Seminar

Database and Information Systems

Security Primitives and Methods

Betreuer: Boris Stumm

Yingyan Zhang
zhangyin@rhrk.uni-kl.de
Angewandte Informatik

02.07.2004

Introduction

- Security Primitives
- Methods and Applications
- Protocols
- Conclusion

Security primitives derived from the definition of information systems security

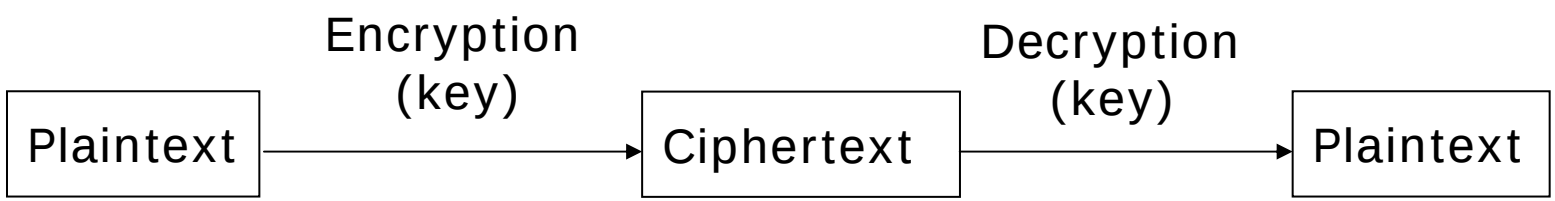
Definition	Primitives
„Information Systems Security is the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document and counter such threats.“	Authentication Confidentiality Integrity Availability

Realization of security primitives

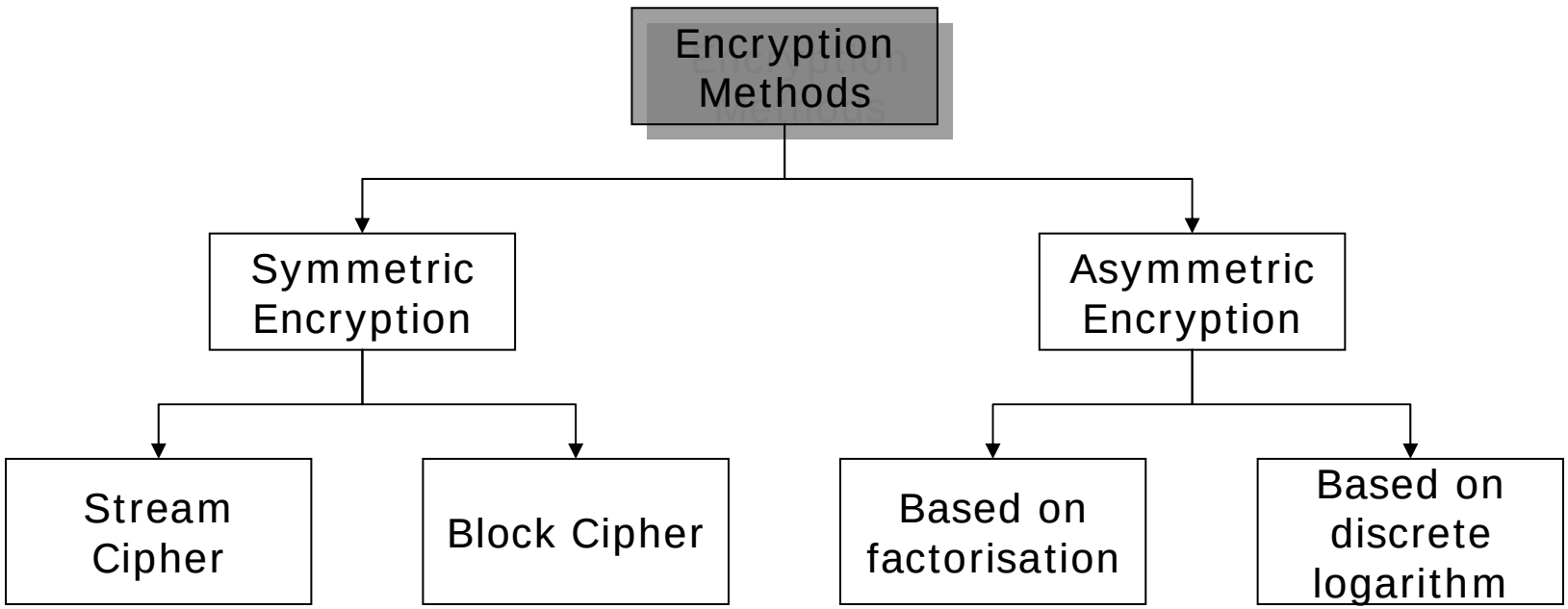
- Confidentiality
  - Encryptions
- Integrity
  - Hash Function, Digital Signature
- Authentication
  - Digital Signature
- Availability
  - backups, fail-over system, disaster recovery plans

Cryptography is the basic technique

Cryptography = kryptos (hidden or secret) + graphos (writing)



Categories of encryption methods



Symmetric Encryption

- Uses the same key to encipher and decipher.

- Two fundamental classes:
  - Stream Cipher
    - Encrypts the plaintext letter by letter
  - Block Cipher
    - First divides the plaintext into blocks, then enciphers

Stream Cipher: Vigenère Cipher

- The formula of Vigenère Cipher is mathematically represented as:

  Ciphertext = Plaintext + Key modulo 26

- Here is an example:

  Plaintext: tob eor not tob eth ati sth equ est ion

  Key: run run run run run run run run run run

  Ciphertext: kio vie eig kio vnu rnv jnu vkh vmg zia

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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

Stream Cipher: One-Time Pad

- The only secure encryption method.
  - The key length is as long as the plaintext.
  - The key is not repeatedly used.
- It is expensive for most of the applications.
- How to exchange the key safely?

