Cryptography, Summer Term 2013

Harald Baier

Chapter 1: Security goals and cryptographic techniques

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
fbi
FACHBEREICH INFORMATIK

CASED

da/sec
BIOMETRICS AND INTERNET-SECURITY
RESEARCH GROUP

A real life example

Pfungstadt sucht Bürgermeister/in

Start zum 1. Januar 2014. Die Bewerbungsfrist endet wahrscheinlich im Mai 2013.

Eine interessante und gut dotierte Position (B 4) – mit einem hohen Anforderungsprofil: Über 30 Millionen Euro Schulden sind zu bewältigen, ein defizitärer Haushalt ist zu sanieren, 257 Mitarbeiter/innen wollen angeleitet und motiviert werden, die Struktur der Stadt ist weiterzuentwickeln – alles in allem also nichts für berufliche Anfänger, sondern für jemand der erfahren ist, der tatkräftig und entscheidungsfreudig dafür sorgt, dass die 25.000 Bürgerinnen und Bürger eine gute Zukunft in ihrer Heimatstadt Pfungstadt und in ihren Stadtteilen haben.

Wenn Sie sich das zutrauen, bewerben Sie sich oder sprechen Sie vorab mit Pfungstädtern, die die Situation kennen, die Sie gern im Detail informieren (auch wenn Sie zunächst anonym bleiben wollen): Lutz Feldmann Tel 06157.930483, Friedrich Herrmann Tel 06157.3359, Manfred Gröninger Tel 0171 4408200.

Samstag, 2. Februar 2013 · ECHO

Security Goals in Cryptography (1/2)

- Authenticity (Handbook of Applied Cryptography):
  - It should be possible for the receiver of a message to ascertain its origin.
  - An intruder should not be able to masquerade as someone else.
- Integrity (Handbook of Applied Cryptography):
  - It should be possible for the receiver of a message to verify that it has not been modified in transit.
  - An intruder should not be able to substitute a false message for a legitimate one.

Security Goals in Cryptography (2/2)

- Non-repudiation (Handbook of Applied Cryptography):
  - A sender should not be able to falsely deny later that he sent a message.
- Confidentiality (ISO-17799):
  - Ensuring that information is accessible only to those authorised to have access.

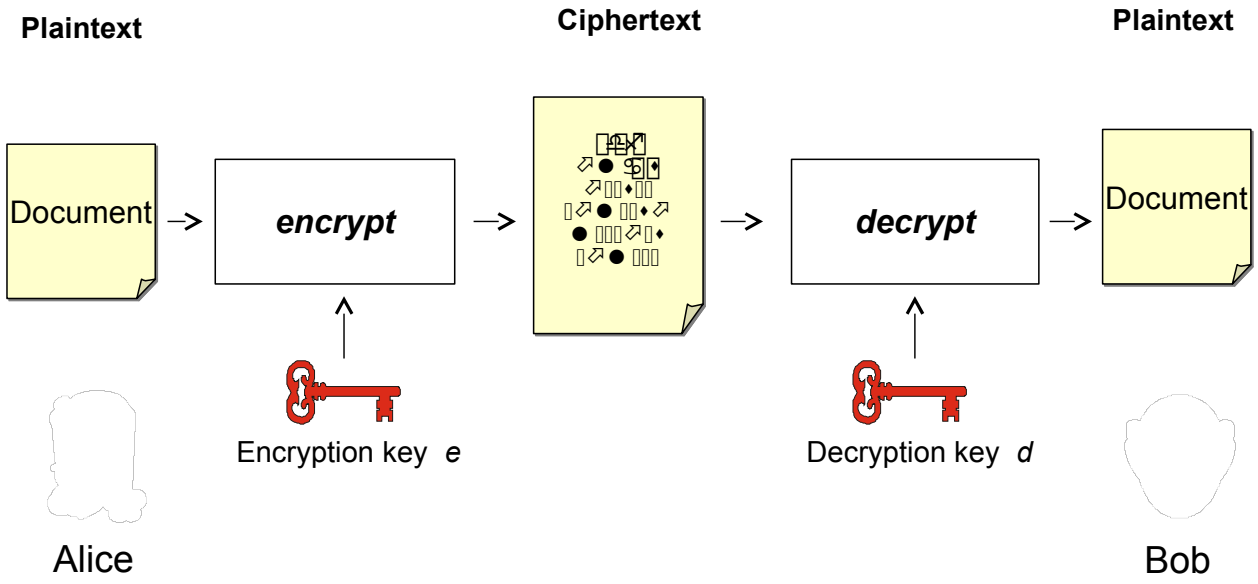
Security Goals vs. Cryptographic Techniques

- Fundamental question:
  - How may we reach each security goal in IT systems?
  - By means of cryptographic techniques
  - Ideas?

Security Goals vs. Cryptographic Techniques (cont.)

