Network Security

• The security problems in the networks may be subdivided in four cathegories:

- **confidentiality**
- **authenticity**
- **non repudiation**
- **integrity**

• **confidentiality :** requires that information sent on the network only be accessible for reading to authorized parts.

• **authenticity:** requires that it is possible to verify the identity of the subjects involved in the communication.

• **non repudiation** : requires that it is impossible to repudiate the sending of a message.

• **integrity :** requires that the received message **is** the same respect to that sent.

Types of threats

a)Sniffing (snooping)

• A **packet sniffer** is a software that is able to capture each packet flowing in the network and, if needed, to decode and to analyze its content.

• Attack to the data **confidentiality**.

• **Use of criptography techniques** (VPN)

b)Address spoofing

• **IP spoofing** refers to the creation of IP packets with a forged source IP address, called **spoofing**, with the purpose of concealing the identity of the sender or impersonating another computing system.

• The machine that receives spoofed packets will send response back to the forged source address, which means that this technique is mainly used when the attacker does not care about the response.

•

Denial of service

• A **denial-of-service attack** (**DoS attack**) or **distributed denial-of-service attack** (**DDoS attack**) is an attempt to make a computer resource unavailable to its intended users.

• It consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely.

.

Example: TCP SYN flood attack

• When a client attempts to start a TCP connection to a server, the client and server exchange a series of messages (TCP three way handsake)

.

• The client requests a connection by sending a SYN (*synchronize*) message to the server.
The server *acknowledges* this request by sending SYN-ACK back to the client.
The client responds with an ACK, and the connection is established.

.

• In case of attack a malicious client can skip sending the SYN ACK message. The server will wait for the acknowledgement for some time, as simple network congestion could also be the cause of the missing ACK.

•If these *half open connections* bind resources on the server, it may be possible to take up all these resources **by flooding the server with SYN messages**. Once all resources set aside for half-open connections are reserved, no new connections (legitimate or not) can be made, resulting in denial of service .

Trojan Horse

• A **Trojan**, (**Trojan horse)**, is a program that appears to perform a desirable function for the user but instead facilitates unauthorized access to the user's computer system.

• Trojan horses are designed to allow a hacker **remote access** to a target computer system. Once a Trojan horse has been installed on a target computer system, it is possible for a hacker to access it remotely and perform various operations.

•Examples: attacks of spamming, DDoS, Data theft (e.g. passwords, credit card information, etc.),Installation of software (including other malware) ,Downloading-uploading of files ,modification or deletion of files, keystroke logging,..

Backdoor

• A **backdoor** is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected.

•A backdoor can be designed during the development or maintenance phases of a program to allow the direct acces to the code or it may be derived by errors in designing or coding a program.

Attack to a DNS server

• Attack to the data integrity or to the service availability.

• Attack based on backdoor techniques: modification of the data-base containing the corrispondence among logical and binary addresses

•DOS attack: the server is not accessible by the network nodes

.

Cryptology

•**Cryptography**: design and development of cryptographic systems.
A plaintext is converted into apparently random non sense, referred to as encrypted text

•**Cryptanalys:** The process of attempting to decrypt the encrypted text.