Block Cipher: Playfair

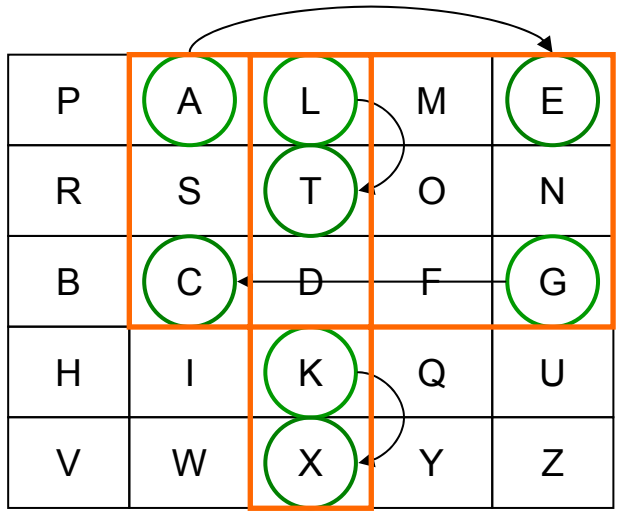
Plaintext:
The rain in Spain stays mainly on the plain.

Step 1:
therainінspainstaysmainlyontheplain

Step 2:
th er ai ni ns pa in st ay sm ai nl yo nt he pl ai n

Step 3:
th er ai ni ns pa in st ay sm ai nl yo nt he pl ai nz

Step 4:
rk pn sw su rt al us to mw oa sw te mf ro up am sw ge



Block Cipher: AES

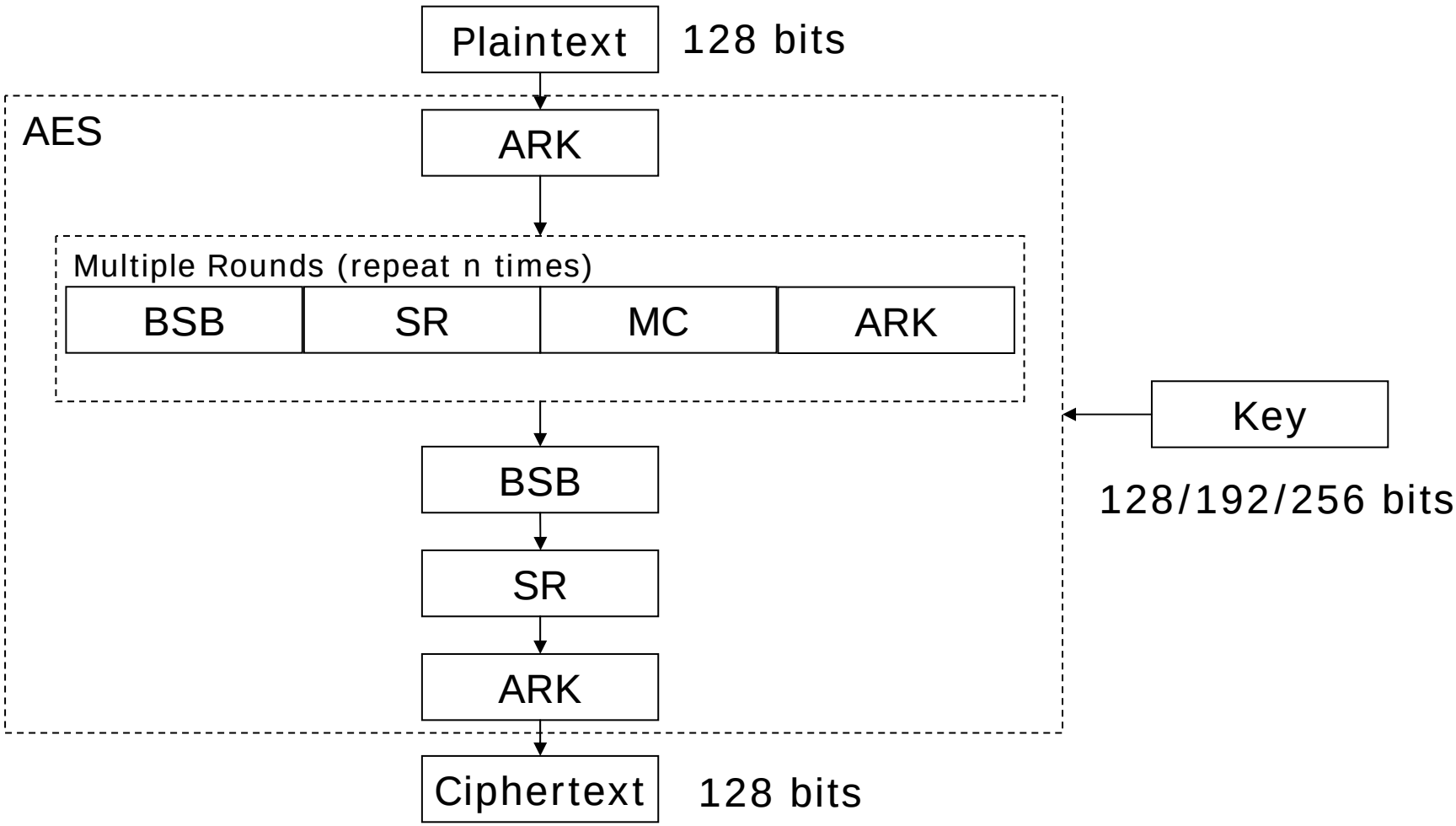
- In 1997 in America, the National Institute of Standards and Technology (NIST) initiated a process to select a symmetric-key encryption algorithm to be used to protect sensitive Federal information.

