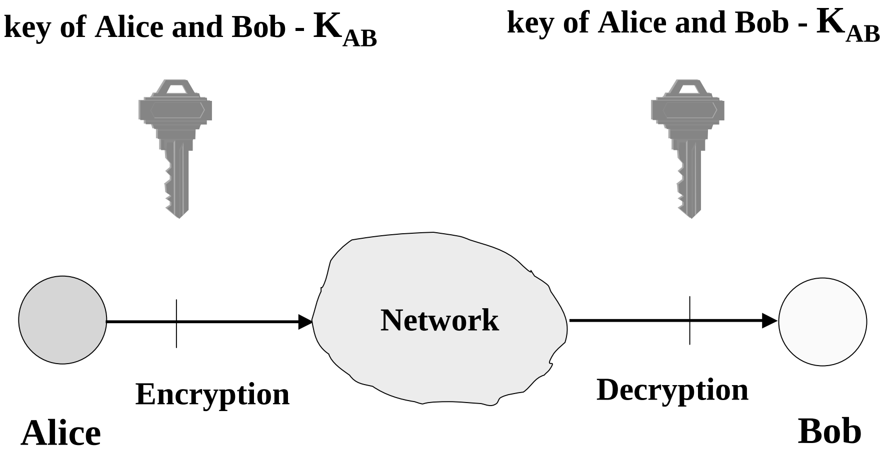
ECE297:11 - Lecture 2

Types of Cryptosystems

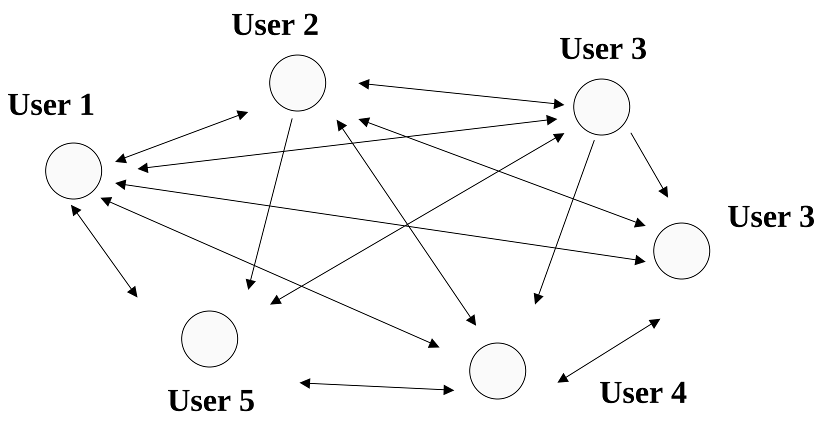
Implementation of Security Services

Secret-key vs. public-key ciphers

Secret-key (Symmetric) Cryptosystems



Key Distribution Problem



N - Users ⇨ $\frac{N \cdot (N-1)}{2}$ Keys

Users	Keys
100	5,000
1000	500,000

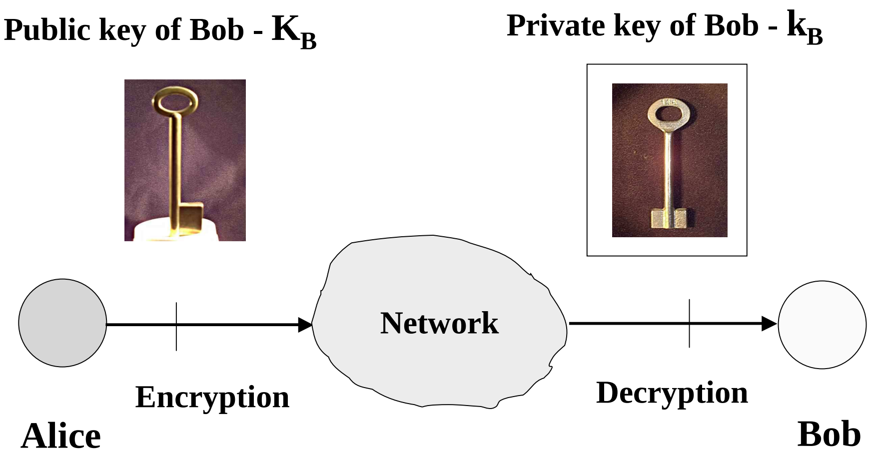
Digital Signature Problem

Both corresponding sides have the same information and are able to generate a signature