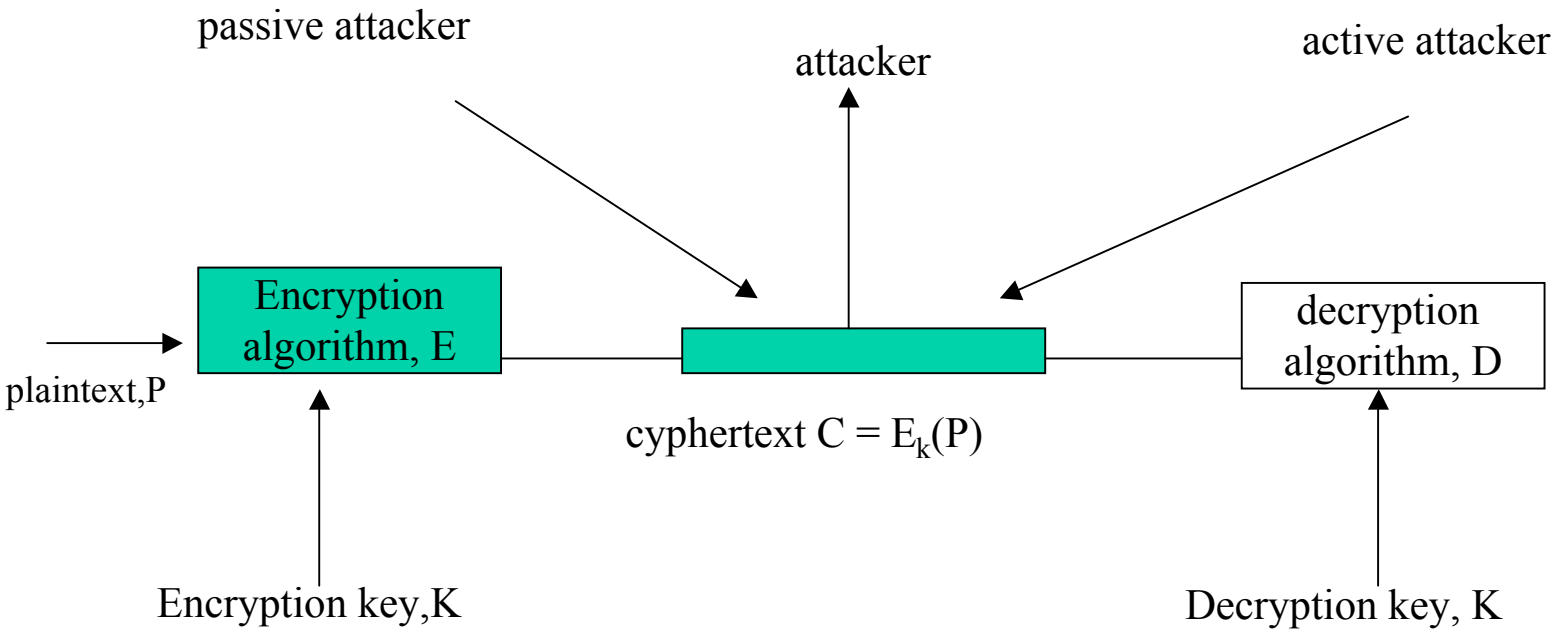
Conventional Encryption Model

• The encryption process consists of an **algorithm and a key**

• The key is a value indipendent of the plaintext. The algorithm will produce a different output depending on the specific key being used at the time. Changing the key changes the output of the algorithm.

•The security of conventional encryption depends on the **secrecy of the key**, not the secrecy of the algorithm.

•The fact that the algorithm need not to be kept secret means that manufactures can and have developed low- cost chip implementation of data encryption algorithms.


passive attacker
attacker
active attacker
Encryption algorithm, E
decryption algorithm, D
plaintext,P
cyphertext C = $E_k(P)$
Encryption key,K
Decryption key, K

$D_K(E_K(P))=P$

• **E, D** are mathematical functions named **encryption algorithms or decryption algorithms**. **The algorithms**, generally, are **public** and well known. **The secret is the key.**

• While the alghorithm always operare the same way, a different key used on the same plaintext will produces different ciphertext.

• **A cryptographic key** is a string used to characterize a known algorithm.

.

- It is foundamental that the algorithm is public.

- A cryptographyc system based on a secret algorithm presents serious drawbacks. In fact, it is necessary to change it everytime the danger exists that it is no more unknown.

- Instead, a key may be easily modified.

.

- The basic model of a cryptographic system is constituted. of a solid, well known algorithm and a fixed size or variable size “strong key” .

Criptography

Criptographic systems are generally classified along three independent dimensions:

•**The type of operations used for transforming plaintext to ciphertext**.

All encryption algorithms are based on two general principles: **substitution**, in which each element in the plaintext (bit, letter, group of bit or letters) is mapped into another element, and **transposition,** in which elements in the plaintext are rearranged.

Most systems, referred to as **product systems**, involve multiple stages of subsitution and transposition.

•The number of keys used

If both sender and receiver use the same key, the system is referred to as symmetric, single key, secret key or conventional encryption.

If the sender and the receiver each use a different key, the system is referred to as asymmetric, two key, or public key encription.

•The way in which the plaintext is processed.

A **block cypher** processes the input one *block of elements* at a time, producing an output block for *each input block*.

A **stream cypher** processes the input elements continously, producing output one element at a time, as it goes along.

Cryptanalysis

• **brute force attack** is a strategy used to break the encryption of data.

•It involves traversing the search space of all possible keys until the correct key is found.

•The resources required for a brute force attack scale exponentially with encreasing key size, not linearly. As a result, doubling the key size for an algorithm does not simply double the required number of operations but rather squares them.

•Although there are algoritms which use 56-bit symmetric keys (e.g. Data Encryption standard),usually 128-256 bit keys are standard. .

• If some words in the encrypted text are known, the decryption is simplified

- in english language **e** is the most common letter, followed by **t,o,a,n,i**,etc..

- two letters (digrams) more common: **th, in, er,re,an**.

- Three letters (**trigrams**) more common: **the,ing, and, ion**

•The relative frequency of the letters of the encrypted text is evaluated; to the letter with higher frequency the **e** letter is associated, then the letter **t** etc..
•If there are trigrams of the form **tXe** the letter X is substituted by **h,** ec..

