Introduction to Security in Communication

Miroslav VOZNAK & Peppino FAZIO

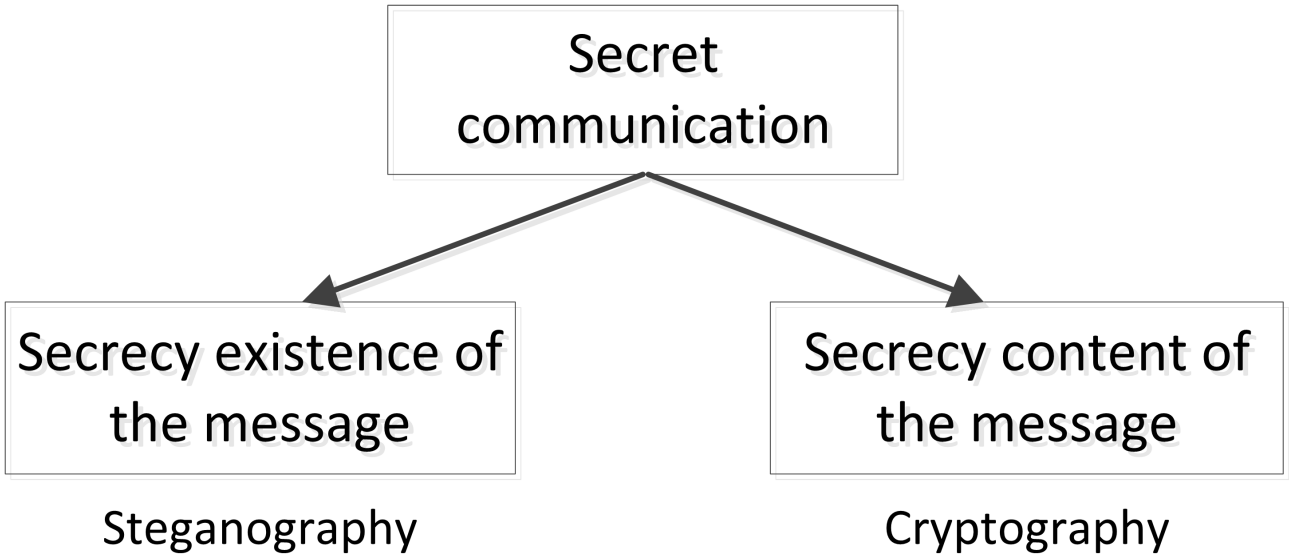
voznak@ieee.org

April 2016

Secret Communications

Since the ancient times, people need to hide some communication, message or the communication itself.

- **Steganography** conceals existence of the message, respectively existence of communication.
- **Cryptography** encrypts the content of the message so that the content of the message could not gain unauthorized person, and the plaintext was known only to the communicating sites.



Cryptology and Notation

Cryptology - branch of science covering cryptography and cryptoanalysis.

- **Cryptography** - design and construction of cryptographic algorithms.
- **Cryptoanalysis** - method of obtaining the plaintext without knowing the key and examines the robustness of cryptographic algorithms.

Notation

- **Plain text (PT)** - information in a readable form, being encrypted
- **Cipher Text (CT)** - the result of information after encryption
- **Encryption** - using encryption algorithm and key
- **Decryption** - getting plaintext from the ciphertext using decryption algorithm and key
- **Message**
- **Key** - the secret parameter of a cryptographic algorithm
- **Alice, BoB, Eva**

Steganography

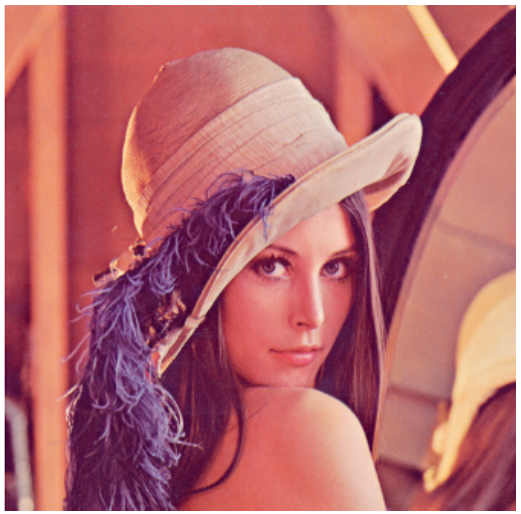
Example of ancient Greece: Shaving slave's head on which was written a message.

