

Security in Computer Networks

Exercise by

Dipl.-Math. Kerstin Luck

BB 910

Tel.: 0203 –379 2583

Mail: kerstin.luck@uni-due.de



Literature

- W. Stallings – Cryptography and Network Security, Prentice Hall, 4th ed. 2005
- B. Schneier – Secrets and Lies. Digital Security in a Networked World , John Wiley & Sons 2004
- B. Schneier – Applied Cryptography, John Wiley & Sons 1996
- A.S. Tanenbaum – Distributed Systems, Prentice Hall 2002
- R. Oppliger – Internet and Intranet Security, Artech House 1998
- D. Kosiur – Virtual Private Networks, Wiley 1998



Distributed Systems
Dipl.-Math. Kerstin Luck

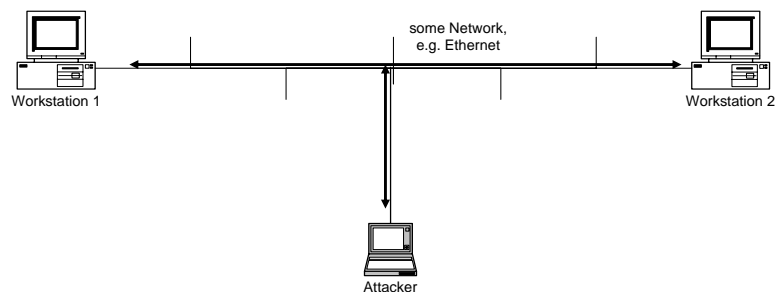
Security in Computer Networks

Security

- **Computer Security**
With the introduction computers protecting files and other information stored on the computer became evident.
- **Network Security**
Use of networks and communication facilities for distributing data among computers/users made it necessary to protect data during the transmission.
- **No clear boundaries between these two forms**

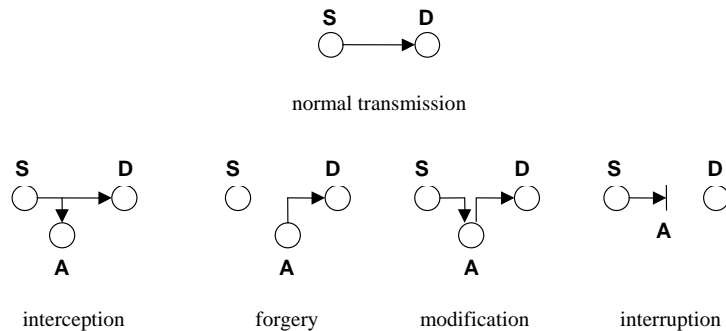
A Network Intruder

- An open network is used by „normal“ users as well as by attackers.



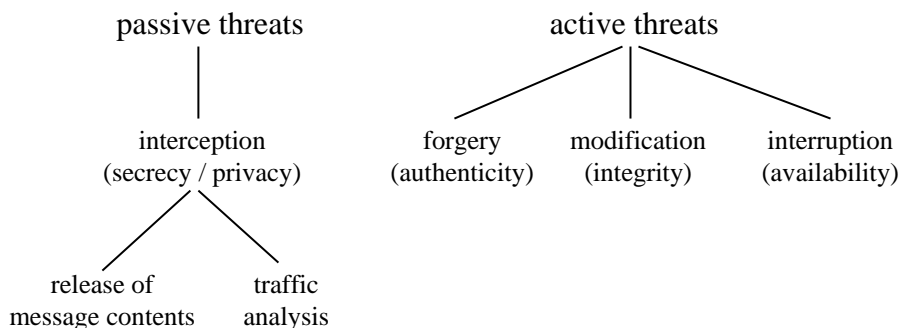
Security Threats

- By transferring data, some security threats are faced.



Active and Passive Threats

- One can distinguish between active and passive threats.



Active and Passive Threats

- Passive:
 - Interception is either release of content or „just“ traffic analysis.
- Active:
 - Modification and forgery often use masquerade (pretending to be someone else) to achieve their goal.
 - Forgery may also use replay attacks (sending an old package).

Security Mechanisms (1)

1. Encipherment
2. Digital Signature Mechanisms
3. Access Control Mechanisms
4. Data Integrity Mechanisms
5. Authentication Exchange Mechanisms
6. Traffic Padding Mechanisms
7. Routing Control Mechanisms
8. Notarization Mechanisms

Security Mechanisms (2)

- *Encipherment* is used either to protect the confidentiality of data units and traffic flow information, or to support or complement other security mechanisms.
- *Digital Signature Mechanisms* are used to provide an electronic analog of hand written signatures for electronic documents.
- *Access Control Mechanisms* use the authenticated identities of principals, information about these principals, or capabilities to determine and enforce access rights.