Average time required for exhaustive key search

keys size (bits)	number of altenative keys	time required at 10^6 decript/sec
32	$2^{32} = 4.3 \times 10^9$	2.15 msec
56	$2^{56} = 7.2 \times 10^{16}$	10 hours
128	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	5.9×10^{30} years

Computationally secure encryption scheme

- The cost of breaking the cipher exceeds the value of the encrypted information.
- The time required to break the cipher exceeds the useful lifetime of the information.

•The criptographic methods are subdivided in two cathegories:

- **Transposition technique**
- **Substitution technique**

In a **transposition technique** the units of the plaintext ((single letters, pairs of letters,..) are rearranged in a different and usually quite complex order, but the units themselves are left unchanged.

•In a **substitution technique**, the units of the plaintext are retained in the same sequence in the cybertext, but the units themselves are altered.

Substitution technique

- **Caesar cipher**

  each letter of the alphabet in the plaintext is replaced with the letter standing three places further down the alphabet.

For instance,

plaintext:	de bello gallico
encrypted text:	gh ehoor ldoonfr

A⇔D, B⇔E, C⇔F…Z⇔C

- Note that the alphabet is wrappep around, so that the letter following Z is A. We can define the trasformation by listing all possibilities, as follows:

plain: a b c d e f g h i j k l m n o p q r s t u v w x y z
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

- If we assign a numerical equivalent to each letter (a=1,b=2,..) for each plaintext letter p, substitute the letter C

$$C=E(p)=(p+3)\bmod 26$$

•A shift may be of any amount, so that the general Caesar algorithm is:

$$C=E(p)=(p+k)\text{mod}(26)$$

where k takes on a value in the range 1 to 25.

• The decryption algorithm is

$$P=D(C)=(C-k)\ \text{mod}(26)$$

• There are only 25 possible keys

Monoalfabetic Ciphers

• Each character in the plaintext is replaced by an another character (arbitrary substitution).

plaintext: : a b c d e f g h i j l m n o p q r s t u v w x y z
cipher line: Q W E R T Y U I O PR S T U V W X Y Z X C V B N M

• The cipher line can be any permutation of the 26 alphabetic characters, then there are 26! ($4x10^{26}$ **) possible keys.**

•However, if the cryptanalyst knows the nature of the plaintext (e.g. non compressed english text) then the analist can exploit the regularities of the language (relative frequence of the letters,frequence of two letter combination,..)

- in english language **e** is the most common letter, followed by**t,o,a,n,i**,etc..

- Two letters (digrams) more common: **th, in, er,re,an**.

- Three letters (**trigrams**) more common: **the,ing, and,e ion**

•The relative frequency of the letters of the encrypted text is evaluated; to the letter with higher frequency the **e** letter is associated, then the letter **t** etc..
•If there are trigrams of the form **tXe** the letter X is substituted by **h,** ec..

Transposition Techniques

•Columnar transposition

M E G A B U C K → **key** (no duplicated letters)
7 4 5 1 2 8 3 6 → numerical position in the alphabet
p l e a s e t r
a n s f e r o n
e m i l l i o n …
d o l l a r s t
O m y s w i s s
…….

plaintext: pleasetransferonemilliondollarstomyswiss…
Testo cifrato:
AFLLSKSOSELAWAIATOOSSCTCLNMOMANTESILYNT..

The encrypted text is read by columns beginning from the column with lowest key letter.

Even in this case the statistical properties of the language may be usec to facilitate the work of a cryptoanalyst.

monouse blocks

a) **Key:** random generated string of bit

b) The plain text is converted ia string of bit using, ad example, the ASCII representation for the characthers.

c)XOR of the two strings is evaluated.

• The encrypted text cannot be decrypted independently tenrisultante **non può essere forzato** indipendentemente da quanta potenza di calcolo si utilizzi.

• The encrypted message does not contain any information because all the possible plaintext with the same probability are contained in it

•**Example**

Message “i love you” is converted using a 7 bit ASCII code

Message :

1001001 0100000 1101100 1101111 1110110 1100101 0100000 1111001 1101111 1110101 0101110

Monouse block:

1010010 1001011 1110010 1010101 1010010 1100011 0001011 0101010 1010111 1100110 0101011

Encrypted text

0011011 1101011 0011110 0111010 0110100 0000110 0101011 1010011 0111000 0010011 0000101

•To decrypt the message all the possible monouse blocks can be used in order to examine the corresponding plaintexts. It is possible to find more acceptable plaintexts.

