Application Layer (1)

Functionality:

- providing applications (e-mail, Web service, USENET, ftp etc)
- providing support protocols to allow the real applications to function properly (e.g. HTTP for Web appl.)
  - *security* comprising a large number of concepts and protocols (PGP, SSL)
  - *DNS* (Distributed Name Service) handling naming within the Internet
  - *network management* (SNMP)

Network security nowadays is regarded as one of the biggest problems for upcoming Internet applications

Objective:

providing secure Internet applications like

- secure e-mail system (PGP and extensions (S/MIME))
- secure e-commerce - transactions (SSL and extensions (TLS))

Network Security (1)

Secure communication in general addresses four different topics:

- *secrecy (Vertraulichkeit, Geheimhaltung)*: keeping information secret
- *authentication (Authentifikation)*: determining whom you are talking to before revealing information
- *nonrepudiation (Verbindlichkeit)*: ensuring trustworthiness between the communication partners
- *integrity (Datenintegrität)*: ensuring the originality of received messages (not being modified)

Solutions to all problem areas are mainly based on **cryptographic** (Greek: secret writing) principles

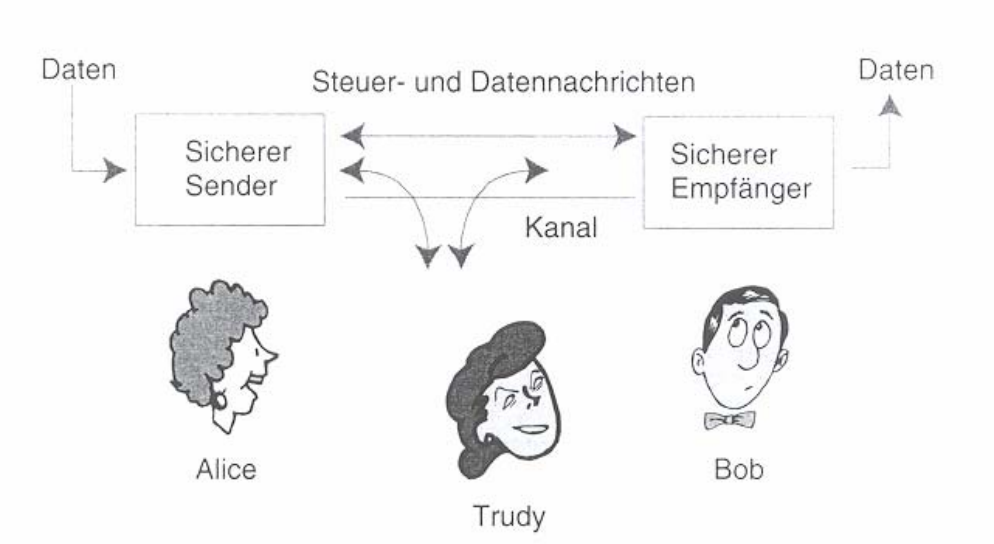
Historically, until the second half of the 20th century, only 2 human areas have used and contributed to the art of cryptography:

- military
- diplomacy

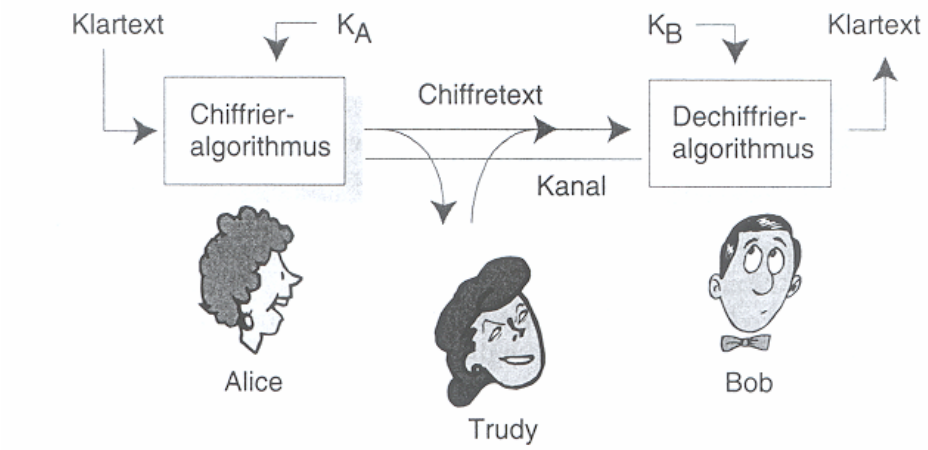
Today, **economy** is becoming the most important application area where cryptography is used.