- In 2000 the algorithm invented by Vincent Rijmen and Joan Daemen was selected as Advanced Encryption Standard (AES)

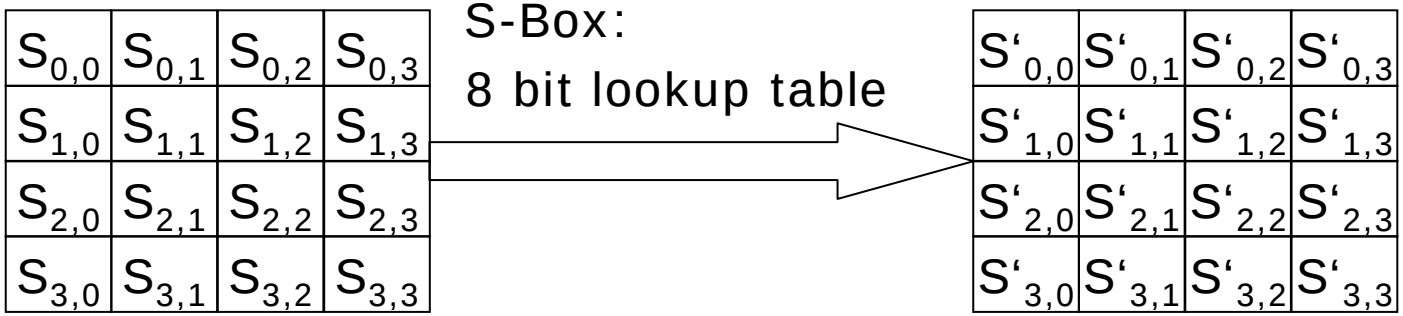
Basic data of AES

- AES has a block size of 128 bits, key size of 128, 192, 256 bits.
- The general working sectors of AES are:
  - Add Round Key (ARK);
  - Byte Substitution Byte (BSB);
  - Shift Row (SR);
  - Mix Column (MC)
- The number of rounds depends on the key size.
  - 128 bits key: 9 rounds
  - 192 bits key: 11 rounds
  - 256 bits key: 13 rounds

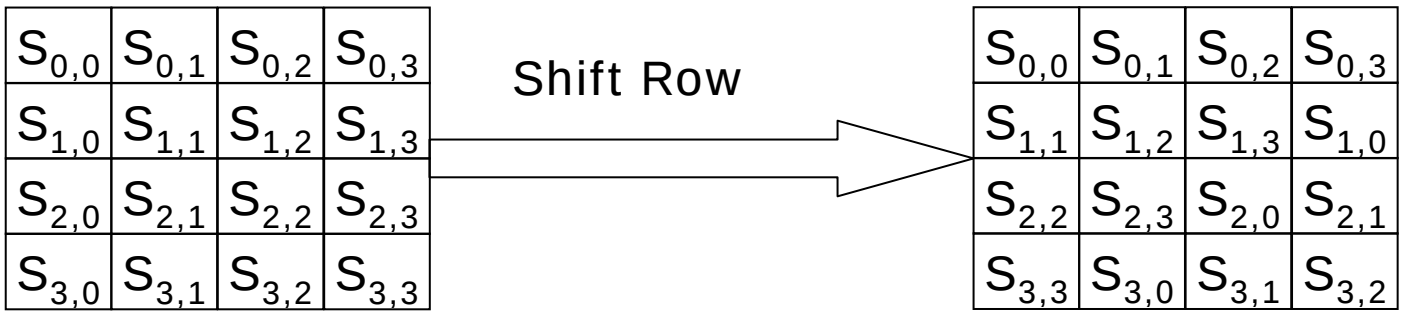
Working process of AES



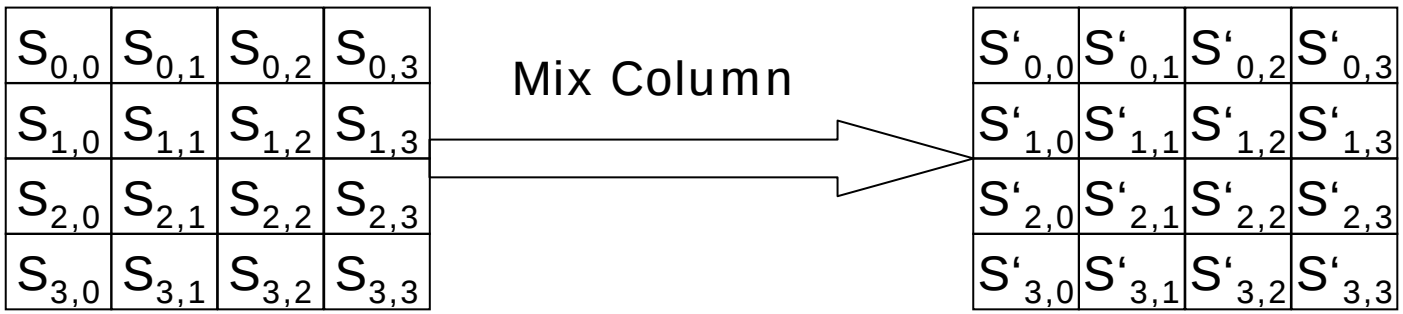
Byte Substitution Byte: Each byte will be replaced by another byte using the S-box