•. **There is no information on the encrypted text.**

Monouse blocks:problems

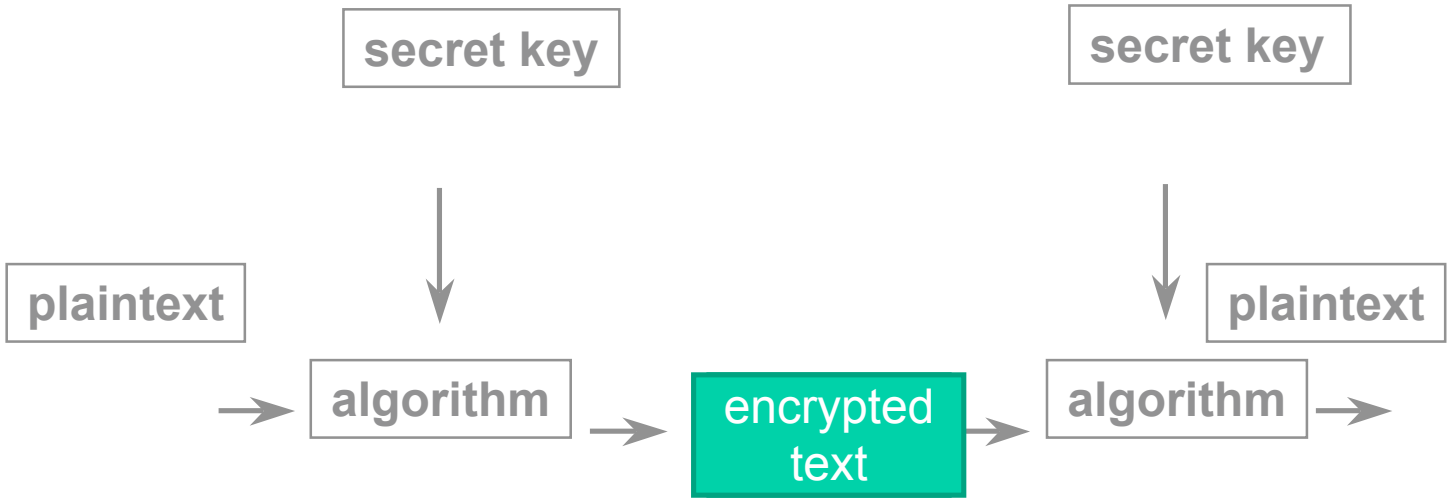
• Sender and receiver must know a copy of the key (network transmission).

• The amount of sent data is limited by the key length.

•Per una trasmissione sicura in rete si può ricorrere alla **crittografia quantistica.** Soluzione ancora sperimentale.

•Si basa sul fatto che la luce viene trasportata in piccoli pacchetti detti fotoni e che può essere polarizzata facendola passare attraverso filtri polarizzatori.

Symmetric key algorithms



Two types

- A **block cypher** processes the input one block of elements at a time, producing an output block for each input block.
- A **stream cypher** processes the input elements continously, producing output one element at a time, as it goes along.

DES (Data Encryption Standard)

- Adopted in 1977 by the National Bureau of Standards as Federal Information Processing Standard.
- DES encrypts 64-bit blocks and uses a key 56 bits; longer blocks of plaintext are encrypted in blocks of 64 bits
- DES processes plaintext by passing each 64-bit input through 16 iterations, producing an intermediate 64-bit value at the end of each iteration. Each iteration is essentially the same complex function that involves a permutation of the bits and substituting one bit pattern for another. The input at each stage consists of the output of the previous stage plus a permutation on the key bits , where the permutation is known as a subkey.
- DES utilizes logical and arithmetic operations that can be easily hardware implemented.

The strength of DES

- There was some criticism from various parties about a shortened key length and the mysterious evidence of improper interference from the NSA. The suspicion was that the algorithm had been covertly weakened by the intelligence agency so that they — but no-one else — could easily read encrypted messages.
- January, 1999, distributed .net and the Electronic Frontier Foundation collaborated to publicly break a DES key in 22 hours and 15 minutes using a special purpose “DES cracker” machine that was built for less than $ 250,000.
- Hardware prices will continue to drop as speed increase, making DES worthless.
- Fortunately, there are a number of alternative available in the marketplace.

Triple DEA

- Given the potential vulnerability of DES to a brute force attack, there has been considerable interst in finding an alternative.
- One approach, which preserves the existing investment in software and equipment, is to use multiple encription with DES and multiple keys.
- Triple DEA (TDEA) usese three keys and three executions of the DES algorithm (168-bit key length)

Symmetric algorithms

- CAST
- IDEA (128-bit key)
- RC2, RC4, RC5 (key length variable);
- SKIPJACK (80-bit key);
- GOST(256 bit-key)

Symmetric encryption problems

- Key distribution
- Source authentication and non repudiation

Key distribution

- For symmetric encryption technique to work, the two parties to an exchange must share the same key, and that key must be protected from access by others.
- Key distribution technique:

  -A key can be selected by A and phisically delivered to B

  - A third part can select the key and phisically deliver it to A and B

  - If A and B each has an encrypted connection to a third party C, C can deliver a Key on the encrypted links to A and B (**KDC, Key Distribution Center**)

• In a distributed system, any given host may need to engage in exchanges with many others hosts over time. Thus, each host needs a number of keys supplied dynamically.