The method is derivate from the Greek words steganos (hidden) and graphein (to write).

- **Technical steganography** uses secrecy techniques such as invisible elements, hiding data or extreme reduction size of the message. Used in various forms today, e.g. microdots.
- **Linguistic steganography** uses a different form of notation, such as various positions in the text. To obtain a different form is necessary to have a grid with holes at these positions (Cardan grid).

Steganography

- Modern steganography realizes secret communication in the background of non-secret communication. Related area is watermarking, which is based on inserting additional information into the message or object and allows insert trademark.
- The basic requirement is reliable localization, extraction, secrecy, robustness, or immunity to alteration or removal trademark.



Obrázek: Source: USC-SIPI Image Database, University of Southern California

Goal of cryptography

The primary goal of cryptography is to keep the message content using encryption: Cipher, cryptographic, encryption algorithm, cryptosystem = mathematical procedure E(M)

Kerckhoffs's principle: The basic axiom draft of the cryptographic algorithm was formulated in 1883 by the Dutch linguist Auguste Kerckhoffs in the Journal of Military Science. **Security of a cryptographic system can not depend on secrecy of the algorithm, but only on secrecy of the key.**

Kerckhoffs determined basic axioms for the design of cryptosystem.

- only the key is secret
- cryptographic algorithms are not secret
- we have to assume that the attacker knows the principle encryption system

Cryptographic methodologies

Classical cryptography - substitution and transposition

- **Substitution** - replacing each symbol unencrypted messages to other symbol that remains in the same place as the original symbol
- **Transpositions** - rearrangements unencrypted message symbols in a selected way (e.g. permutations) which forming an encrypted message.

Some mathematical operations are easy in one direction, and the opposite direction are very difficult. With the number of operations required, calculation time grows. The difficulty of calculating provides mainly two basic approaches:

- **factorization** of large prime numbers
- a computation complexity of **discrete logarithms**.
- a new field is a **quantum cryptography**.

Modern Cpyptography

Objectives of modern cryptography

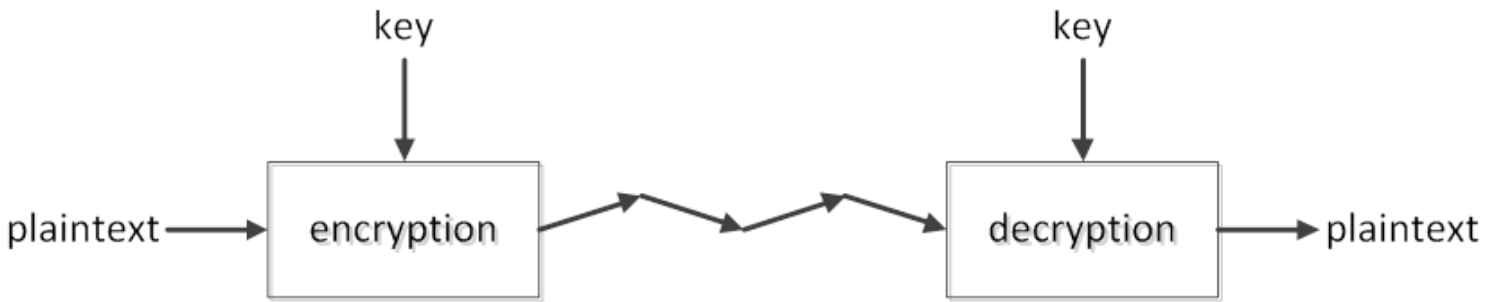
- **Confidentiality** - Keeping transmitted information in secret
- **Authentication** - verifying identity, i.e. verification that the communicating person is really "the one"with which we think we communicate
- **Authorization** - Confirm an origin of the data. The data was created by "the one"who we think is an author.
- **Non-repudiation** - ensures that the author of the data can not deny his authorship. Non-repudiation is related to authorization, eg. banking transactions is not disputed
- **Integrity** - relates to preventing unauthorized modification of data remains in the same place as the original symbol