Shift Row: Shift the row according to the row number

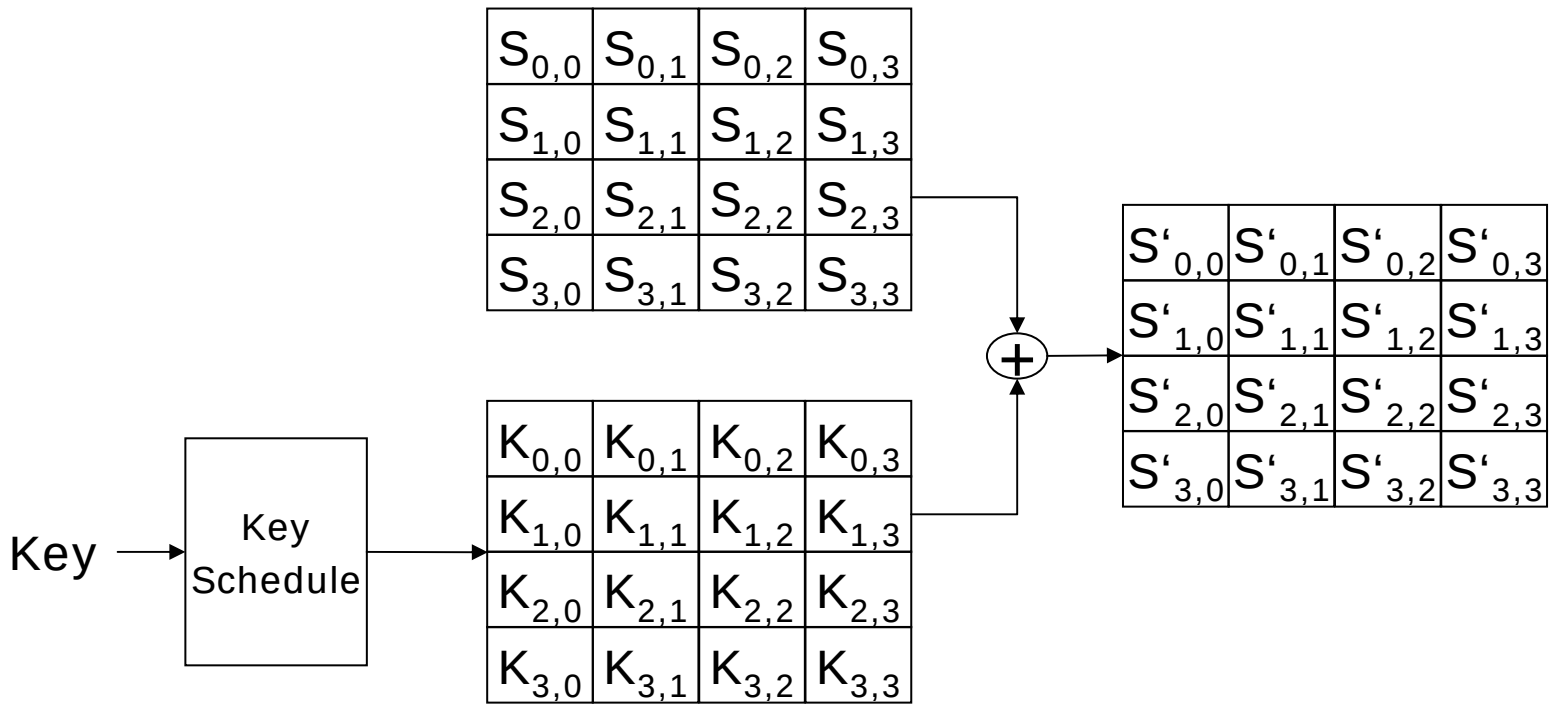


Mix Column: Every byte in a column will be mixed



$$\begin{pmatrix} S'_{3,0} \\ S'_{2,0} \\ S'_{1,0} \\ S'_{0,0} \end{pmatrix} = \begin{pmatrix} 02 & 01 & 01 & 03 \\ 03 & 02 & 01 & 01 \\ 01 & 03 & 02 & 01 \\ 01 & 01 & 03 & 02 \end{pmatrix} \begin{pmatrix} S_{3,0} \\ S_{2,0} \\ S_{1,0} \\ S_{0,0} \end{pmatrix}$$

Add Round Key: The selected round key is added to the text with XOR



Asymmetric Encryption

- Uses different keys to encrypt and decrypt
  - Encryption: public key
  - Decryption: private key

- Based on the difficulty of solving a certain mathematical problem:
  - Factorisation: It is hard to solve a composite number into its factors if this number is big enough.
    - RSA
  - Discrete logarithm: For each natural number y, it can be expressed as $y \equiv g^x$ modulo p.
    - ElGamal

RSA: Background Knowledge

- RSA was invented by Ron Rivest, Adi Shamir and Len Adleman in 1978.