• Thus, if there are N hosts the number of required keys is N(N-1)/2.

• A network using node-level encryption with 1000 nodes would need to distribute as many as half a million keys. If the same network supported 10000 applications, then 50 milion keys may be required for application level encryption.

Public key encryption

•The encryption technique assign each user a **pair of keys**. One of the user's keys, called the **private key**, is kept secret, while the other, called the **public key**, is published along the name of the user, so everyone knows the value of the key.

•The cryptographic algorithm has the mathematical property that a message encrypted with the public key can be decrypted only with the relative private key.

•It is computationally infeasible to determine the decryption key given only knowledge of the cryptographic algorithm and the encryption key.

The essential steps for sending an encrypted message :

• Each user generates a pair of keys to be used for the encryption and decryption of messages.

• Each user places one of the two keys in a public register or other accessible file (public key). The other key is private.

• If Bob wishes to send a private message to Alice, Bob encrypts the message using Alice's public key.

• When Alice receives the message, she decrypts it using her private key. No other recipient can decrypt the message because only Alice knows Alice's private key.

Authentication

• Suppose that Bob wants to send a message to Alice and, although it is not important that the message be kept secret, he wants Alice be certain that the message is indeed from him.

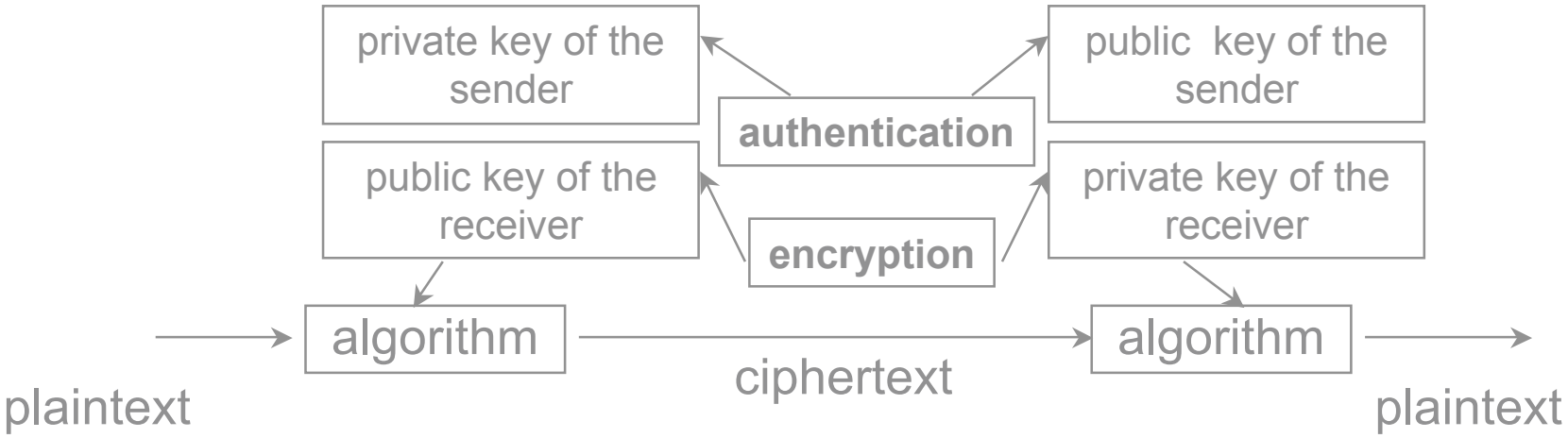
• Bob uses his own private key to encrypt the message. When Alice receive the ciphertext, she finds that she can decrypt it with Bob' public Key, thus proving that the message must have been encrypted by Bob.

• No one else has Bob' private key and therefore no one else could have created a cyphertext that could be decrypted with Bob's public key.

Confidentiality and Authenticity

- Two levels of encryption can be used to guarantee that a message is both authentic and confidential.
- First the message is encrypted by using the sender private key. Second, the encrypted message is encrypted again using the recipient's public key.
- At the receiving end, the decription process is the reverse of the encryption process.
- First the receiver ueses his private key to decrypt the message.Second, the recipient uses the sender's public key to decrypt the message again.

Public key Encryption



RSA

- Rivest, Shamir, Adleman. MIT (1978)

- Keys of at least 1024 bit are required in order to obtain a good seurity. The algorithm is computationally complex . It is based on the properties of prime numbers.

- It is the only widely accepted and implemented general purpose approach to public key encryption.

.