There is a possibility of the

- **receiver falsifying the message**
- **sender denying that he/she sent the message**

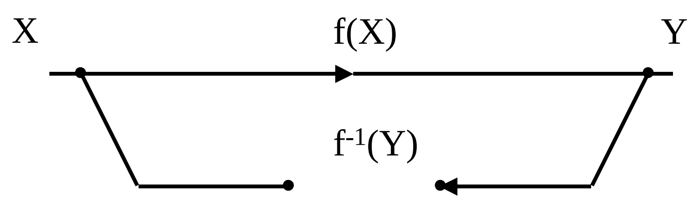
Public Key (Asymmetric) Cryptosystems



Classification of cryptosystems
Terminology

secret-key	*public key*
symmetric	*asymmetric*
symmetric-key	
classical	
conventional	

One-way function



EXAMPLE:

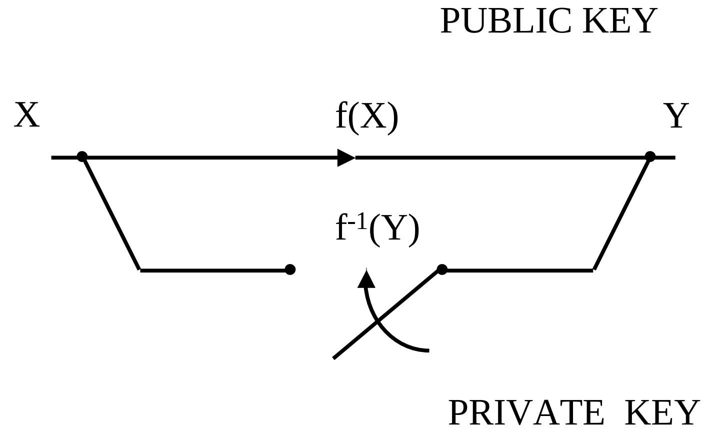
$$f: Y=f(X) = A^X \bmod P$$

where P and A are constants, P is a large prime,
A is an integer smaller than P

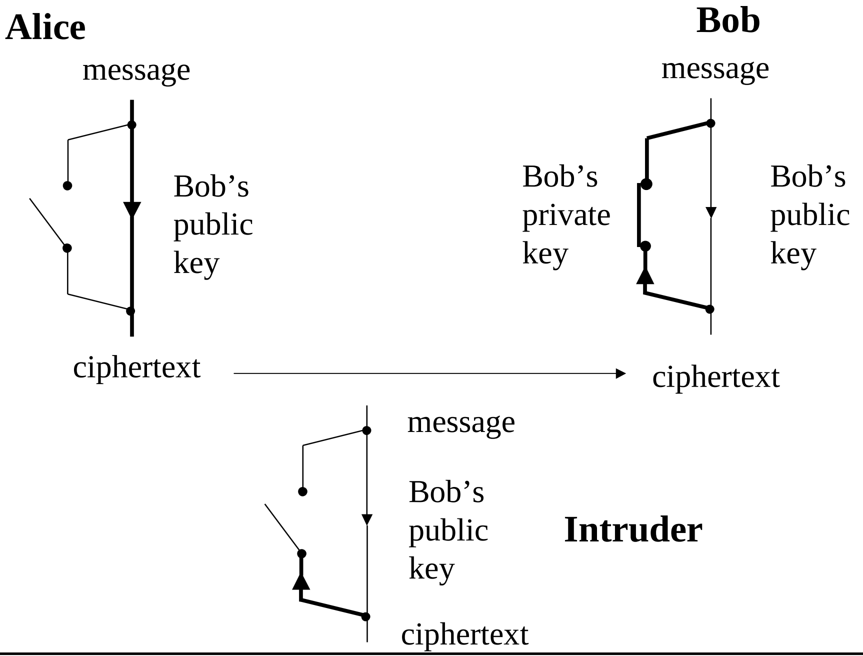
Number of bits of P	Average number of multiplications necessary to compute	
	f	**f^{-1}**
1000	1500	10^{30}

