

Université de Genève
SES - Département des Systèmes d'Information

Dimitri Konstantas

Introduction to Computing Security

Références :

Charles P. Pfleeger, *Security in Computing*, Prentice Hall 1989.

Introduction to Computing Security

Security against what?

- ❑ ***Interruption***

A system becomes lost or unavailable or unusable.
Ex. erasure of a file, malicious destruction of a device.

- ❑ ***Interception***

An unauthorized party gains access to an asset.
Ex. Illicit copying of program or data files, wiretapping.

- ❑ ***Modification***

A party not only access but tampers with an asset.
Ex. modification of files, program alteration.

- ❑ ***Fabrication***

An unauthorized party fabricates counterfeit objects.
Ex. adding records to a database, send messages posing for someone else.

Computer security consists of maintaining all of the following:

- ❑ ***Secrecy***

Only authorized parties can access the assets.

- ❑ ***Integrity***

Only authorized parties can modify the data.

- ❑ ***Availability***

Assets are available to authorized parties.

Ex. A system can preserve perfect secrecy and integrity by preventing everyone from accessing a particular object!

Vulnerabilities of computing systems

❑ Attacks on Hardware

- Accidental damage (spilling coffee to the hardware)
- Malicious destruction
- Theft

❑ Attacks on Software

- Software deletion
- Software Modification
 - Updates
 - Viruses
 - Logic bombs
 - Trojan Horses, trapdoor
 - Information leakages
- Software theft

❑ ***Attacks on Data***

- Secrecy breach
 - wire tapping
 - bugs in output devices
 - bribing key employees
 - inferring one data point from other values)
- Data modification
 - Requires more sophistication than simple secrecy breach.
 - Modifying interest rates
 - Message replying

- ❑ Other exposed assets
 - Storage media
 - Networks
 - Access to computing equipment
 - Key people

Who is the attacker

The identity and personality of the “computer criminal” can not be defined. It can anybody, from your kid playing at night to the high executive of a bank.

The motives can range from a simple game up to serious criminal activity.

The results can be negligible (some computing time used) up to costs of millions.

Who is the person most likely to attack your system

- ❑ Amateurs

The most active class! Can start as a small game and end up in using a foreign computer for running a company!

- ❑ Computer addicts

The most repudiated class (*hackers, crackers, whiz kids*)
Networks of “secrets of success” (ex. Warez)

- ❑ Carrier Criminals

The most sophisticated class.
Sometimes they are untouchable and highly paid!

Defense methods

- ❑ Encryption
 - Data secrecy
 - Data integrity (cannot be read, cannot be modified!)
 - Availability (encryption in protocols that verify the access rights of the user)
- ❑ Software controls
 - Development controls (standards for the design of secure and safe software)
 - Operating system controls (the OS must be in a consistent state to ensure certain security levels)
 - Internal program controls (enforcing security restrictions)
- ❑ Hardware controls
 - Encryption hardware

- ❑ Company policies
 - Procedures to enforce and control the system security (ex. frequent change of passwords, copying control)
- ❑ Physical means
 - Lock the door before leaving!
 - Backup important data and keep a copy in a *secure* place
 - Anticipate physical destruction (fire, flooding ...)
- ❑ Passing the message
 - Making the personnel believe that security is important
 - Do not rely on a single check point control (the system is as strong as is weakest part)

Encryption and decryption

Encryption is the process of encoding a message :: **E**

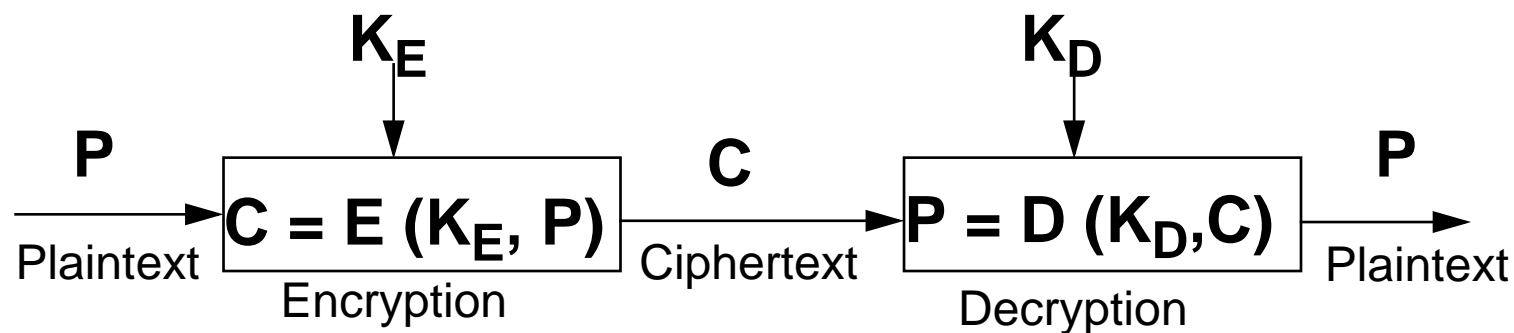
Decryption is the reverse process : transforming an encrypted message to its normal form :: **D**