The public key and private key generation

1.Choose two distinct **prime numbers** p,q (at random and of similar bit - length)

2. Compute n=pxq

3. Compute f(n)= (p-1)(q-1)

4.Choose an integer **e** such that 1<e<f(n) and e , f are coprime

5. Determine d= 1/e (mod f(n))

The public key consists of the modulus n and public exponent e
The private key consists of the private exponent d which must be kept secret.

•The message M is trasformed into an integer $0<m<n$ by using a padding scheme.

•Encryption

$$C = m^e \bmod n$$

•Decryption

$$m = C^d \bmod n$$

•Note that, although **n** is publicly known**, p** and **q** are not. This condition is allowed because, as is well known, it is difficult to factor **n.** Consequently, the integers **d** and **e** cannot be guessed easily.

Example.
p=5 and **q**=7. Then **n**=35 and (**p**-1)x(**q**-1)=24

e =11 is relative prime to 24

Suppose that **m**=3, we have:

$$C = \mathbf{m}^{e} \bmod \mathbf{n} = 3^{11} \bmod 35 = 12$$

and

$$C^{d} \bmod \mathbf{n} = 12^{11} \bmod 35 = 3 = m$$

Then if we encode **m** using **e**, we can decode **m** using **d.**

- To factor a number n means to find a set of numbers such that their product is the number
- There are different kinds of factorization. 24=2x12=2x3x4=3x8..
- Prime numbers factorization : looking for a set of factors of the number n that are prime numbers.
- Each natural number has one and only one prime numbers factorization .

In 2005 a number of 640 bits (193 decimal numbers) has been decomposed into two 320 bits prime numbers by using an Opteron cluster with 80 processors (2.2 GHZ)during a 5 months period of time .

RSA

• pair of keys for each user

$$(K_{\mathbf{pub}},K_{\mathbf{priv}})_{\mathbf{A}}$$

$$(K_{\mathbf{pub}},K_{\mathbf{priv}})_{\mathbf{B}}$$

•Key properties:

- A message encrypted with one of the two keys is decryptable only with the other
- Known one the two keys (public) is impossible to obtain the other (private)

Performance:

- RSA in **hardware**: is about 1000 times slower than DES
- RSA in **software:** is about 100 times slower than DES

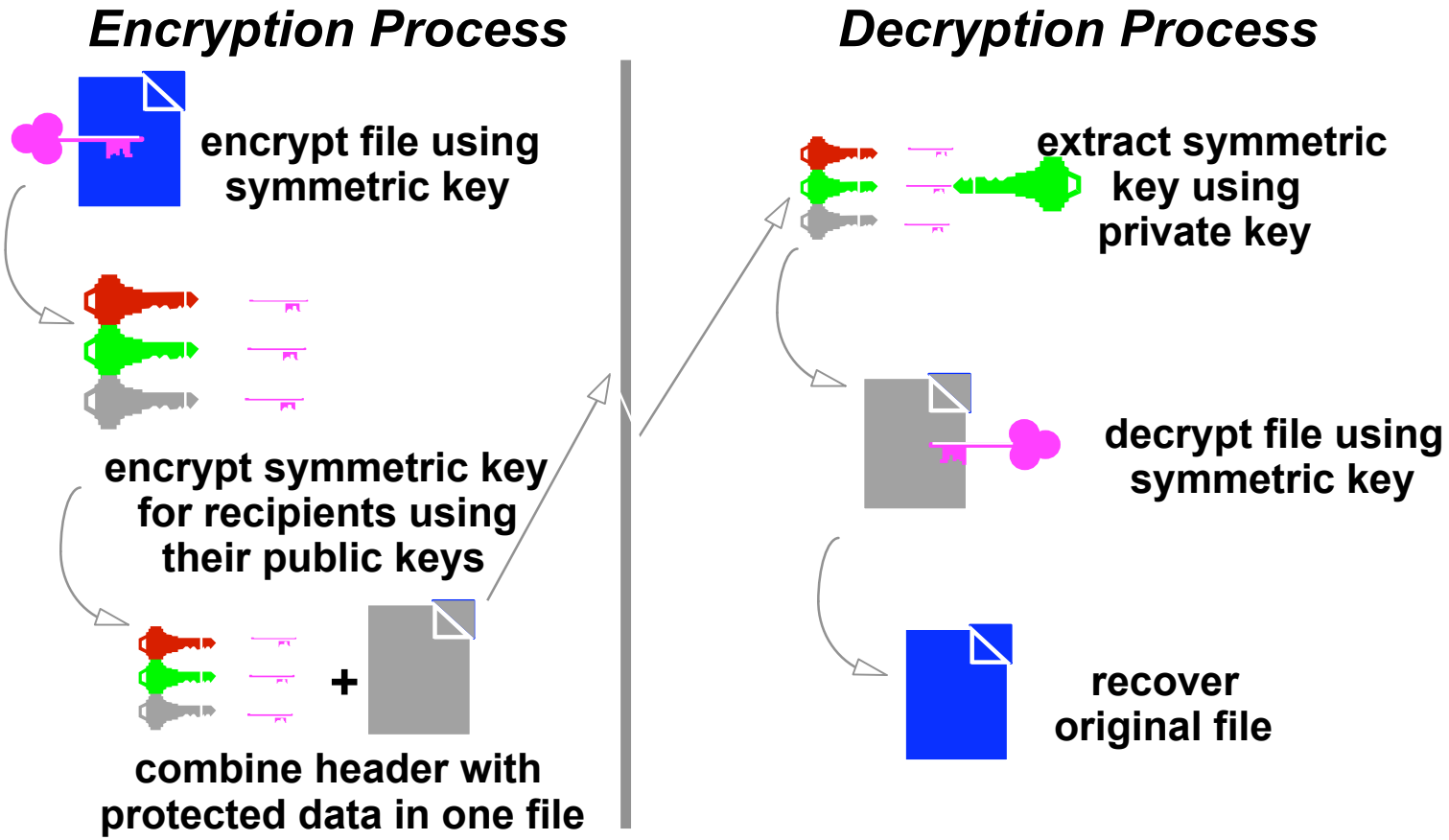
Comunication confidentiality of public key systems