Network Security (2)

Representatives for sender, recipient, and intruder

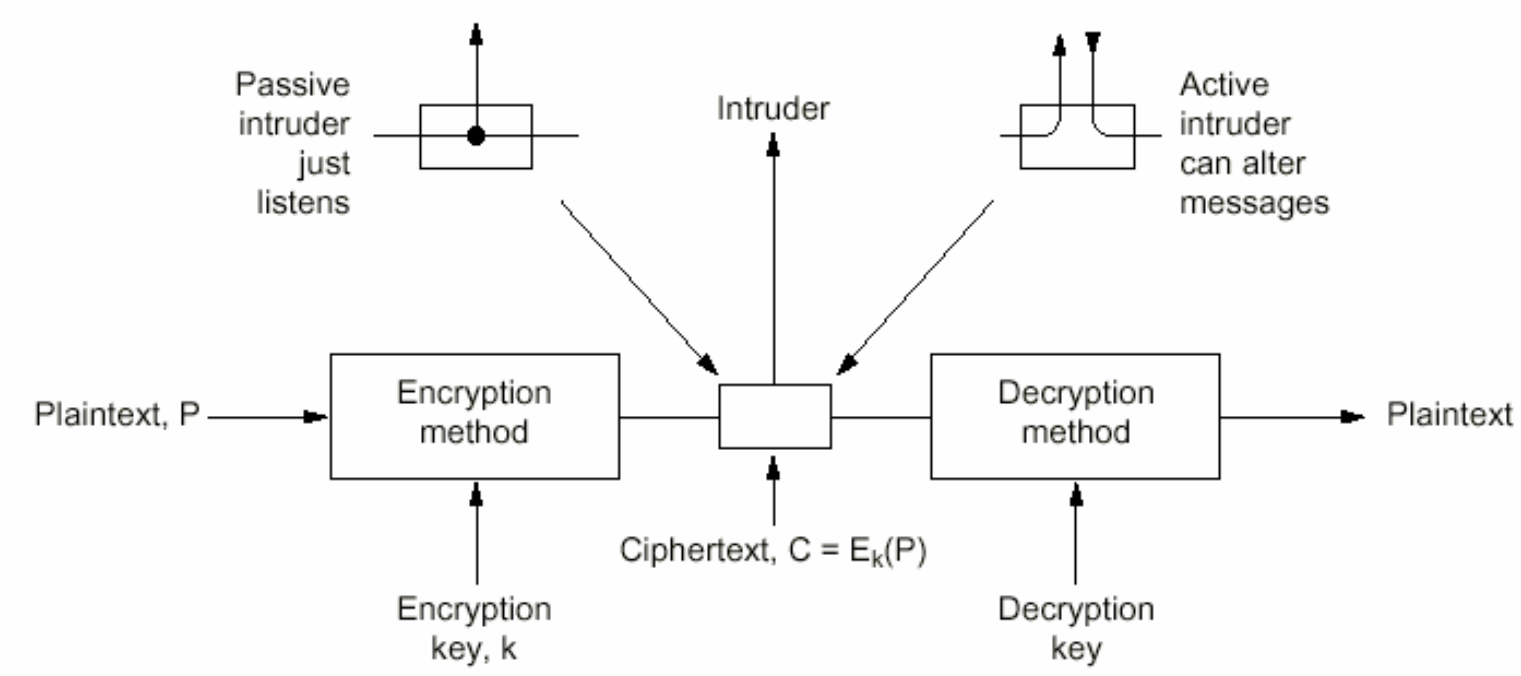


The encryption model (1):



Network Security (3)

The encryption model (2):



Cryptology denotes

- **cryptography:=** the art of devising ciphers **and**
- **cryptanalysis:=** the art of decoding (breaking) ciphers

Secrecy (1)

Symmetric Key System:

Keys of Alice and Bob are identical and secret

Public Key System:

Both, Alice and Bob have a pair of keys, one is public, the other is only known by its holder.

1. Symmetric Key Systems (old)

Traditional encryption methods have been divided historically into two categories:

- substitution ciphers (preserve the order of the plaintext symbols but disguise them)
- transposition ciphers (reorders the plaintext symbols but do not disguise them)

Ancient and simple substitution cipher: **Caesar's cipher**

The ciphertext alphabet results from a shift of *k* letters in the plaintext alphabet (key*:=k*).