Cryptosystem classification

- **codes**
- **steganography and watermarking**
- **symmetric and asymmetric ciphers**
- **hash function**
- **digital signatures**

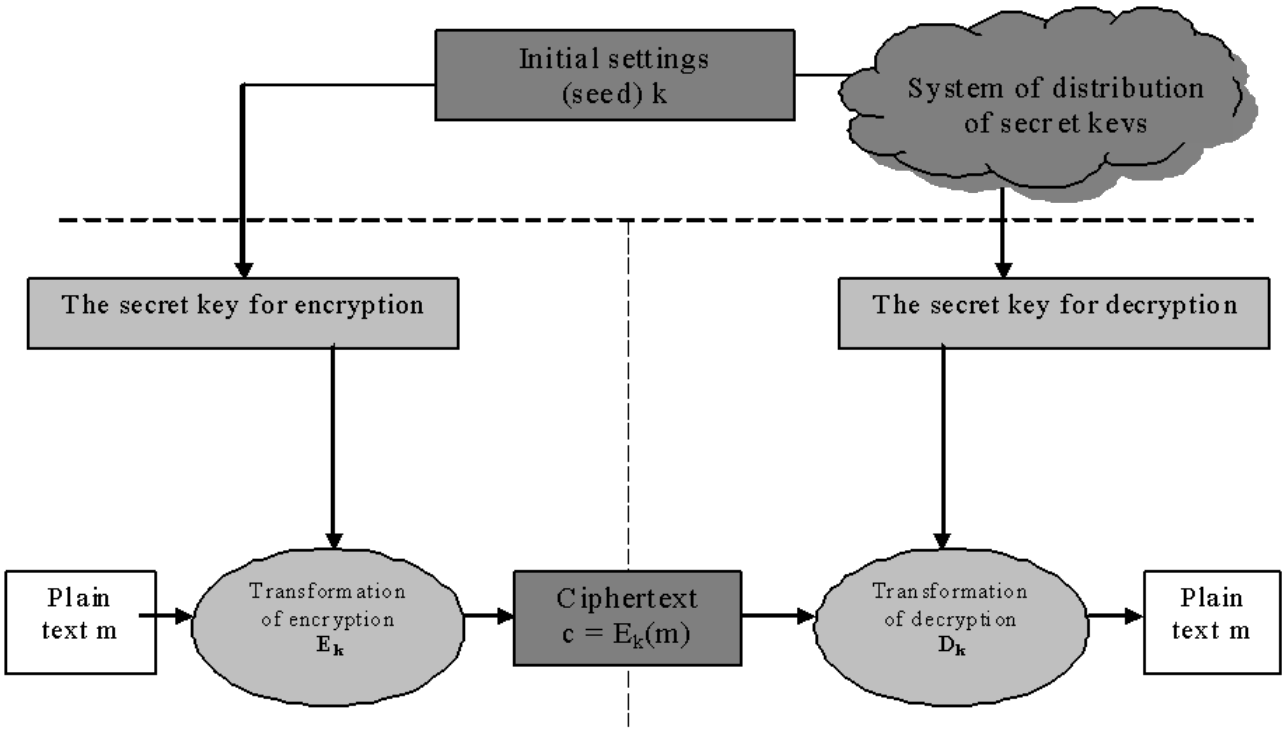
Mostly we use symmetric encryption and assymetric cryptography for key distribution.

$m \in M, k \in K$, Encryption = $C_k(m)$, Decryption = $D_k(C_k(m)) = m$.