Plaintext is the original message :: **P**

Ciphertext is the encrypted message :: **C**

A **Key** is a value used in the encryption of the message :: **K_E, K_D**

We have single key ($K_D = K_E$) and two-key ($K_E \neq K_D$) systems



Cryptography is the practice of using encryption to conceal text.

Cryptanalysis is the process of breaking the encryption.

How cryptanalysis works

- ❑ Attempt to break a single message
- ❑ Attempt to recognize patterns in encrypted messages in order to be able to break subsequent ones
- ❑ Attempt to find general weaknesses in an encryption algorithm

What is a breakable encryption

An encryption might be breakable, given enough time and data!
Practically however things are different.

A cipher scheme might require 10^{30} operations.

Current technology computers perform 10^{10} operations/sec.

We thus need 10^{20} secs or 10^{12} years!!

However:

- An ingenious approach might require 10^{15} operations, resulting in a computation of roughly one day.
- The technology evolves very fast!

How does encryption works

Most encryption algorithms are mathematical in nature or can be explained and studied with mathematics.

Text symbols are coded with numbers and the encryption operates on the numerical representation of the symbols (ex. ASCII codes).

Substitution ciphers

Monoalphabetic ciphers (simple substitution)

Exchange one letter for another (using a single alphabet).

- Ceasar's cipher.

Cryptanalysis of monoalphabetic ciphers:

At face value monoalphabetic ciphers require 26! decipherments. However using statistical text analysis (frequency of the appearance of letters in the language) deciphering becomes very easy.

Polyalphabetic substitution ciphers.

Basic idea is to eliminate the distribution frequency of the underlying alphabet, by encoding the message using more than one alphabets.

Example using two alphabets:

For the odd position letters we use one substitution alphabet while for the even position letters we use a second alphabet.

Cryptanalysis of a polyalphabetic substitution cipher:

Using repeated patterns in the ciphertext for the given language. (ex. word endings -ing, frequently used words and phrases it was the etc.)

The perfect substitution cipher.

Eliminate repeated patterns.

This can be done by using an unlimited number of alphabets.

The Vernam Cipher.

The basic idea is to use a long list of non repeating random numbers and encrypt the text letters using this list (first letter with first random number, second letter with second random number, etc.).

Cryptanalysis of Vernam's Cipher:

It is based on a random number generator. In computer systems the algorithms for random number generators are more or less known.

Using other lists of “random numbers” makes it more difficult to break (telephone directories, books etc.)

Permutation (transposition) ciphers

The goal of permutation ciphers is to break repeating patterns by rearranging the position of letters.

Columnar transposition is the rearrangement of the plaintext characters in columns and reading the ciphertext in the rows.

Cryptanalysis of permutation ciphers:

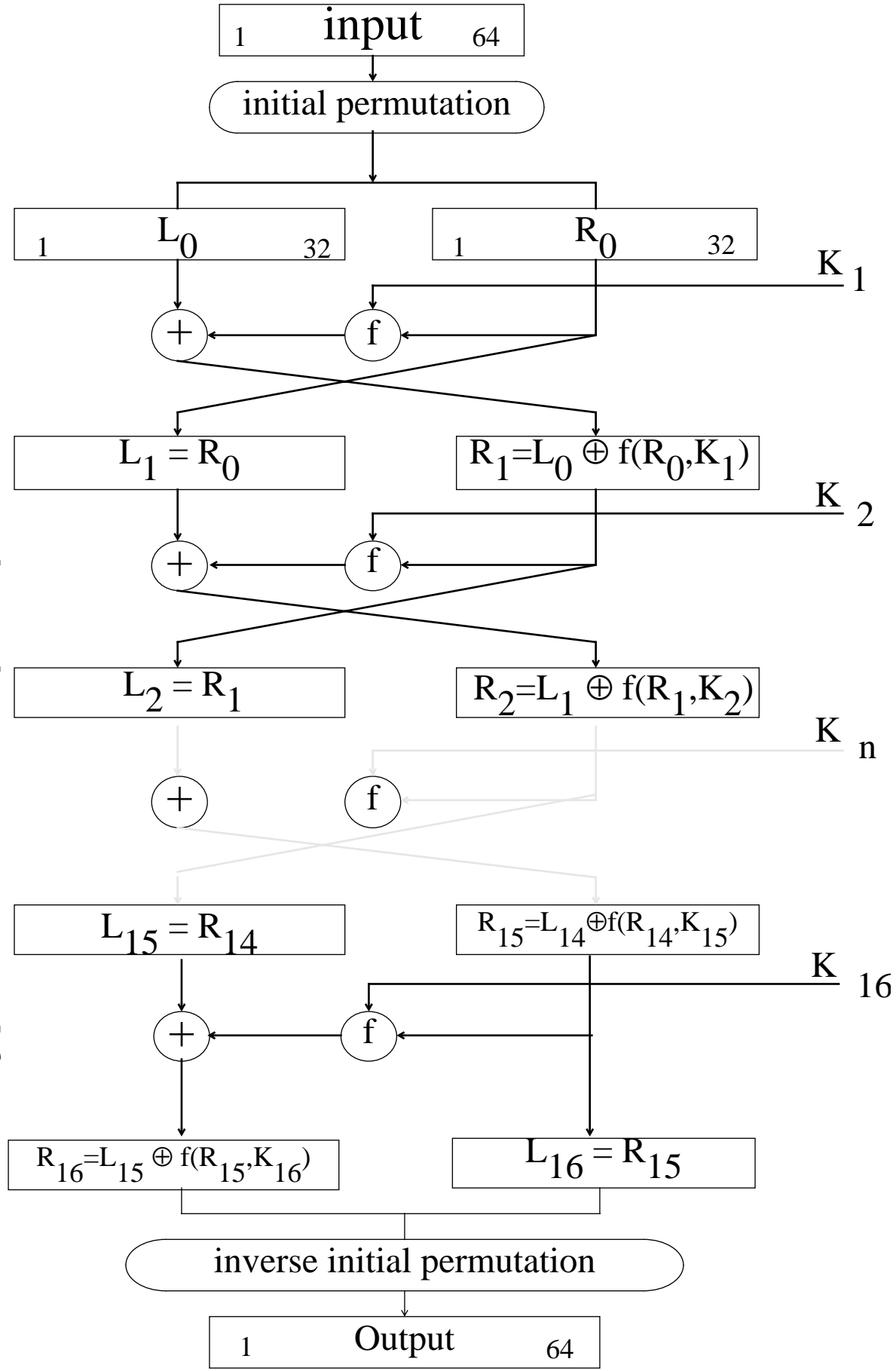
The target is to find out the column rearrangement.

It is based in the frequency of digrams in a language.

The process involves exhaustive comparison of strings using a window of variable size in the ciphertext in order to find patterns of digrams and in consequence define the column (or row) size.

❑ Double transposition algorithms

The Data Encryption Standard (DES)



Principle:

Product of permutation and substitution functions for a total of 16 cycles.

Key size: 56 bits.

Plaintext is encrypted as blocks of 64 bits.

Questions about the security of DES

- ☐ 56 bit keys might not be enough
- ☐ Some algorithm flaws have been identified
- ☐ Questions on the USA government decisions

Secure encryption systems

Based on problems that have a simple algorithm for their solution but the time required for their solution grows exponentially with the size of the problem.

Example: factorizing a number.

Public-Key Systems

The major disadvantage of the private key systems is that they require secure channels for the transmission of the key.

With public key systems each user has a (public) key that does not have to be kept secret, and a (private) key that only he knows.

The public key transformation is a one-way encryption with a secret (private) way to decrypt.

The best and most widely used public key encryption algorithm is the RSA (Rivest-Shamir-Adelman).