Generalization of Caesar's chiffre: **monoalphabetic substitution**

Each letter or group of letters is replaced by another letter or group of letters to disguise it

Example for a monoalphabetic substitution

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

Secrecy (1a)

Two main approaches of crypto analysts to break these type of ciphers

- exploiting statistical properties of natural languages (cipher text only attack)
- guessing a probable word or phrase (known plaintext attack)

Example for the second approach:

CTBMN BYCTC BTJDS QXBNS GSTJC BTSW*X CTQTZ CQV*UJ
QJSGS TJQZZ MNQJS VLNSX VSZJU JDSTS JQUUS JUBXJ
DSKSU JSNTK BGAQJ ZBGYQ TLCTZ BNYBN QJSW

Secrecy (2)

Transposition ciphers

Instead of disguising letters they are reordered

Example for a columnar transposition

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
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
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	**w**	o	a	b	c	d

Plaintext

pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Ciphertext

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

Secrecy (3)

2a) Symmetric Key Systems (modern) based on stream ciphers

Typical example: One-time pads

Method for devising an unbreakable cipher

Algorithm:

- convert a plaintext of any length into a bit string, e.g. by using its ASCII representation
- choose a random bit string of equal length as the key
- compute the EXCLUSIVE OR of both strings, bit by bit, serving as resulting cipher text
- used only once

Main disadvantage:

- the overhead for key management (communicating the key in a secure way to the communication partners once again for each new plaintext) is, in general, beyond any acceptable size

---> not applied in practice

Symmetric Key Systems (1)

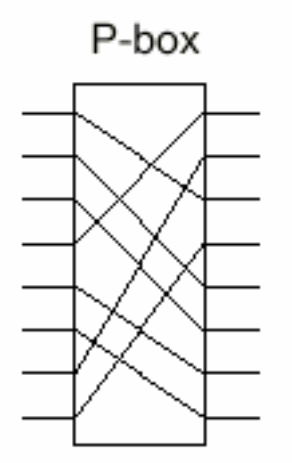
2b) Symmetric Key Systems (modern) based on block ciphers

Principle: Subdividing the plaintext in subsequent blocks of equal length (e.g. 64 or 128 bit)

Idea: Concatenation of standard transposition (permutation) and substitution elements (boxes):

Example for a P(ermutation)**-box** (01234567 ---> 36071245)

The order of sequence has changed



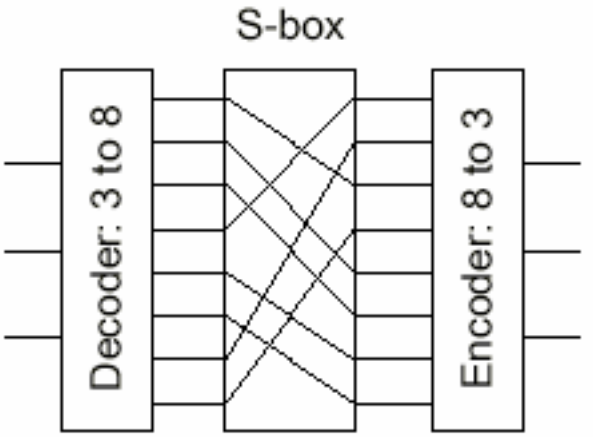
Example for a S(ubstitution)**-box** (3bit plaintext to 3bit ciphertext)

By appropriate wiring of the P-box inside, any substitution can be accomplished.

In this example:

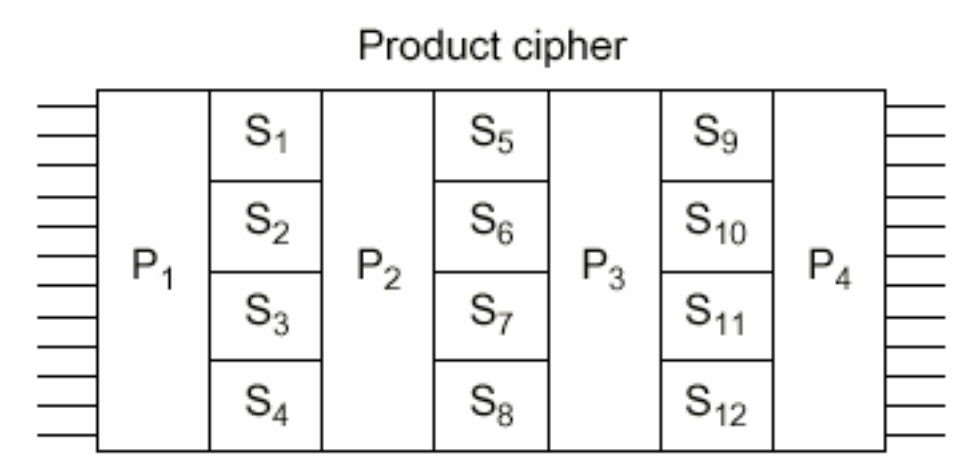
Numbers 0,1,2,3,4,5,6,7 each are replaced by the numbers

24506713



Symmetric Key Systems (2)

Example for a product cipher (concatenation)



Standard: DES

- plaintext is encrypted in blocks of 64 bits
- the algorithm has 19 steps
- the steps for decryption are done in the reverse order of those for encryption

Public Key Systems (1)

3. Public-Key Systems

Basic problem behind:

Is it possible that Alice and Bob can communicate by encrypted messages without having exchanged before a common secret key?

Principal solution:

Each party has a pair of keys, a public one (accessible to everybody) and a private one (only known by itself)

The general model