party is thus called ’certificate authority’.

X.509v3 certificate (RFC 2459)

version	v3
serialNumber	34E6
issuer	c=FI o=VRK-FINSIGN Gov. CA cn=FINSIGN CA for Citizen
validity	begins 11.7.2000 klo 1.59.59 ends 7.7.2003 klo 1.59.59
subject	c=FI cn=LINDEN MIKAEL 10005323B
subjectPublicKeyInfo	3081 8902 8181 00DF B6DF …
extensions	
signatureAlgorithm	SHA-1 & RSA
SignatureValue	AFFF 3081 E5C5 70EB 442A …

Problems: trust

- Why would I trust a certain third party?

- Certificate authority makes its principles and procedures publicly known
  - this document is called ’certificate policy’
- Certificate authority is assessed by a trusted authority
- Certificate authority is trusted by actors that you trust

Problems: identity

- What is the ’I’ that the public key is connected to?

- Resource management and organisation-specific PKI
  - there can be an organisation-specific identifier within the certificate.
- Resource management and non-organisation-specific PKI
  - certificate has to be connected to the user in the user administration information systems.

Overview of FEIDHE

- 6/2000-3/2002
- to find out what it would take to implement a smart card based PKI in HEI
- project members
  - universities and polytechnics
  - related national student unions
  - CSC, the Finnish center for high-performance computing andnetworking

Conclusions (DRAFT)

1. Developing information systems in HEIs requires national coordination by the ministry of education.
2. PKI is a functioning solution for strong authentication and can be utilized in HEIs as well.
3. There are problems in the security of public workstations. The problems and related liability issues need to be resolved.

Conclusions… (DRAFT)

4. Implementations available have certain limitations.
5. User administration systems in HEIs need to be developed, because a large-scale-deployment of PKI requires a possibility to centrally connect a certificate to the user.
6. Distribution of a large number of PKI smart cards is not reasonable before there are enough services in the network available for the card.

Conclusions… (DRAFT)

7. To get prepared for PKI deployment HEI staff needs training and practical experience on the technology.
8. Electronic services and processes need to be developed in HEIs.
9. Implementing inter-organizational network services require national decisions on practices and technology.

Thank you!

Contact:
hstya.funet.fi
pekka.linna@csc.fi