Fundamentals of modern cryptography

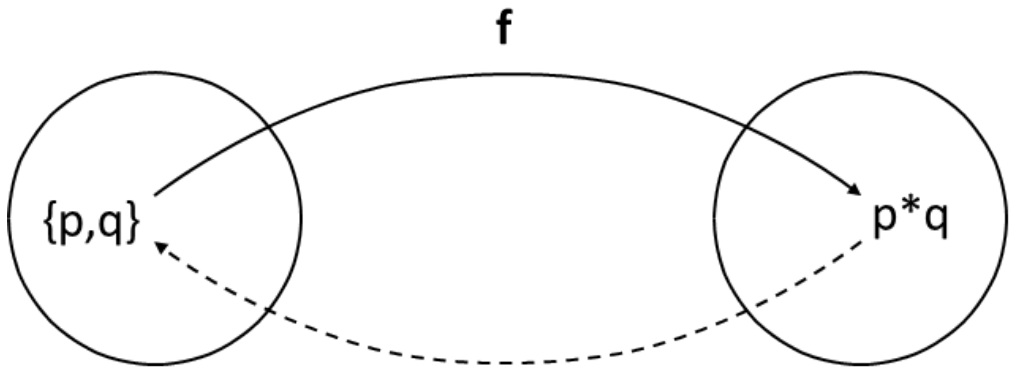
Symmetric encryption is very fast cca 1000 x faster than asymmetric , computationally efficient , DES - Data Encryption Standard (1976, IBM, NSA), the block cipher a word has fixed length (64 bits for DES, which only 56bits is used), 3DES, GOST 28147, RC4, IDEA, CAST-128, AES (Rijndael), **asymmetric encryption** - pivate and public keys (RSA, DSA, DH, ElGamal)



Fundamentals of modern cryptography

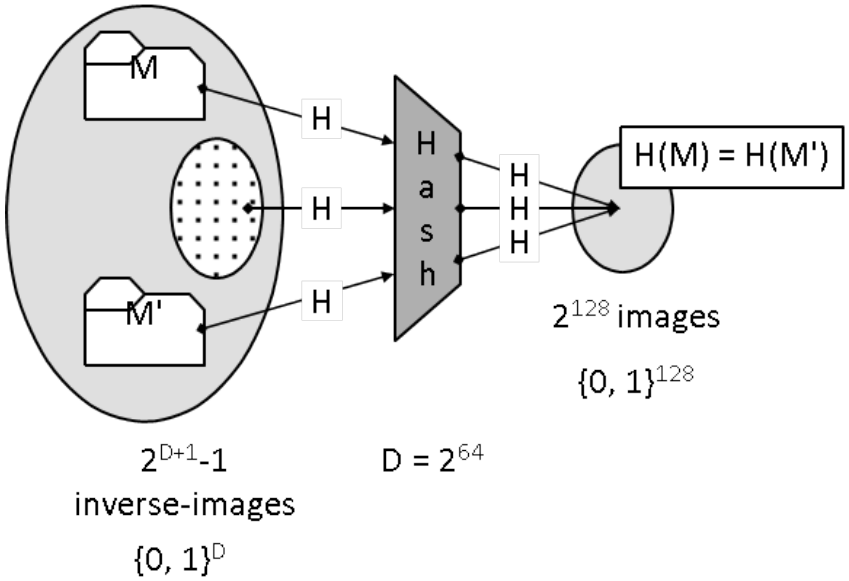
Hash functions is one-way and collisions-free function.

One-way function is a function f: X->Y, for which is to calculate y from any values of x from set X image y = f (x), but for any randomly selected image Y is impossible to find the pattern of X so that y = f (x). At the same time, we know that such pattern exists, but finding it is so computationally intensive that we consider impossible.



Fundamentals of modern cryptography

Hash functions collisions-free function as well. E.g. MD5 - there are so many possible messages $1 + 2^1 + ... + 2^D = 2^{D+1} - 1$ where $D = 2^{64} - 1$, which means a small number of hash codes. For MD5 there are only 2^{128}. It must therefore be a tremendous amount of messages, leading to the same hash code - on average it is of the order of 2^{D-127}. Collision therefore exists a tremendous amount. The point is that finding even a single collision is beyond our computational capability.