Trap-door one-way function

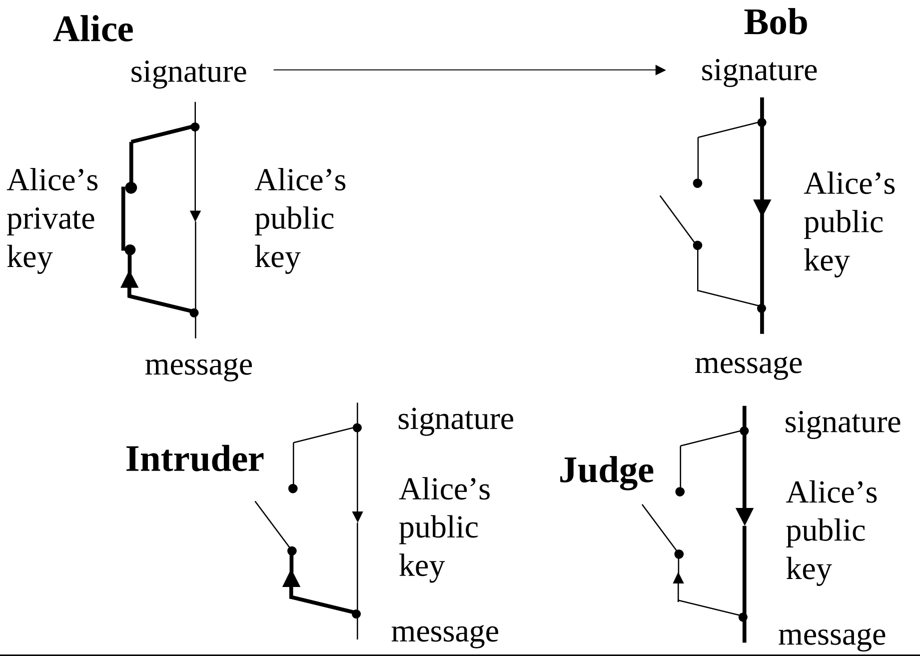
Whitfield Diffie and Martin Hellman
"New directions in cryptography," 1976