RSA encryption

Principle:

It is in the problem of factoring large numbers (for which only exponential algorithms exist for its solution).

Operation:

We have two keys d and e that work in pairs for decryption and encryption. The encryption is

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

and the decryption

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

The encryption key consists of the pair of integers (e, n) and the decryption key of the pair (d, n) .

Choosing keys

- ❑ The starting point is a value for n , which should be quite large and a product of two prime numbers p and q .
Ex: $p = 47$, $q = 71$ so that $n = 3337$.

Typically the prime numbers are approximately 100 digits each, so n is approximately 200 digits long. This way it is very difficult to factorize n and infer p and q .

- ❑ A large integer e is chosen so that it is relatively prime (that is no common factors) to $(q-1)*(p-1)$. An easy way is to choose a prime number larger than $(q-1)$ and $(p-1)$.

Ex: $(q-1)*(p-1) = 3220$

We choose $e = 79$

- ❑ Finally d is calculated from
$$e*d = 1 \text{ mod } (q-1)*(p-1)$$

Ex: $d = 79^{-1} \text{ (mod } (3220)) = 1019$

Encoding the message.

Following the example, we want to encode

$$m = 6882326879666683$$

We break the message in blocks (In this case of 3 digits).

$$m_1 = 688, m_2 = 232, m_3 = 687, m_4 = 966, m_5 = 668, m_6 = 3$$

We encrypt per block

$$688^{79} \pmod{3337} = 1570 = c_1 \text{ etc.}$$

The encrypted message is

$$c = 1570 \ 2756 \ 2714 \ 2276 \ 2423 \ 158$$

Decrypting the message requires performing the same exponentiation using the decryption key (1019, 3337)

$$1570^{1019} \pmod{3337} = 688 = m_1$$

etc.

Security of RSA

110 to 120 digit numbers can be factorized regularly with today's technology.

Secure implementations use 512 bit values (154 digits) and extreme cases using 664 bits (200 digits) are also used in some systems.

A factorization of a 644 bits numbers requires 10^{23} steps. Assuming that today's computer networks can perform 10^{12} steps per second, that means roughly 10^{11} secs or 3.000 years.

A note on the RSA algorithm

It is interesting to note that the RSA algorithm is symmetric. As a result encryption and decryption are mutual inverses and commutative

$$P = C^d \bmod n = (P^e)^d \bmod n = (P^d)^e \bmod n$$

This means that one can apply the encrypting transformation and then the decrypting one, or the decrypting followed by the encrypting one.

This feature can be used for authentication of the message.

Authentication using Public keys

Problem: We want to be sure that the message received comes from the person that claims it has send it.

Using his private key a person U can encrypt his message and send it out. Anyone can read it using U 's public key and verify the authenticity of the message (since only U can create this message).

If a secret message needs to be transmitted from U to P , then U also encrypts his message with P 's public key.

- ☐ Digital Signatures
- ☐ PGP - Pretty Good Privacy

A public domain authentication and encryption package.

Security involving programs

Fact:

All data are treated by programs that someone wrote.

Result:

Programs can introduce, accidentally or on purpose, security flaws.

- ☐ Tradoors
- ☐ Trojan horses
- ☐ Salami attacks
- ☐ Information leakage
- ☐ Service disruption programs

Trapdoors

An undocumented entry point into a module.

Origins of trapdoors:

- ❑ Forgotten debugging instructions
Ex. : The SMTP bug
Undefined operation codes in microprocessors
- ❑ Poor error checking
- ❑ Intentionally left in the program

How to find the trapdoors:

Exhaustive trials !

Trojan horses

A hidden function in addition to the stated obvious function of a program.

In general the origin of Trojan horses is malicious.

Examples:

- ☐ Password collection (faking the login program)
- ☐ Adding code in the data area of the binary and jumping to it

How to find Trojan horses:

Must analyse and/or recompile the source code

- The trojan horse can be in the compiler!
- Sources might be unavailable

Salami Attacks

Used mostly with programs that compute amounts of money, collecting small amounts from many sources.

Examples:

- ❑ In interest rate calculation of bank accounts the amounts after the third decimal point are transferred in a specific account (roundoff errors).
- ❑ A few centimes from the interest is transferred to a specific account.

How to find salami attacks

Must analyse the source code (extremely difficult)!