Euclidean algorithm

The best known method for efficient calculation of the greatest common factor of large numbers is Euclidean algorithm. The input of the algorithm are two natural numbers A and B. The algorithm at each step divides number A by number the B, if the remainder is not zero, then number B is assigned to the number A and division remainder is assigned to release variable B and the whole process repeats. If the remainder of the division is zero, then in the variable B is stored greatest common divisor of numbers A and B.

$$A = xB + remainder$$

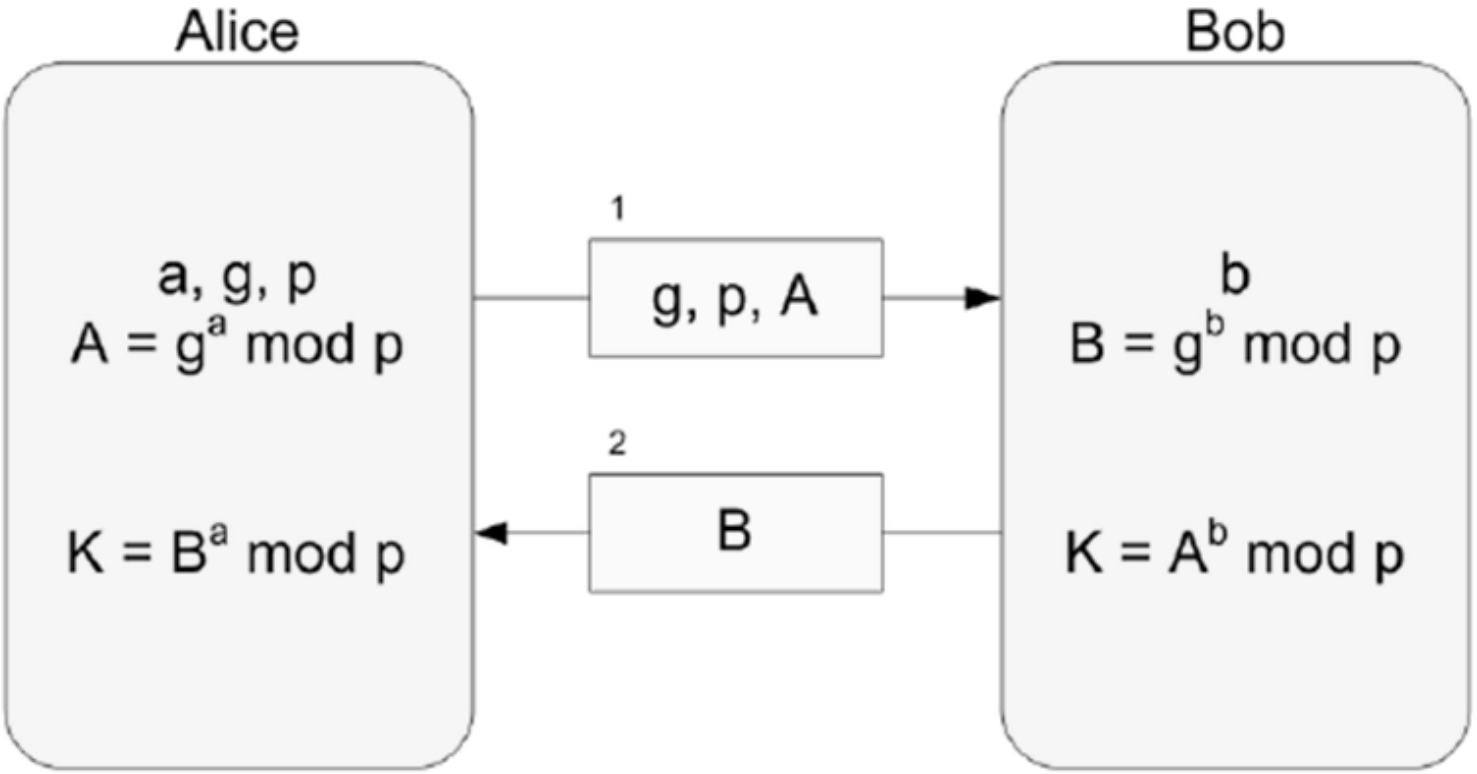
greatest common divisor (gcd) gcd (133,15) = ? , gcd (140,15) = ?
least common multiple (lcm) , lcm (140,15)=420