Problemes:

- **the public key algorithms are computationally complex**
- **the protocol does not provide source authentication.**
- How is possible that Alice be sure that the public key found in the database actually belongs to Bob?

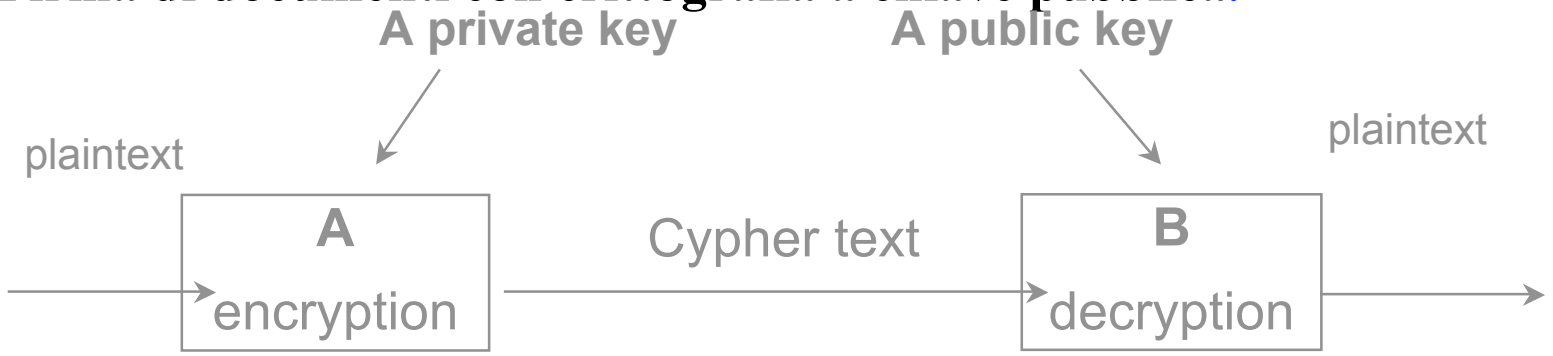
Key authenticity problem => solution= the assurance scheme is improved in terms of scalability and security when it is based on the trust in a third party (**CA, Certification Authority**) that ensures the integrity and the authenticity of the public key stored in the database

Distribution of symmetric keys using public-key techniques



Digital signature

Firma di documenti con crittografia a chiave pubblica:



- The public key algorithms do not provide good performances in the signature of high dimension documents.
- To improve the perfomance in implementing the digital signature **hash functions** are introduced.

Hash Functions

- A hash value is generated by a function H of the form

$$h=H(M)$$

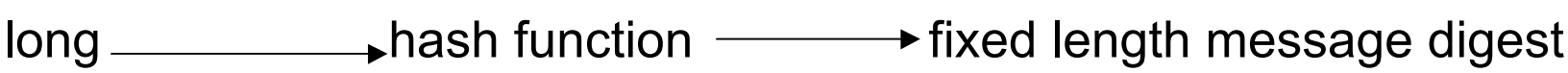
where M is a variable-length message and H(M) is the fixed-length hash value.

- The purpose of a hash function is to produce a “ digest” of a file, message or other block of data.

Requirements for a hash function:

- H can be applied to a block of data of any size.
- H produces a fixed -length output
- **H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical.**
- **For any given code h, it is computationally infeasible to find x such that H(x)=h (one- way property)**
- **For any given block x, it is computationally infeasible to find y=x with H(y)=H(x). This is sometimes referred to as a weak collision resistance.**

It is computationally infeasible to find any pair (x,y) such that H(x)= H(Y). This is sometimes referred to as strong collision resistance.