- Encryption
  - Symmetric encryption
  - Public key encryption (= asymmetric encryption)
- Digital Signature
  - Message Authentication Code (MAC)
  - Electronic Signature (= asymmetric signature)
- Which technique guarantees which security goal?

Encryption



Which key must not be revealed?

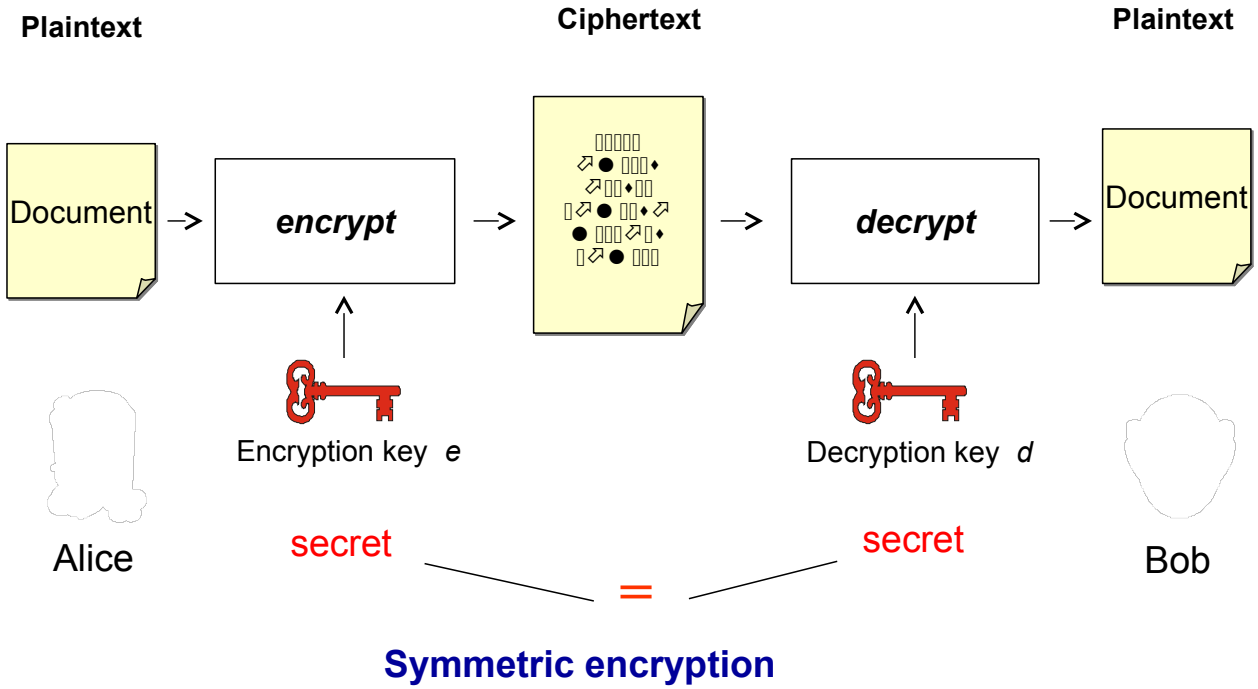
A more formal definition of a cryptosystem

- Cryptosystem is a five tuple of sets $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$
  - $\mathcal{P}$ is the the set of plaintexts units.
  - $\mathcal{C}$ is the the set of ciphertexts units.
  - $\mathcal{K}$ is the set of keys.
  - $\mathcal{E} = \{E_k: k \text{ from } \mathcal{K}\}$ is set of encryption functions $E_k: \mathcal{P} \rightarrow \mathcal{C}$.
  - $\mathcal{D} = \{D_k: k \text{ from } \mathcal{K}\}$ is set of decryption functions $D_k: \mathcal{C} \rightarrow \mathcal{P}$.
  - For every encryption key e from $\mathcal{K}$ there is a decryption key d from $\mathcal{K}$ with $D_d(E_e(m)) = m$ for all plaintexts m.

The two types of encryption schemes

- Symmetric Encryption:
  - Encryption key *e* = Decryption key *d*
  - = in the sense 'essentially equal'
  - Both keys (which essentially is only one) are accessible to both Alice and Bob
  - Consequence: Both keys have to be kept secret
- Asymmetric Encryption:
  - Encryption key *e* ≠ Decryption key *d*
  - ≠ in the sense 'sufficiently different'
  - Encryption key *e* public: Public Key
  - Decryption key *d* secret: Private Key

Symmetric Encryption



Symmetric Encryption: Examples

- Classical (analogue) schemes:
  - Simple monoalphabetic substitution ciphers
    - Caesar's cipher
    - General shift cipher
  - Vigenère's polyalphabetic substitution cipher
- Rotor machines:
  - The German Enigma
- Digital Ciphers:
  - Data Encryption Standard (DES)
  - Advanced Encryption Standard (AES)