swisscom

Cryptological Concepts

Charles Clavadetscher, SGS-CT-ITA

swisscom

Cryptology = Science of secrecy

- **Cryptography** = The art or science encompassing the principles of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form
- **Cryptoanalysis** = The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key (codebreaking)

swisscom

Conventional notation

Convention

- **E** encipher, encrypt
- **D** decipher, decrypt
- **k** key
- **kpub** public key
- **kpriv** private key
- **P** plaintext
- **C** ciphertext
- **MD** message digest
- **d** digest

Examples

$$C = E_k(P)$$

$$P = D_k(C)$$

$$d = MD(P)$$

swisscom

Definition

- **Cipher:** an algorithm for transforming an intelligible message into one that is unintelligible
- **Plaintext:** the original intelligible message
- **Ciphertext:** the transformed message
- **Key:** some critical information used by the cipher
- **Encipher:** the process of converting plaintext to ciphertext using a cipher and a key (encrypt, encode)
- **Decipher:** the process of converting ciphertext back to plaintext using a cipher and a key (decrypt, decode)

swisscom

Message digest

- One-way hash function
- Input = variable length stream of bytes (pre-image)
- Output = fixed-length byte array (hash value)

- Easy to compute hash value
- Hard to generate a pre-image that hashes to a particular value
- collision-free: difficult to generate 2 different pre-images with the same hash value
- One bit changed in pre-image -> complete different hash value

swisscom

Basic principles: Security

- **The level of security does not depend on the secrecy of the algorithm. Algorithms must be publicly discussed.**

- **Perfect security is impossible. A cipher is considered secure if an attack using the most recent technological resources cannot be broken within a useful time.**

swisscom

Basic principles: Transposition

- Text remains the same before and after transposition, but the order of characters is shuffled around

Example:

Text: Cryptography can be fun

Key = 6:
```
CRYPTO
GRAPHY
CANBEF
UN
```

Ciphertext: CGCU RRAN YANP PBTH EOYF

swisscom

Basic principles: Substitution

- Each character of the plaintext is substituted with another character in the Ciphertext

Example:

Text: Computers are silly

Key:
```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
EFGHIJKLMNOPQRSTUVWXYZABCD

P: COMPUTERSARESILLY
C: GSQTYXIVWEVIWMPPT
```

swisscom

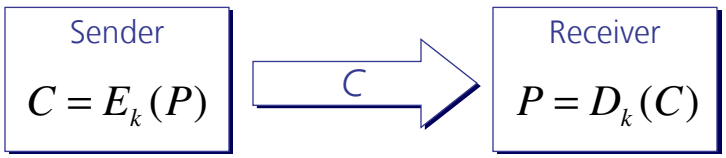
Basic principles: Stream vs. block cipher

- **Stream cipher:** Algorithm operates on one bit (or character) at the time.
- **Block cipher:** Algorithm operates on fixed-sized groups of bits (or characters).
  - Mode: How blocks of plaintext are encrypted into blocks of ciphertext (Electronic Code Book: one-one, Cipher Block Chaining: XOR-chain, etc).
  - Padding: The length of a plaintext must be a multiple of the block size. If the text is too short padding is used.

swisscom

Symmetric cipher: principle

- Sender and receiver share the same key



- Stream or block cipher

$$P = D_k(E_k(P))$$

swisscom

Symmetric cipher: Vigenère

- Stream cipher

$$C_i = (P_i + k_i) \bmod n$$
$$P_i = (C_i + n - k_i) \bmod n$$
$$i = Character\ at\ i-th\ place$$
$$n = Number\ of\ \ possible\ characters$$

```
P: THISISAVERYCOOLEXAMPLE
K: HALLOHALLOHALLOHALLOHA
C: AHTDWZAGPFFCZZZLXLXDSE
```


swisscom

Symmetric cipher: One-time pad

- **Perfectly secure!**
- Vigenère with 3 additional conditions:

1. Key must be truly random

2. Key must be at least as long as plaintext

3. Key must be used only once

swisscom

Symmetric cipher: balance

- **Advantages**
  - **Simple**
  - **Quick**
- **Disadvantages**
  - **Key exchange must be done securely**

swisscom

Key agreement: Diffie-Hellmann

- A and B agree on two numbers **a** and **p** where a<p
- A chooses any number k_1 and B any number k_2