- The two basic mathematic theories supporting RSA are:
  - Fermat's Little Theorem:

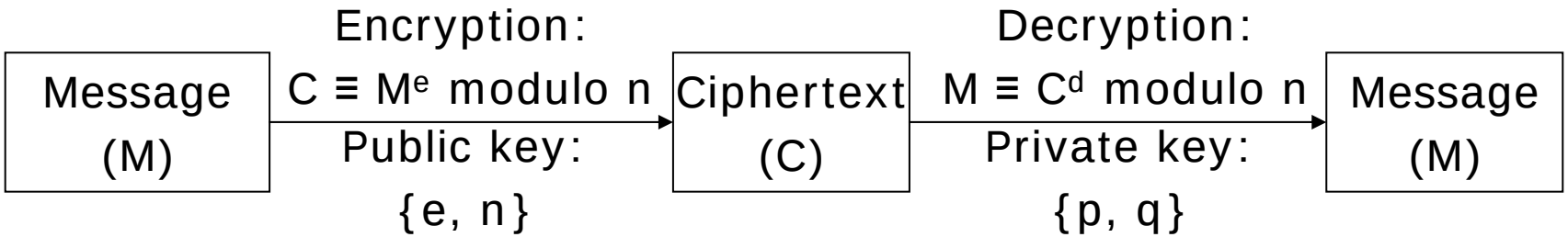
    For all primes p not dividing a, $a^{p-1} \equiv 1$ modulo p
  - Euler's function f(n):

    f(n) is the number of positive integers less than n with which it has no divisor in common.

    So if n is the product of two primes p and q, then:

    f(n) = (p-1) (q-1)

RSA: encryption and decryption formulas



$C^d \equiv \{M^e\}^d \equiv M^{ed} \equiv M^{1+k \bullet f(n)} \equiv M \bullet M^{k \bullet f(n)} \equiv M \times 1 \equiv M$ module n

n: a natural number with fators p and q

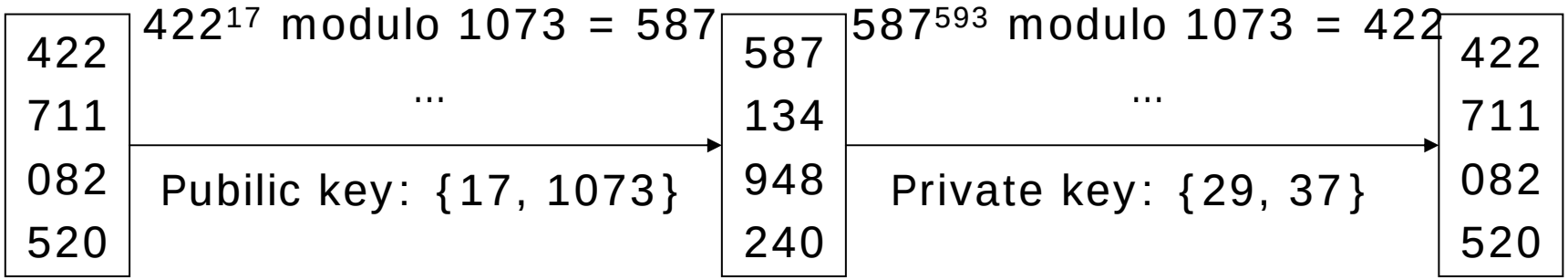
p: a prime number between [0, n-1]

q: a prime number between [0, n-1]

e: exponent between [0, n-1] without common factors of p-1 and q-1

d: a number between [0, n-1] with $d \cdot e \equiv 1$ modulo f(n)

RSA: Example



M = 422711082520; n = 1073; p = 29;
q = 37; e = 17; d = 573;
C = 587134948240

ElGamal: Background

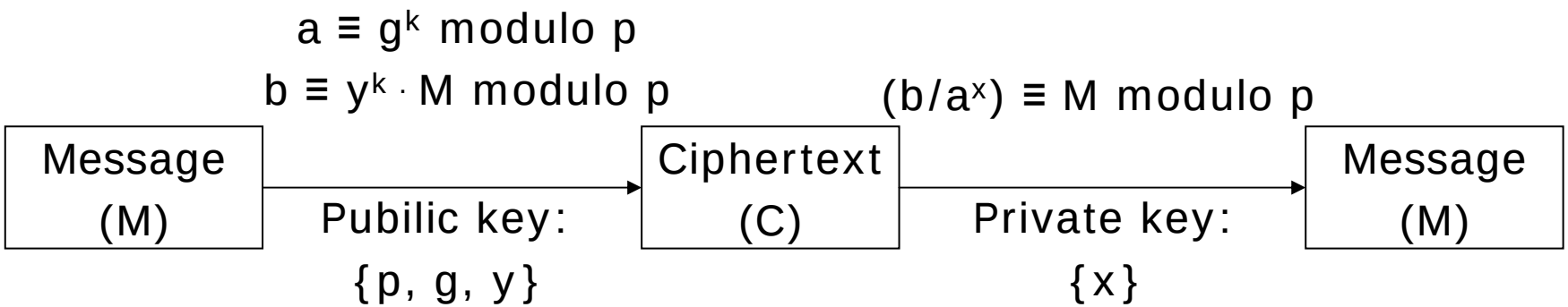
- ElGamal was invented by Taher Elgamal.
- The theory behind ElGamal is:
  - For each natural number y, there is a number x, which satisfies the equation: $y \equiv g^x$ modulo p. p is a random prime number. y, g, x are natural numbers smaller than p.
  - It is easy to find the corresponding x for y by calculation as long as p is small. If the number is big it will be very difficult.