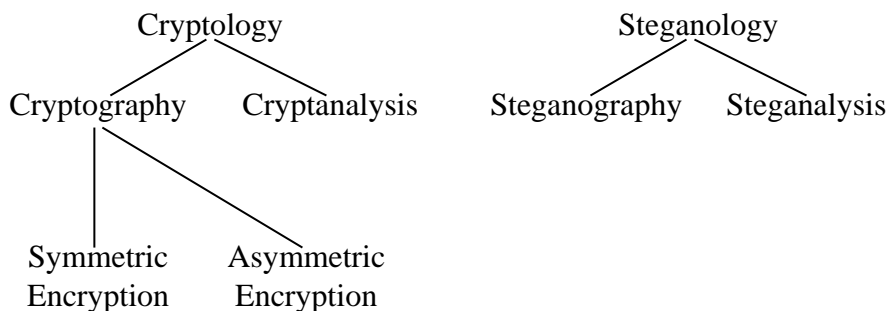
Security Mechanisms (3)

- *Data Integrity Mechanisms* are used to protect the integrity of either single data units and fields within these data units or sequences of data units and fields within these sequences of data units.
- *Authentication Exchange Mechanisms* are used to verify the claimed identities of principals.
- *Traffic Padding Mechanisms* are used to protect against traffic analysis attacks.

Security Mechanisms (4)

- *Routing Control Mechanisms* can be used to either dynamically or by prearrangement chosen specific routes for data transmission.
- *Notarization Mechanisms* can be used to assure certain properties of the data communicated between two or more entities, such as its integrity, origin, time, or destination.

Introduction to Encipherment



Cryptology

- *Cryptography* is the art of writing something in a way that only authorized people can read the message. For the others, the text doesn't make sense.
- *Cryptanalysis* is the attempt to read an encrypted text without knowing the secret.
- *Cryptology* is the generic term for both disciplines of science.

Steganology

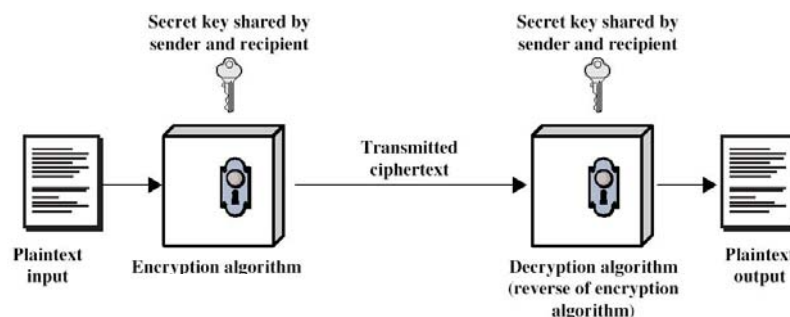
- *Steganography* is the art of hiding a message in an inconspicuous carrier material, like text, images, audio, or video files.
- *Steganalysis* tries to read out a hidden message or even detect that a message is hidden.
- *Steganology* is the generic term for both disciplines of science.

Examples

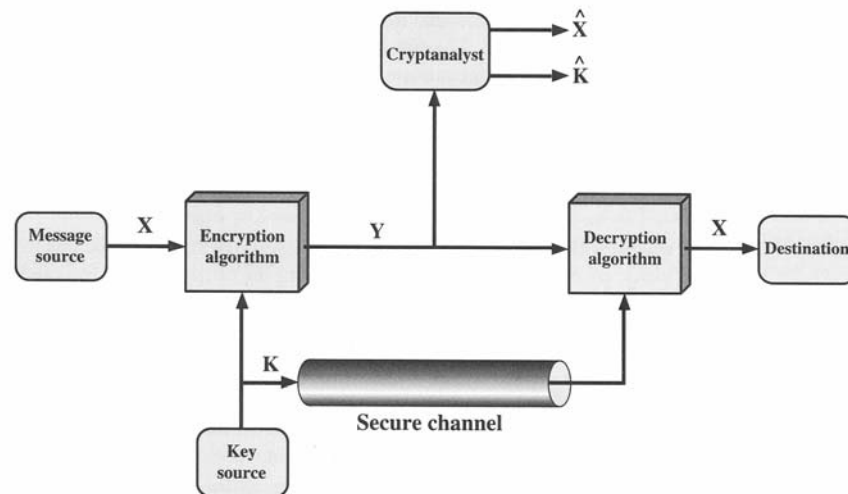
- Some examples for encryption technologies will be given hereafter.
- Steganography or Data Hiding is a pretty young field of research. A historic example for steganography is „invisible ink“. A software that embeds data in carrier material is, e.g. the Steganos Security Suite™. A special area in the field of steganography is digital watermarking.

Cryptography in general

- Encryption is the technique to modify a given message with a special algorithm and an additional secret information, called the „**key**“.