$A: y_1 = a^{k_1} \bmod p$ $\qquad$ $B: y_2 = a^{k_2} \bmod p$

$(a^{k_2})^{k_1} \bmod p = a^{k_2 k_1} \bmod p$ **=** $(a^{k_1})^{k_2} \bmod p = a^{k_1 k_2} \bmod p$

Example:

$a = 7; p = 11$

$A: k_1 = 4 \rightarrow 7^4 \bmod 11 = 3$

$B: k_2 = 8 \rightarrow 7^8 \bmod 11 = 9$

$both: 7^{9 \cdot 3} \bmod 11 = 5 = key$

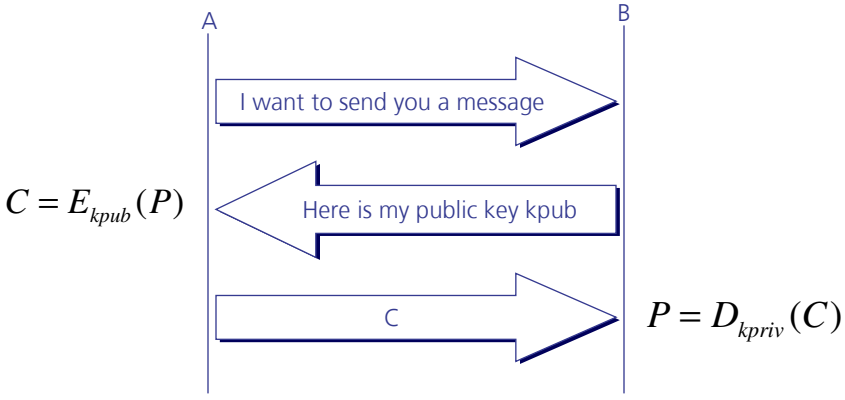
swisscom

Asymmetric cipher: principle (1)

- Each user has a **key pair**
- A key pair consist of a **public key** and a **private key**
- The private key **always** remains with the owner
- The public key must be given in order to receive encrypted messages.

swisscom

Asymmetric cipher: principle (2)



swisscom

Asymmetric cipher: balance

- **Advantages**
  - Private key never goes on public ground
  - Public key can be published everywhere
- **Disadvantages**
  - Slow

swisscom

Digital signature: principle

- Based on asymmetric ciphers
- Signer encrypts message using his own private key
- Receiver decrypts message using the sender's public key

$$signed\ message = E_{kpriv}(P)$$

$$P = D_{kpub}(signed\ message)$$

swisscom

Encrypt and sign at once

$$A: C_{signed} = E_{kpub_B}(E_{kpriv_A}(P))$$
$$B: P = D_{kpriv_B}(D_{kpub_A}(C_{signed}))$$

swisscom

Real life... one

- Asymmetric ciphers are too slow to encrypt large amount of data. Possible strategies:
  - Exchange a symmetric key for encryption using an asymmetric cipher
  - Compute a message digest of a text and sign only the digest

swisscom

Real life... two

A wants to send a signed message to B. He computes a digest **d** and generates a symmetric key **k**. He signs the digest, encrypts the plaintext with k and encrypts the symmetric key with B's public key

$$d = MD(P)$$
$$d' = E_{kpriv_A}(d)$$
$$C = E_k(P)$$
$$k' = E_{kpub_B}(k)$$

$$A\ sends\ C, d'\ and\ k'$$

swisscom

Real life... three

B decrypts the symmetric key with his own private key and decrypts the ciphertext using this key. He computes the digest for the message received and decrypts the digest received with A's public key. If both d match the verification of the signature succeded.

$$k = D_{kpriv_B}(k')$$
$$P = D_k(C)$$
$$d = MD(P)$$
$$d = D_{kpub_A}(d')$$

swisscom

Certificates

- A certificate is a public key signed with the private key of a Certification Authority (CA)
- A CA is an entity recognized as such by a community
- The CA certificates the identity of the owner of a public key

swisscom

Bibliography

- SCHNEIER, Bruce, *Applied Cryptography*, John Wiley & Sons, ISBN 0-471-11709-9 (The bible for practical cryptography, goes very deep into algorithm details. Requires mathematical knowledge)
- SINGH, Simon, *The Code Book*, Fourth Estate, ISBN 1-85702-879-1 (A history of cryptography in a very exciting style. No mathematical knowledge required)
- KNUDSEN, Jonathan, *Java Cryptography*, O'Reilly, ISBN 1-56592-402-9 (Basic description of cryptography and detailed introduction in using the JCE)

swisscom

ULRALCFH

(Vigenère encrypted, key=BERN)