Key Distribution

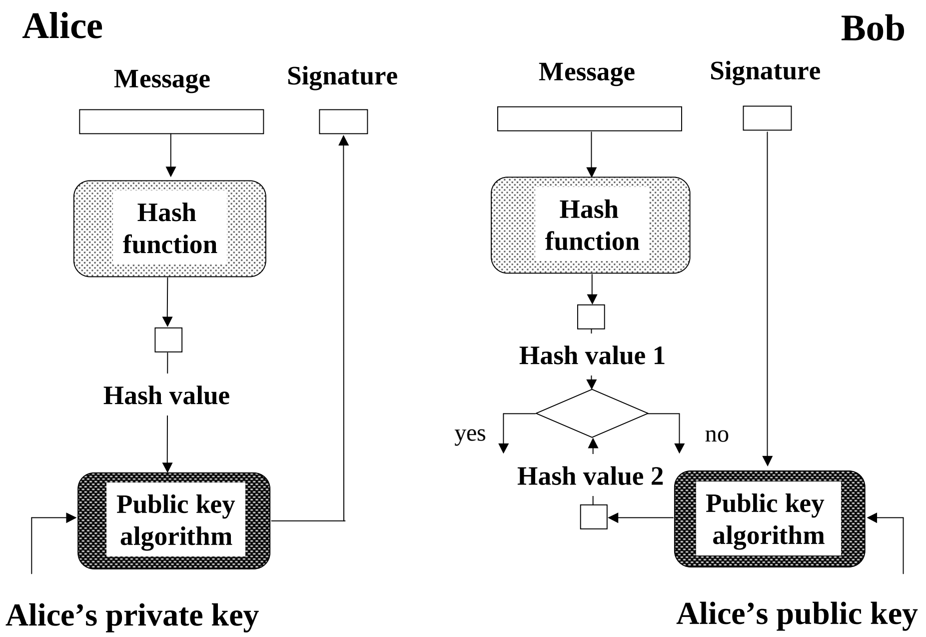


Digital Signature

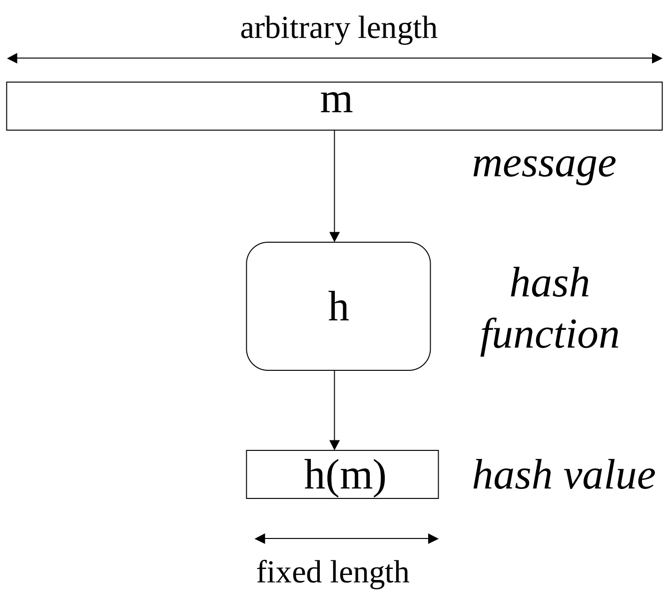


Implementation of Security Services

Non-repudiation



Hash function



Hash functions

Basic requirements

1. Public description, NO key

2. Compression

   arbitrary length input $\rightarrow$ fixed length output

3. Ease of computation

Hash functions

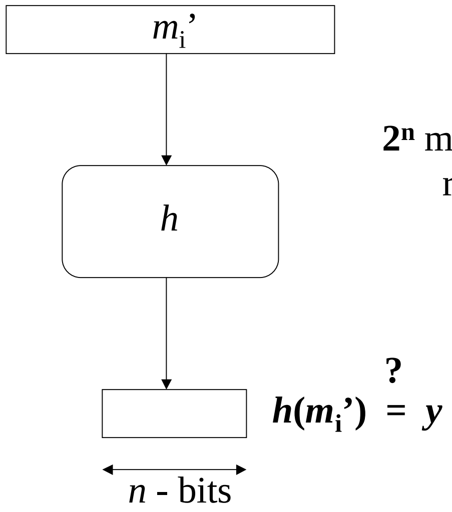
Security requirements

It is computationally infeasible

	Given	To Find
1. Preimage resistance	$h(m)$	m
2. 2nd preimage resistance	m and $h(m)$	$m' \neq m$, such that $h(m') = h(m)$
3. Collision resistance		$m' \neq m$, such that $h(m') = h(m)$

Brute force attack against One-Way Hash Function

Given *y*



i=1..2^n

2^n messages with the contents required by the forger

Creating multiple versions of the required message

I {state / confirm} {thereby / -} that I {borrowed / received}

{$10,000 / ten thousand dollars} from {Mr. / Dr.} {Kris / Krzysztof}

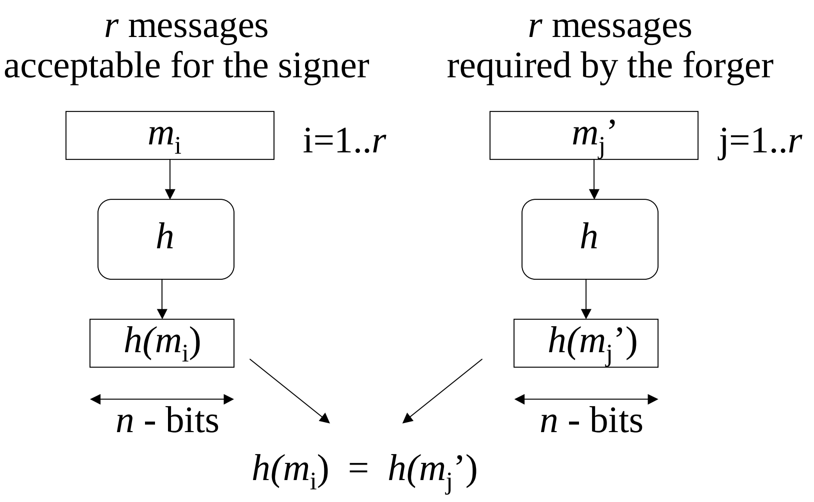
Gaj on {June 4, / 06 / 04} 2002. This {money / sum of money}

{should / is required to} be {returned / given back} to {Mr. / Dr.} Gaj

by the {end / middle} of {June / July} .

Brute force attack against Collision Resistant Hash Function

Yuval



Message required by the forger

I {state / confirm} {thereby / -} that I {borrowed / received}

{$10,000 / ten thousand dollars} from {Mr. / Dr.} {Kris / Krzysztof}

Gaj on {June 4, / 06 / 04} 2002. This {money / sum of money}

{should / is required to} be {returned / given back} to {Mr. / Dr.} Gaj

by the {end / middle} of {June / July} .