Find indications of an attack (ex. an account that grows without deposit transactions)

Information Leakage

In systems that handle sensitive data (ex. banks) the operators and programmers do not have access to the (customer) data.

However knowledge of this information can be obtained through extraordinary paths of communication.

For example, the program that prints a public statistics page after accessing the sensitive data can print out hidden information by changing parts in the printout:

- ☐ using '.' instead of ':' in the hours indication (18:35 vs 18.35)
- ☐ adding an 'S' in the word TOTAL (TOTAL vs TOTALS)
- ☐ leaving one or more spaces in specific places

Service disruption programs

Programs that consume or destroy resources.

- ☐ Greedy programs
Code errors like infinite loops
Process table overflow
I/O blocking, etc.
- ☐ Viruses
- ☐ Worms

Protection of software copyright

Software programs need to be protected from unauthorized copying (software theft).

- ❑ Disk based protection methods
Methods to make diskette copying difficult.
 - Use of innermost track and half-tracks
 - Track synchronization, Damaged media, etc.
- ❑ Physical protection devices
 - Dongles
 - Security protection chips
- ❑ Non-electronic methods
 - Birefringent plastic key device (color challenge)
 - Lenslok (optical scrambling)

Operating system security

In a multiprogramming operating system several objects need to be protected:

- ☐ Memory
One program should not be able to access the memory area of another
- ☐ I/O devices
Disk data protection
Coordination of serial I/O devices (ex. printers)
- ☐ Sharable programs
- ☐ Sharable data

Computer Network Security

Networks have security problems because of

- ❑ Sharing
Access is open to large number of users *and* systems
- ❑ System Complexity
A network combines more than one Operating systems
- ❑ Unknown perimeter
It is difficult to define the perimeter of the network to which a computer is connected
- ❑ Many points of attack
Access to a remote resource might pass over several different machines
- ❑ Unknown access path
With packet routing the path that is followed is random

Methods for network security

- ❑ Data encryption (protection and integrity)
- ❑ Access control
 - Port protection
Automatic Call-Back
Secure ports for accessing certain data
 - Node authentication (trusted hosts)
- ❑ User authentication
 - Passwords (user, group ..) and passphrases
 - Challenge-response systems
 - Smart Cards
 - Personal characteristics
- ❑ Data existence hiding
 - Pad traffic (random data in the unused channel)
 - Active routing control

The CERT Coordination Center

The CERT Coordination Center is the organization that grew from the computer emergency response team formed by the Defense Advanced Research Projects Agency (DARPA) in November 1988 in response to the needs identified during the Internet worm incident.

CERT services include:

- ☐ 24-hour technical assistance for computer security incidents
- ☐ product vulnerability assistance
- ☐ technical documents
- ☐ mailing lists for CERT advisories

- ❑ web (www.cert.org) and anonymous FTP ([info.cert.org](ftp://info.cert.org)) site, where security-related documents, CERT advisories and tools are available.

Communication lines' security

The transmission media need to be protected from intruders.

- ❑ Copper Cables
Wiretapping
Passive (just listening) and active (injecting data)
 - Physical cut of the wire
 - Electro-magnetic Induction
- ❑ Optical fiber
Impossible to tap without being detected
Repeaters, however, are easily taped.
- ❑ Microwave and satellite
Very simple to intercept
However the heavy multiplexing makes it difficult to intercept a specific signal.

Physical protection

Computer security also means protecting from these destruction due to natural disasters or human intervention.

- ❑ Natural disasters
 - Flooding
Rising water, Falling water
 - Fire
 - Power loss
UPS, Spike suppressor
 - Heat
- ❑ Intruders
 - Theft prevention
 - Access to the installation

Measures for physical protection

- ☐ Backups of the system
Recover from data/software loss
- ☐ Off-site backups
Recover after a natural disaster (fire)
- ☐ Cold site
Restart operations at minimal time at another site (no system is installed at the empty site)
- ☐ Hot site
Full system installation at another site
(can be a leased/shared system, or owned one)
- ☐ Destruction of “old” storage media before disposal
Magnetic data erasers (overwriting, degausers)

Legal Issues

- ☐ Ownership rights
- ☐ Licensing
- ☐ How to prosecute intruders
- ☐ What do courts recognize for damage liabilities
- ☐ ...