Conventional Cryptosystem



Classical Cryptography

- Transposition ciphers
 - The order of the characters is changed, e.g. Skytala, Rail Fence Cipher.
- Substitution ciphers
 - One character is substituted by another, e.g. Caesar, Vigenère, Playfair.
- Product ciphers
 - This is a combination of substitution and transposition, e.g. DES.

Rail Fence Cipher - Encryption

- Write down characters like a fence.
- The depth gives you the number of rows.
- Example

Plaintext: securityinnetworks

Key: *depth 4*

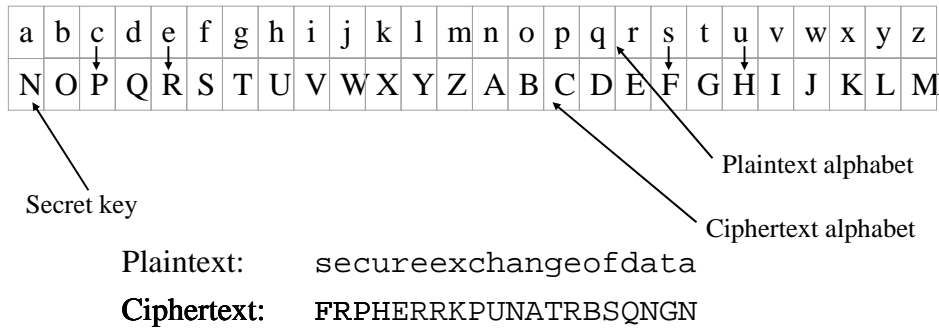
s	r	i	t	k	
e	i	n	w	s	
c	t	n	o		⇒ SRITKEINWSCTNOUYER
u	y	e	r		

Rail Fence Cipher - Decryption

- Cipher text: SRITKEINWSCTNOUYER
- Key: *depth 4*
- # characters of the ciphertext divided by the depth: $18 : 4 = 4$ remainder 2
- 4 columns, only the first 2 rows consist of 5 columns:

S	R	I	T	K	
E	I	N	W	S	
C	T	N	O		⇒ securityinnetworks
U	Y	E	R		

The Caesar Cipher



The Caesar Cipher

- Problem: Caesar can easily be broken. Either one searches through all possible keys (brute-force attack) for a valid or sense making text or one uses frequency of letters.
- The most frequent letter in English is the ,e'. So, count all letters in the text and try if the most frequent letter fits to ,e'.

Breaking Caesar

- Ciphertext: FRPHERRKPUNATRBSQNGN
- The most frequent letter (4 times) is ,R‘.
Assume, that ,R‘ is the substitute of ,e‘.

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
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

- Hence, the secret key is N.
- Decoding the message gives:

secureexchangeofdata

or

,secure exchange of data‘.

How can we improve Caesar?

- Let's use many Caesar alphabets! This is called a polyalphabetic cipher.
- Invent a keyword that is the secret key. This keyword gives you the order of which Caesar alphabets you use.
- A smart guy from France came up with that idea 1586. His name was Blaise de **Vigenère**.
- For a long time, scientists believed the Vigenère cipher to be unbreakable, but it is.

The Vigenère Cipher (1)

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

The Vigenère Cipher (2)

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

Plaintext: security

Key: key

Usage: security
keykeyke

*Different plaintext characters,
but same ciphertext characters
because of key!*

⇒ Ciphertext: CIAEVGDC

Playfair (1)

- Plaintext is considered in pairs $x_i y_i$.
- Key is a key word or sentence and is transferred into a 5x5 matrix A. The first character is a_{11} , the second is a_{12} , ..., the 6th is a_{21} , ... Repeated characters are skipped and at the end the matrix is filled up by the remaining characters of the alphabet (J is substituted by I).
- x_i is replaced by the character of the matrix found in the same row as x_i and the same column as y_i .
- y_i is replaced by the character of the matrix found in the same row as y_i and the same column as x_i .

Playfair (2)

- Exceptions:
 - If x_i and y_i are in the **same row** the righthand neighbor is used in each case.
 - If x_i and y_i are in the **same column** the lower neighbor is use in each case.
 - If neighboring characters are the **same** they are seperated by 'x', e.g. aa becomes axa.
 - If there is a **lonely** character at the end a 'x' is appended.

Playfair (3)

- Plaintext: security in networks considered as:

se cu ri ty in ne tw or ks

- Key sentence: 'we are secure' :

W	E	A	R	S
C	U	B	D	F
G	H	I	K	L
M	N	O	P	Q
T	V	X	Y	Z

se → WA ne → VU
cu → UB tw → WC
ri → AK or → PA
ty → VZ ks → LR
in → HO

Playfair (4)

security in networks
becomes

WAUBAKVZHOVUWCPALR

For **decryption** the same matrix and the same rules are used with some short exceptions:

If x_i and y_i are in the same row the lefthand neighbors are used.

If x_i and y_i are in the same column the upper neighbors are used.