Message acceptable for the signer

$$\text{I} \left\{\begin{array}{l}\text{state}\\ \text{confirm}\end{array}\right\} \left\{\begin{array}{l}\text{thereby}\\ \text{-}\end{array}\right\} \text{ that on } \left\{\begin{array}{l}\text{June 4,}\\ \text{06 / 04}\end{array}\right\} \text{ 2001}$$

$$\text{I} \left\{\begin{array}{l}\text{borrowed}\\ \text{received}\end{array}\right\} \text{ from } \left\{\begin{array}{l}\text{Mr.}\\ \text{Dr.}\end{array}\right\} \left\{\begin{array}{l}\text{Kris}\\ \text{Krzysztof}\end{array}\right\} \text{ a } \left\{\begin{array}{l}\text{book}\\ \text{manuscript}\end{array}\right\}$$

$$\text{on} \left\{\begin{array}{l}\text{fast}\\ \text{efficient}\end{array}\right\} \left\{\begin{array}{l}\text{implementations}\\ \text{realizations}\end{array}\right\} \text{ of } \left\{\begin{array}{l}\text{ciphers}\\ \text{cryptosystems}\end{array}\right\} .$$

$$\text{This} \left\{\begin{array}{l}\text{text}\\ \text{book}\end{array}\right\} \left\{\begin{array}{l}\text{should}\\ \text{is required to}\end{array}\right\} \text{ be } \left\{\begin{array}{l}\text{returned}\\ \text{given back}\end{array}\right\}$$

$$\text{to} \left\{\begin{array}{l}\text{Mr.}\\ \text{Dr.}\end{array}\right\} \text{ Gaj by the } \left\{\begin{array}{l}\text{end}\\ \text{middle}\end{array}\right\} \text{ of } \left\{\begin{array}{l}\text{November}\\ \text{December}\end{array}\right\} .$$

Birthday paradox

How many students there must be in a class for there be a greater than 50% chance that

1. *one of the students shares the teacher's birthday (day and month)?*
2. *any two of the students share the same birthday (day and month)?*

Birthday paradox

How many students there must be in a class for there be a greater than 50% chance that

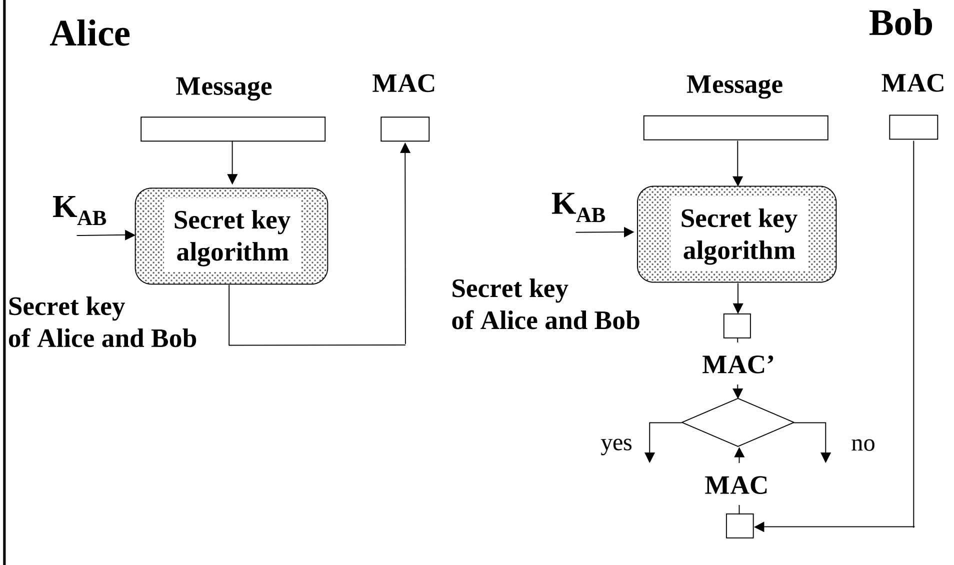
1. one of the students shares the teacher's birthday (day and month)?