$$lcm(n1, n2) = \frac{n1\ n2}{gcd(n1, n2)}$$

Diffie - Hellman algorithm

- Algorithm was designed in 1976 by Diffie Witfield and Martin Hellman.
- It allows over an insecure communications channel between the parties to create an encrypted connection.
- Algorithm allows to create an encrypted key that can be used for subsequently encrypted communication.
- Using an algorithm can not verify the identity of communicating sites.

Diffie - Hellman algorithm



$$K = A^b mod\ p = (g^a mod\ p)^b mod\ p = g^{ab} mod\ p =$$
$$(g^b mod\ p)^a mod\ p = B^a mod\ p$$

Fermat's little theorem

For each p and $a \in Z$ not divisible by p, i.e. $gcd(a, p) = 1$

$$a^{p-1} \equiv 1 \ mod \ p$$

$$a^{p} \equiv a \ mod \ p$$

example: $3^{203} \ mod \ 101$

$$3^{100} \equiv 1 \ mod \ 101$$

$$3^{203} = 3^{100} 3^{100} 3^{3}$$

$$3^{203} \ mod \ 101 = (1 \cdot 1 \cdot 27) mod \ 101 = 27$$

Euler's theorem (also known as the Fermat–Euler theorem)

Euler's function $\Phi(n)$ is an arithmetic function that counts the positive integers ≥ 1 less than or equal to n that are not divisible by n.
If n is prime then

$$\Phi(n) = n - 1$$

Euler's function is a multiplicative function, if m and n are not divisble each other (are coprime), i.e.

$$\Phi(m \cdot n) = \Phi(m) \cdot \Phi(n)$$

.
If n is $k - th$ power of prime p then:

$$\Phi(n) = \Phi(p^k) = (p-1) \cdot p^{k-1}$$

.

Euler's theorem (also known as the Fermat–Euler theorem)

If p and q are coprime and $n \in Z$ then

$$n = p \cdot q, \Phi(n) = \Phi(p) \cdot \Phi(q) = (p-1) \cdot (q-1)$$

Euler's theorem may be used to easily reduce large powers $modulo\ n$. For each $n \in Z$, $n \geq 2$, each a and n which are coprime:

$$a^{\Phi(n)} \equiv 1\ mod\ n$$

RSA algorithm

In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. We choose two distinct prime numbers p and q so that $p \cdot q$ is higher then the highest encrypted number,

$$p = 3, q = 7$$

We compute **Modulus** n (n is used as the modulus for both the public and private keys)

$$n = p \cdot q, p = 3 \cdot 7 = 21$$

We choose an integer e such that $1 < e < \Phi(n)$, e and $\Phi(n)$ must be coprime.

$$\Phi(n) = (p-1) \cdot (q-1), \Phi = 2 \cdot 6 = 12$$

$e = 5$, the **public key exponent**

RSA algorithm

Decryption exponent d is kept as the **private key exponent**. We have to determine d from

$$e \cdot d \; mod \; \Phi = 1$$

$$e \cdot d = x \cdot \Phi + 1$$

complying

$$d = 17, x = 7$$

Public key $e = 5$, **modulus** $n = 21$, **Private key** $d = 17$.

RSA algorithm

Example:

Message M is plain text , $0 < M < (n-1)$,let's $M = 2$

$$C = M^e mod\ n$$

$$C = 2^5 mod\ 21 = 32\ mod\ 21 = 11$$

$$M = c^d mod\ n$$

$$M = 11^{17} mod\ 21 = 50544702849929377 1\ mod\ 21 = 2$$

Thank you for your attention

mailto:voznak@ieee.org