Backup 2

- For example: suppose p = 11, g = 7:

y	x	because
1	10	7^{10} modulo 11 = 1
2	3	7^{3} modulo 11 = 2
3	4	7^{4} modulo 11 = 3
4	6	7^{6} modulo 11 = 4
5	2	7^{2} modulo 11 = 5
6	7	7^{7} modulo 11 = 6
7	1	7^{1} modulo 11 = 7
8	9	7^{9} modulo 11 = 8
9	8	7^{8} modulo 11 = 9
10	5	7^{5} modulo 11 = 10

ElGamal: encryption and decryption formulas



x: a natural number between [0, p-1]

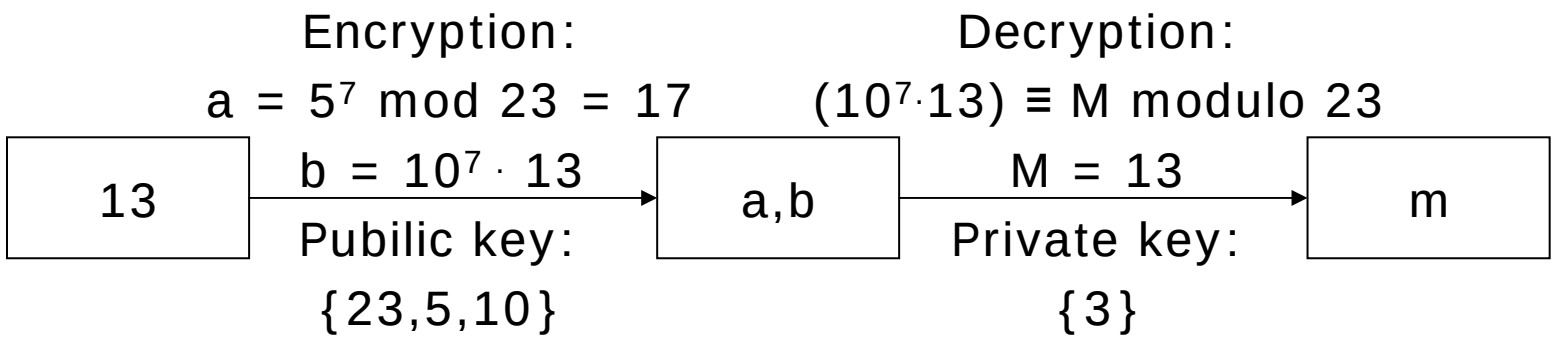
y: a natural number between [0, p-1], $y \equiv g^x$ modulo p

g: a natural number between [0, p-1]

p: a random prime number

k: a random natural number

ElGamal: example



x = 3; g = 5; p = 23;

y = 10; k = 7;

Comparison of Symmetric and Asymmetric Encryption

Symmetric

(+) The calculation in symmetric encryption is relatively easy, like addition, muliplication

(-) A large number of keys are needed

2 Perons: 1 keys

100 Persons: 4950 keys

Can be compensated by the application of Key Distribution Center (KDC).

(-) Risk to exchange the secret key safely.

Asymmetric

(+) No need to exchange the private key.

(+) The number of keys needed is reduced.

2 Perons: 2 keys

100 Persons: 200 keys

(-) The calculation is relatively complex.

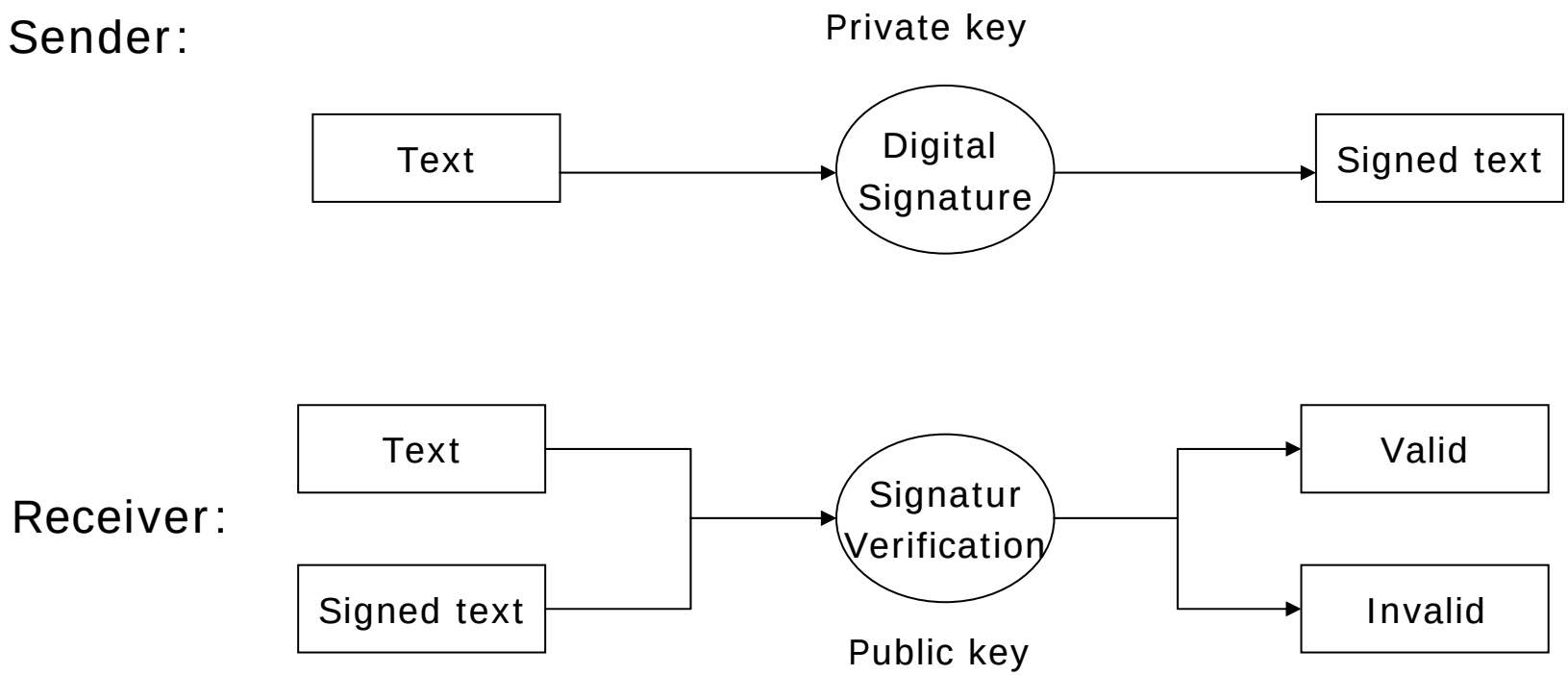
(-) Comparing with symmetric encryption, the key size is big.