~ 366/2 = 188

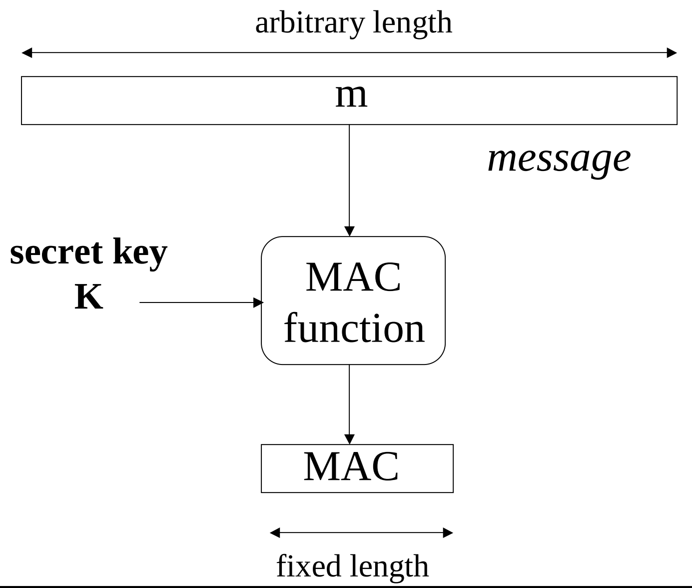
2. any two of the students share the same birthday (day and month)?

$$\sim\sqrt{366} \approx 19$$

Authentication



MAC - Message Autentication Codes (keyed hash functions)



MAC functions

Basic requirements

1. Public description, SECRET key parameter

2. Compression

   arbitrary length input → fixed length output

3. Ease of computation

MAC functions

Security requirements

Given zero or more pairs

$$m_i, MAC(m_i) \qquad i = 1..k$$

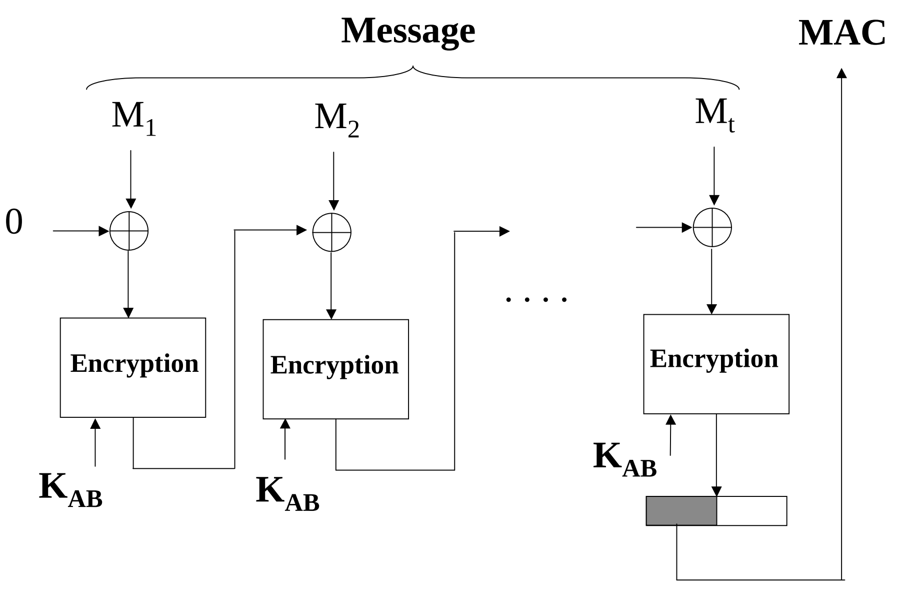
it is computationally impossible to find any new pair

