Cryptology part II

Keränen, Teeriaho / Ramk 2006

Contents :

Litterature;

1. Menezes &Co Handbook of Applied Cryptography , CRC Press 2001
web: http://www.cacr.math.uwaterloo.ca/hac/
2. Bruce Schneier: Applied Cryptography
3. Henk C.A. van Tilborg, Fundamentals of Cryptology, Kluwer 2000
4. Shon Harris: CISSP certification exam quide , McGraw-Hill 2003

1 Introduction

■ 1.1 Definition of cryptology

Cryptology is a science researching encryption algorithms and their security

Cryptology = Cryptography + Cryptanalysis

■ 1.2 Cryptology as a part of data security

Data security (information security) has following goals:

1) To secure **confidentiality** of information
2) To secure **integrity** of information
3) To **autenthicate** the communicating parties
4) To provide **non-repudiation** services
5) To provide **access control**
6) To provide **availability** of information

Confidentiality means, that only the sender and the intended receiver can read the message.
Integrity means that no third party is able to change the informationand messages
Authentication means reliable checking of the identities of the parties.

Non repudiation means that the sender of a message can't later deny having sent it.
Availability means, that the information should be easily available to those who need it and are entitled to use it.

Cryptology is a part of **technical data security**. It provides solutions for confidentiality, integrity, authentication and non-repudiation.

■ 1.3 Cryptography and cryptanalysis

Cryptology is divided into two parts: **cryptography and cryptanalysis**. Cryptography develops encryption algorithms and cryptoanalysis develops methods of breaking cryptosystems

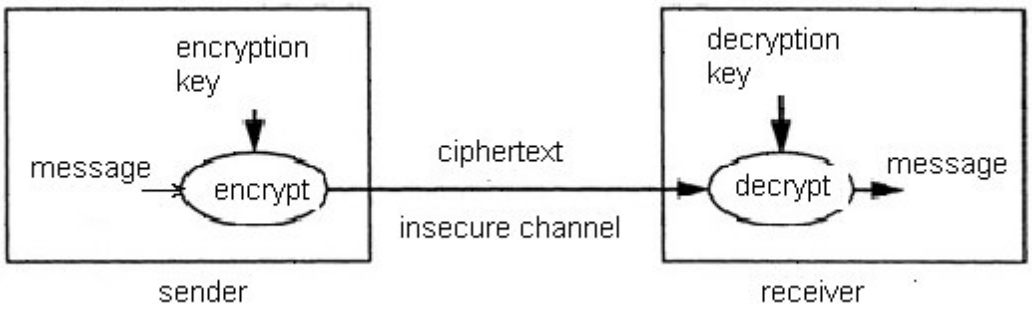
■ 1.4 Cryptological services

▪ A) Encryption of messages

Encryption of messages **provides confidentiality of messages.** It is the oldest service of cryptology.

A Roman **Aeneas Tacticus** wrote 360 BCr in his book about the art of warfare a chapter about ”secret messages”. Today cryptology is used in everyday applications (mobile phones, email). F.e. GSM calls are encrypted, many files of companies are encrypted. Basic idea has remained same for centuries: to transform messages into a form, that only the intended receiver can understand.

The principle of encryption.



Message M (plaintext) is represented as a sequence of characters of a finite alphabet: f.e ”Meet you at 12”.

C = **e** (**M**) **-** is a standard notation for the encrypted message. Letter **e** comes from **encryp-**

tion .

C is called **cipher, ciphertext, or cryptogram** .

Decryption function d is used to open the encryption:

$$d\,(\,e\,(\,M\,)\,)\,=M$$

Function d returns the plaintext from the cipher.

In practice e is a function algorithm which uses parameter called **keys** . For keys we use symbol K.

We can write :

encryption $C = e(M, K_1)$

decryption $M = d(C, K_2)$

M = message , C = cipher ,
K_1 = encryption key , K_2 =decryption key
e = encryption function , d = decryption function

Symmetric key encryption and public key encryption

In symmetric key encryption algorithms the encryption key K_1 and decryption key K_2 are same.

The types of symmetric algorithms are stream ciphers and block ciphers

In stream ciphers message is encrypted one character (or bit) at the time.

In block ciphers the message is encrypted in blocks (often 64 bits or 128 bits).

First block ciphers were developed during 1970's, when IBM planned a cryptosystem called Lucifer. US authorities joined the project and the result was DES - block cipher. DES was an

official standard in USA from 1977 till 2001.

From stream ciphers the most famous is A5, is used to encrypt GSM- and GPRS - calls. It is used since 1991.

Public key encryption

* Each user has two keys: a private key and a public key.

* The sender of a message encrypts the message with the public key of the receiver. The receiver decrypts the cipher with his private key.

The principle of public key encryption was presented by Diffie and Hellman v. 1977

1. No agreement on symmetric key is necessary

2. Encryption algorithm is completely public.

3. Every user A of the system has a public key, which is used to encrypt messages to A.

4. Every user A has also a private (secret) key for decryption.

5. Public key - private key pairs can be easily created, but deriving the private key from the public key is very difficult even with a great computing capacity.

- **B) Hash functions**

A hash function is a **one way function**, which is used to calculate a fixed length (often 128 -bit) hash value (also called message digest, digital fingerprint) from the message

The *one way function* property of hash-functions means, that it is impossible to calculate the message from its hash. A good hash function must meet also other requirements , which we talk about later.