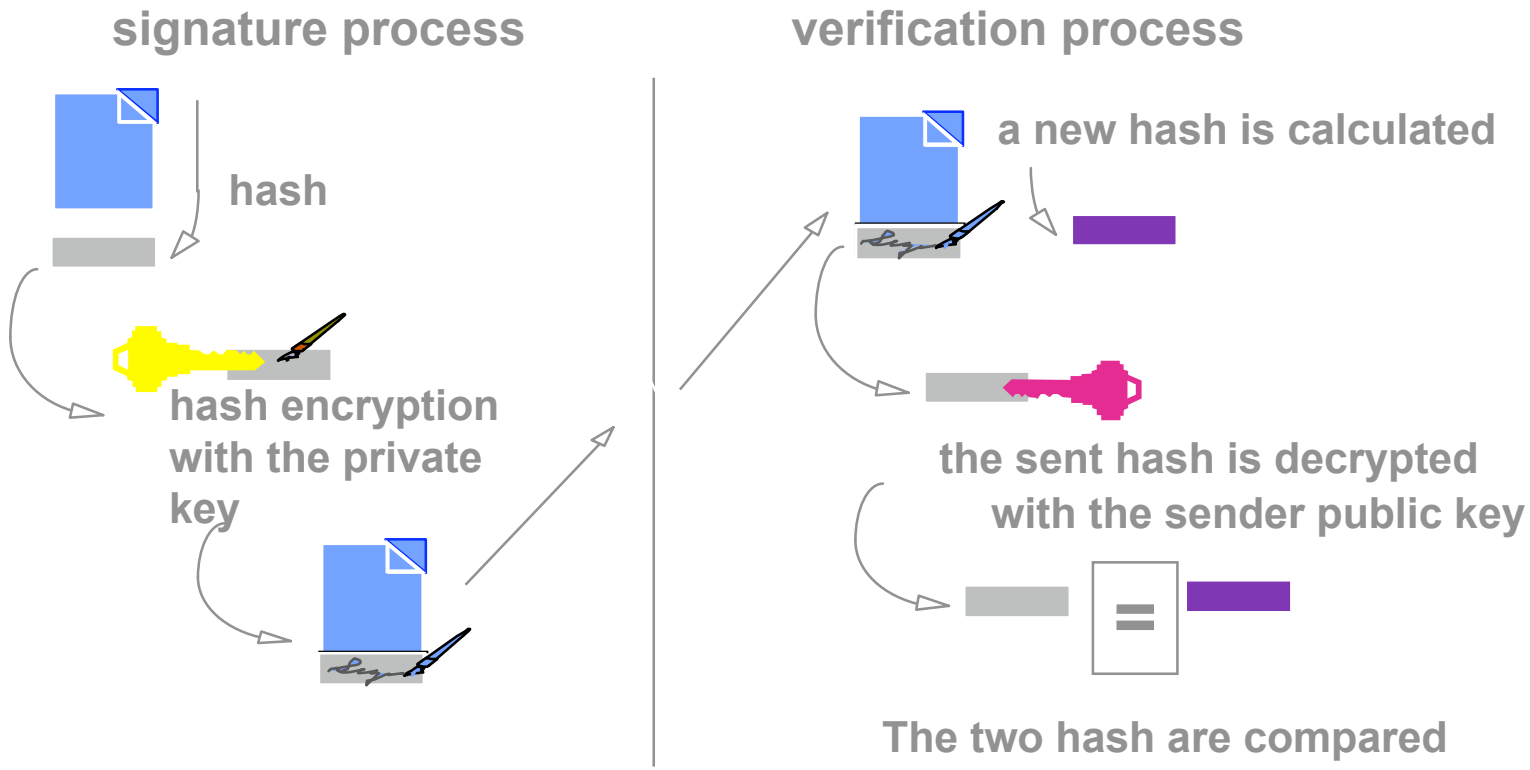
Examples:

• **MD5 Algorithm** di Ron Rivest (RFC1321)
produces a 128 bit digest

• **SHA-1 Algorithm** (Secure Hash Algorithm)
federal standard (USA)
produces a 160 bit digest

Digital Signature

Digital signature obtained using public key criptography and one-way hash functions



- Security may be provided in each of the following levels:

- **Application level**. The security is provided for a specific protocol of the application level, The applications that use the protocol will receive security services as confidentiality,authentication and integrity(ex. PGP e-mail)

- **Transport level**. All the applications that use the transport level protocol will receive the security services of the protocol (ex. SSL)

- **Network level**. When the security isprovided to network level from host to host, all the packets of the transport level (and then all the data of the application level) will receive the security services of the network level. Moreover is possible the authentication of IP addresses.