$$m', MAC(m')$$

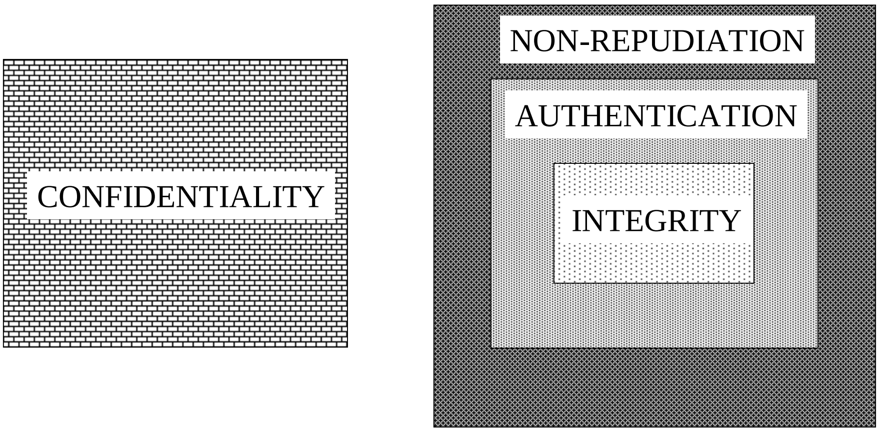
Such that

$$m' \neq m_i \qquad i = 1..k$$

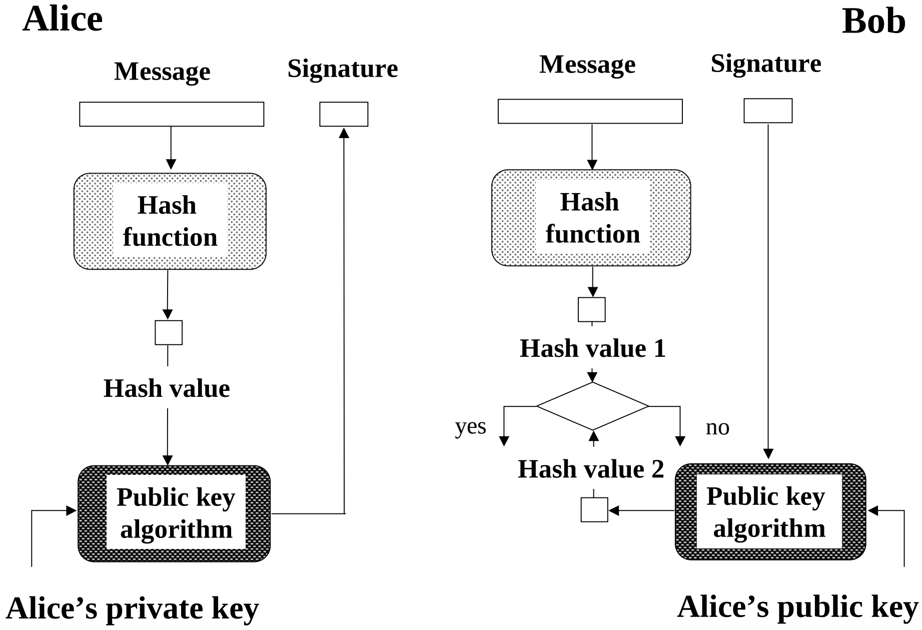
CBC-MAC (Cipher Block Chaining MAC)