(-) It is possible to find the some mathematic solutions in the algorithm.

One-Way Hash Function

- One-way hash function should meet the conditions:
  - The hash value should be relatively small for any input
  - Two different messages should not have the same hash value
  - Only one-direction calculation is possible
- Can be used to create a MIC (message integrity code) to check integrity
- Can be used to compute message digests.

Digital Signature:

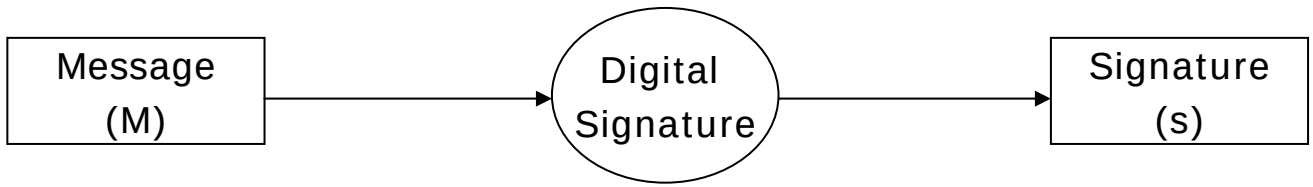


Digital Signature: Using ElGamal Algorithm

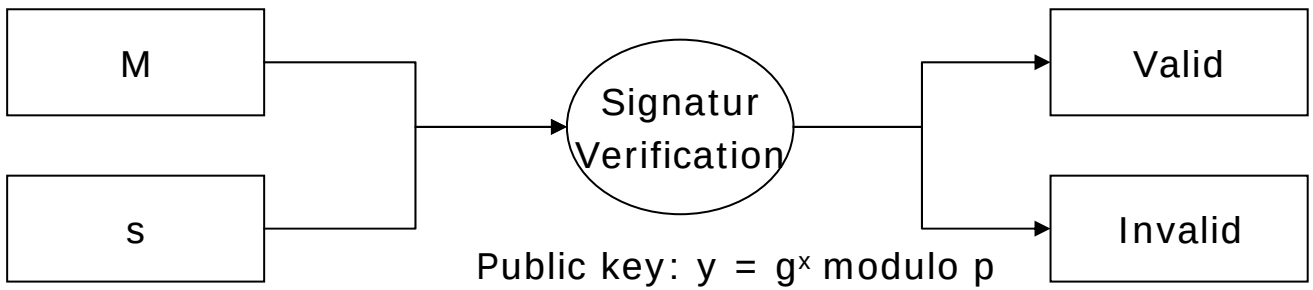
Alice:

Private key: x

rx + sk = M module p-1



Bob:



Public key: $y = g^x$ modulo p

$y^r r^s \equiv g^M$ modulo p

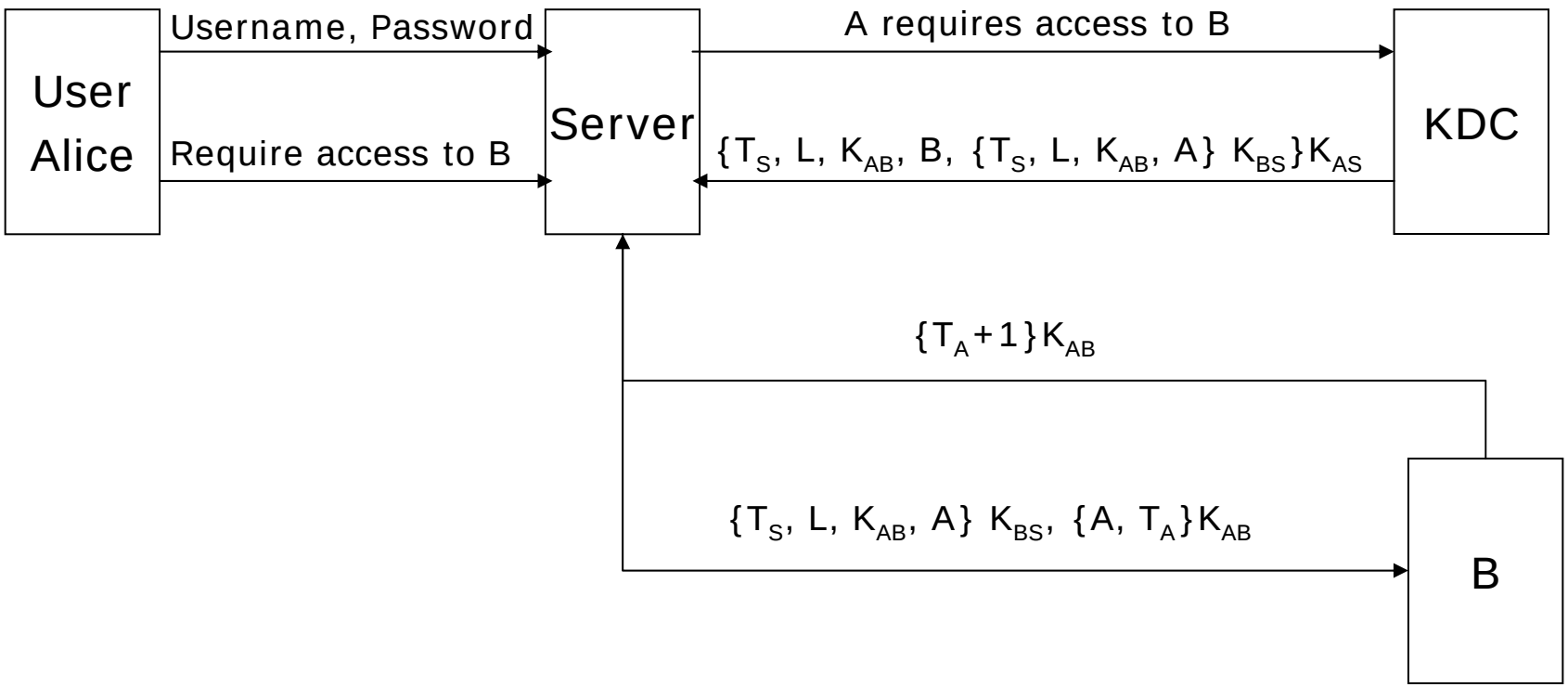
$(= g^{rx}\, g^{sk} \equiv g^M$ modulo p)

k, g are random natural numbers; p is a prime number; $r = g^k$ modulo p

Kerberos

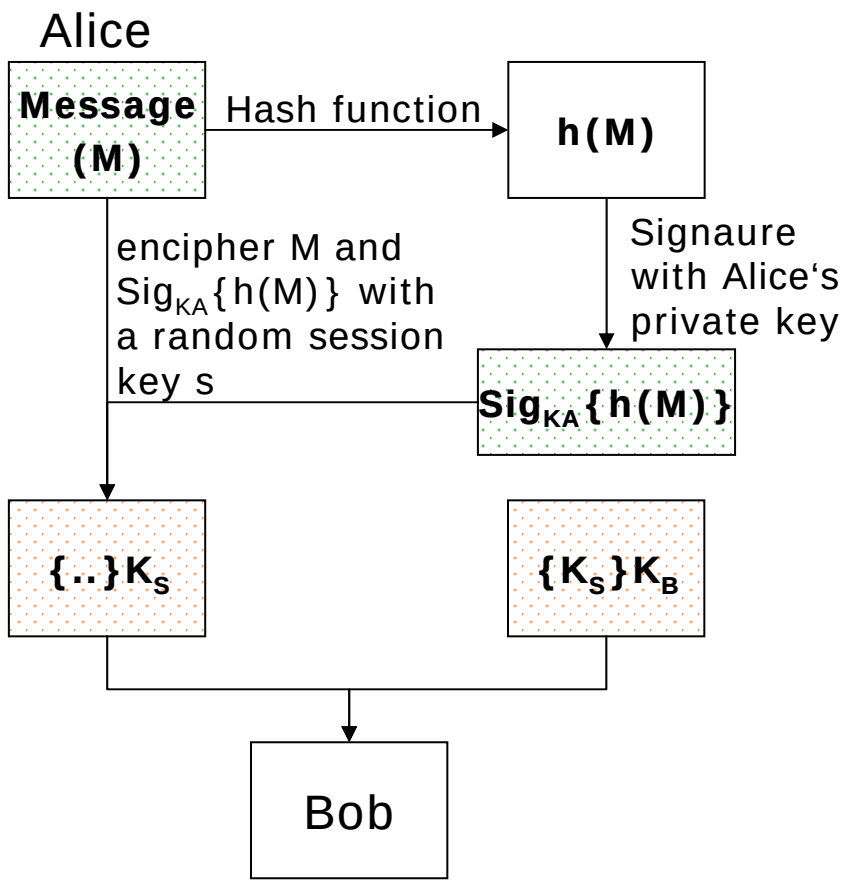
- Kerberos is an authentication protocol using symmetric encryption.
- The name Kerberos comes from Greek mythology: Kerberos is the three-headed dog that guarded the entrance to Hades.
- In computer security, three heads represent client, server and KDC (key distribution center).

Kerberos


User
Alice
Username, Password
Require access to B
Server
A requires access to B
{T_S, L, K_AB, B, {T_S, L, K_AB, A} K_BS}K_AS
KDC
{T_A+1}K_AB
{T_S, L, K_AB, A} K_BS, {A, T_A}K_AB
B

PGP (Pretty Good Privacy)

- PGP is a secure mail protocol. It was invented by Phil Zimmermann in 1991.
- PGP uses both public key encryption and private key encryption.
- PGP is used in Evolution, Eudora, Mozilla Thunderbird.
- Plug-ins implementing PGP is also available for Outlook Express.



Conclusion

- Security Primitives
  - Confidentiality, Authentication, Integrity, Availability
- Methods and Protocols
  - Encryption, Hash Function, Digital Signature, Kerberos, PGP
- Security is only a relative concept