The hash value calculated from the message is needed to *ensure the integrity of the message* during the data transfer. Hash values of passwords are also stored *in password files* f.e in UNIX operating system instead of the passwords themselves.

- **C) Digital signatures**

Digital signatures are used to ensure a) the *authentity* and b) *integrity* of messages. These together quarantee the principle of *non repudiation*.

In Digital signature algorithms the hash value of the message is created and then encrypted with the private key of the sender. The receiver opens the signature with the public key of the sender. Then the receiver calculates the hash value from the message. If in the comparison both hash values are identical, the receiver can be sure of the authentity of the message and also of the fact that the message is unchanged.

In digital signatures two cryptographic algorithms are used: calculation of hash values and public key encryption.

- **D) Authentication servi ces**

Definition:
Authentication is a technique, which ensures one part a) of the identity of the other part and b) of the fact that the other part is active at the moment of authentication.

Note! The difference between digital signatures and authentication has been undestood only during the last decennies. The techniques are close to each other, but the difference lies in the fact that authentication must happen within a certain time window. If this does not happen, denial of service follows. Digital signature is not time-constrained. Digitally signed letter can lie in the inbox file for a long time still being valid.

Digital authentication is used in checking the authentity of bank cards, and smart card services.
Authentication can also be done without cryptoalgoritms using one time password lists.

- **E) Other applications**

Electronic voting systems has beeb researced a lot during last years. Techniques have been developed and they may be in use in some countries very soon.

Secret sharing systems is also an application whch has been explored. It means for example techniques, where to open a door of a top secret safe or laboratory it is enough to use the keys of any six arbitrary members of the staff.

■ 1.5 Secure protocols and - hybrid systems

Cryptoalgorithms work usually inside so called secure protocols without been observed. The following protocol names are familiar to every user:. HTTPS , SSH , SSL, ...
Typically these protocols can be configured to use a variety of encryption algorithms.

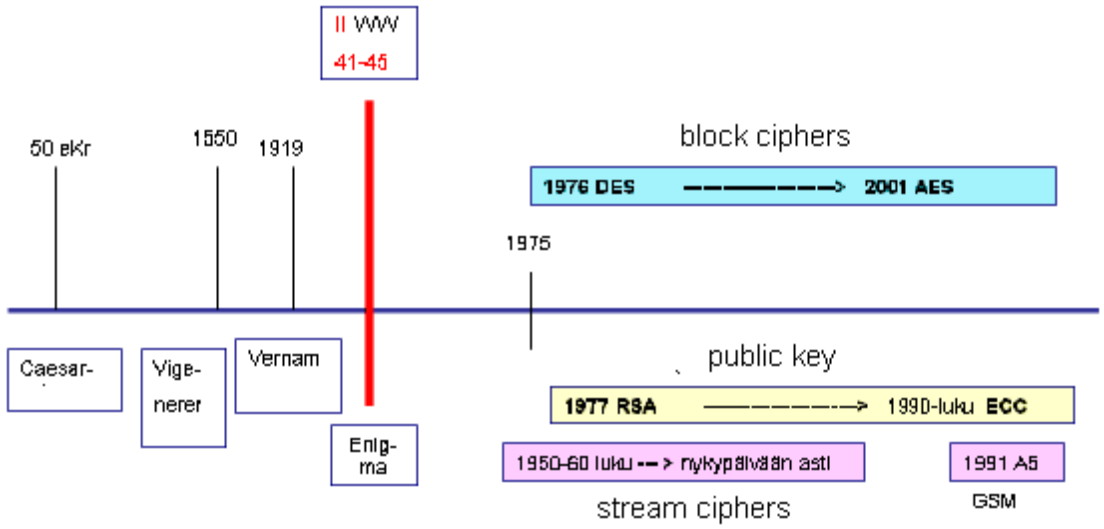
Most cryptosystems are so called **hybrid systems**., where several different cryptoalgorithms are used for different purposes.

1) Enctyption of messages uses a block cipher (AES , IDEA, earlier DES)
2) Key agreement protocol uses publc key algorithm
3) Autenthication uses public key algorithm
4) Digital signature algorithm is based on a public key algorithm

Typically the user has several keys for different purposes.

■ 1.6 Historical development of cryptosystems

The figure below shows some important times:



Classical cryptoalgorithms are algorithms used before the computers and modern telecommunication. Those are f.e Caesar, Vigenere and Vernam ciphers. Also Enigma encryption machine from II Worl War is one of them.

First **symmetric cryptoalgorithms** were stream ciphers, which were used for military purposes during the cold war. The first **block ciphers** were developed in the middle of 1970's. In the late 1970's the first **public key algorithms** were created**.**

■ 1.7 Terminology

cryptology = research of cryptosystems
cryptography = developes cryptoalgorithms
cryptoanalysis = tries to break cryptosystems
cryptographer = researcher of cryptography
cryptoanalyst = researcher of cryptoanalysis
cryptosystem = a system developed for *encryption*
algorithm = a sequence of mathematical rules for obtaining desired result
message, plaintext = a text which is not yet encrypted
cipher, ciphertext = a message which has already been encrypted
encrypt , encipher
encryption
decrypt , decipher = to transform the ciphertext back to plaintext
decryption
key
key space = a set of all possible encryption keys
enemy = a person who wants to reveal the secret message
attack = an attempt to break the ciphertext
eavesdropper = a person who tries to listen to the channel to obtain secret information