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 (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

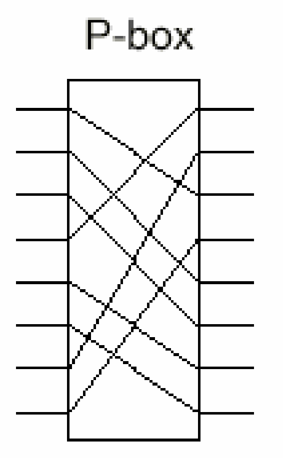
AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

Symmetric Key Systems (1)

2. Symmetric Key Systems (modern)

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

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



The order of sequence has changed

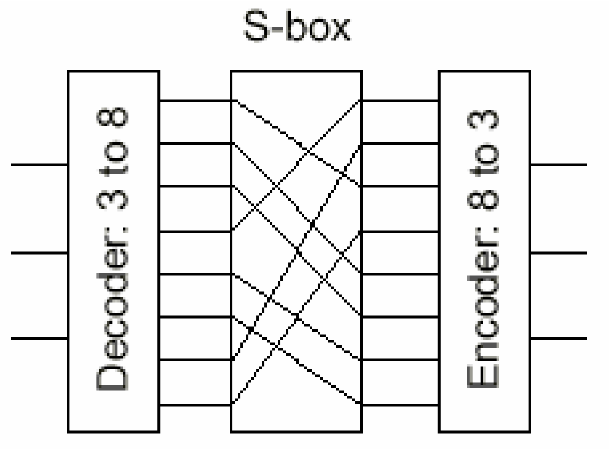
Example for a S(ubstitution)**-box** (3bit plaintext to 3bit ciphertext)

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

In this example:

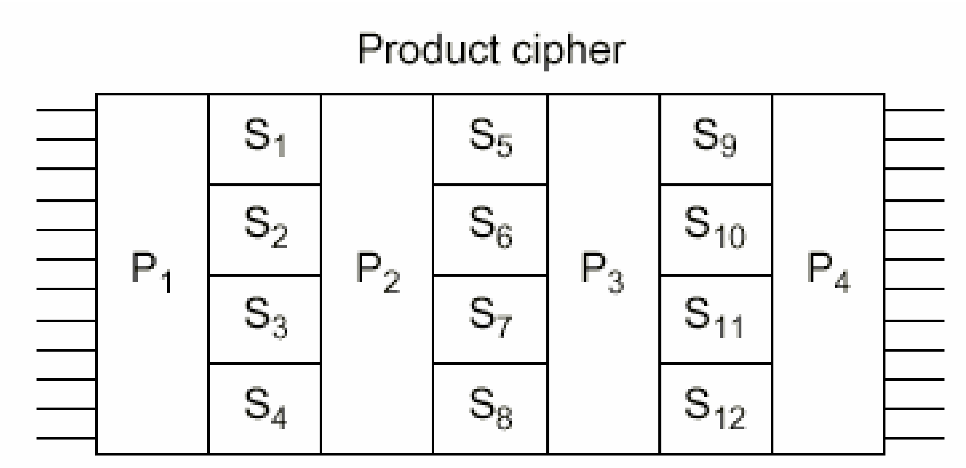
Numbers 0,1,2,3,4,5,6,7 each are replaced by the numbers

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

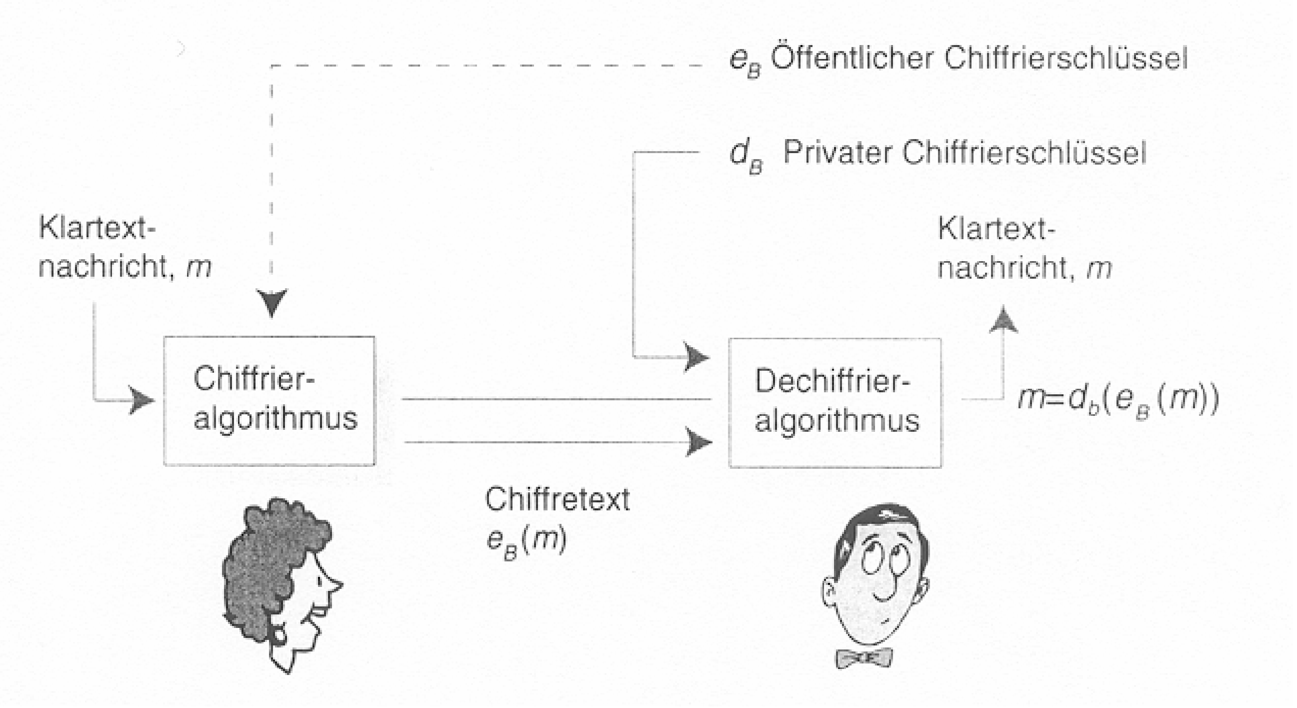
Basic problem behind:

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



Public Key Systems (2)

The RSA algorithm

Two components:

- Selecting the keys
- Applying the encryption and decryption algorithm

Selecting the keys (by Bob):

1. Choose two large primes, p and q
2. Compute $n = p \times q$ and $z = (p-1) \times (q-1)$.
3. Choose a number relatively prime to z, smaller than n and call it e (e is used for *e*ncryption) .
4. Find d such that $e \times d = 1 \; mod \; z$ (d is used for decryption) .
5. The public key is (n,e), the private key is (n,d).

Encryption (by Alice) of a bit pattern (number) m such that $m < n$ by means of Bob's public key (n,e).
The resulting cipher c is:
$c = m^e \; mod \; n$

Decryption (by Bob) of c by means of his private key (n,d) in order to get the plaintext m:
$m = c^d mod \; n$

Public Key Systems (3)

Example of the RSA algorithm

p=5, q=7 ---> n = 35, z=24. Further, Bob selects e=5, d=29 (5*29 - 1 can be divided by 24)

----> public key of Bob: (35,5), private key of Bob: (35, 29)

Alice wants to send the message “LOVE” to Bob by encrypting each letter separately and interpreting each letter as the corresponding number (a maps to 1, ..., z maps to 26)

Tabelle 7.1 Die RSA-Verschlüsselung von Alice, $e = 5$, $n = 35$

Klartextbuchstabe	m: numerische Darstellung	m^e	Chiffretext $c = m^e \bmod n$
L	12	248832	17
O	15	759375	15
V	22	5153632	22
E	5	3125	10

Tabelle 7.2 Die RSA-Verschlüsselung von Bob, e = 29, n = 35

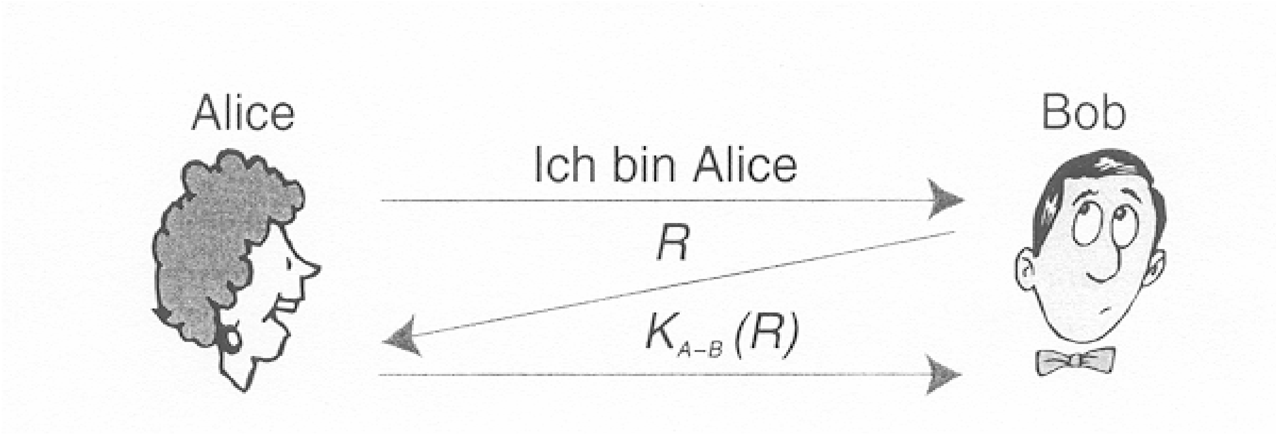
Chiffre-text c	c^d	Chiff-retext $m = c^d \bmod n$	Klartext-buch-stabe
17	481968572106750915091411825223072000	12	l
15	12783403948858939111232757568359400	15	o
22	8.5164331908653770195619449972111e+38	22	v
10	100000000000000000000000000000	5	e

Authentication

Authentication Protocols

- technique by which a process verifies that its *actual* communication partner is who it is supposed to be
- normally done before the partners start to exchange data messages, e.g. e-mails

Version with symmetric keys



Version with public keys