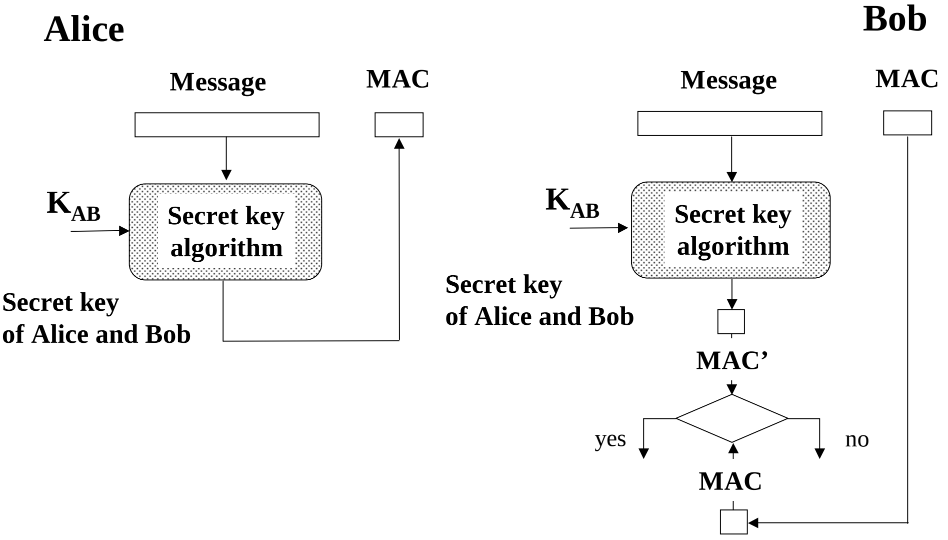
Relations among security services



Non-repudiation

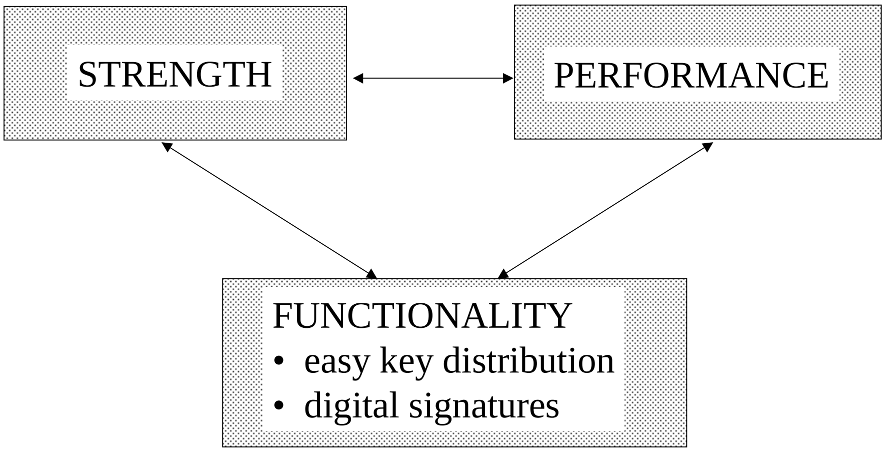


Authentication

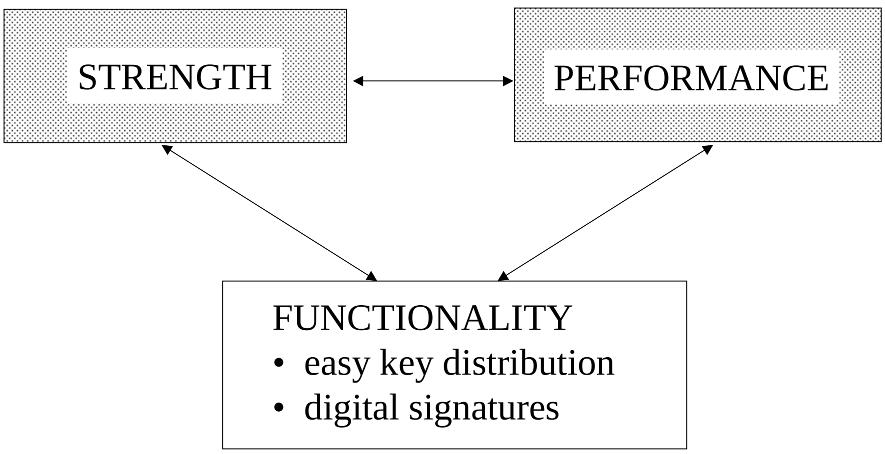


Hybrid Systems

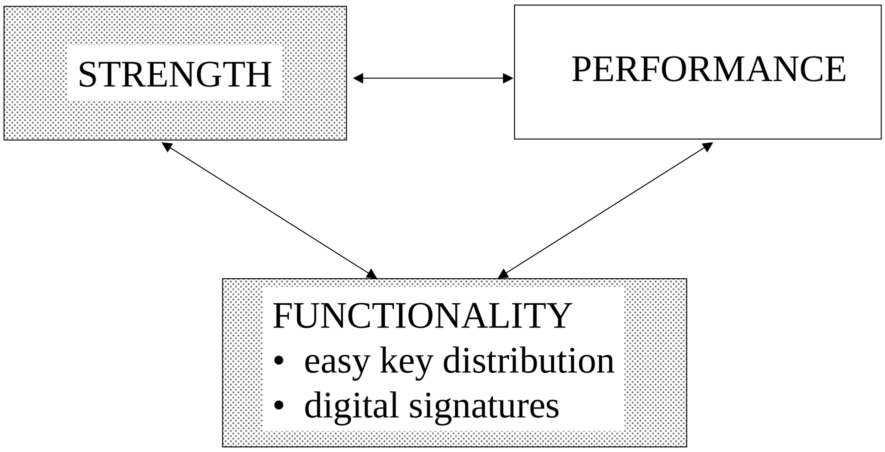
Features required from today's ciphers



Features of secret-key ciphers



Features of public-key ciphers



Ciphering and Deciphering Speed

on average

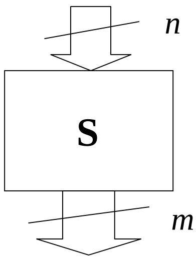
for implementations based on the same technology

	software	**hardware**
$\frac{\text{DES deciphering speed}}{\text{RSA deciphering speed}}$	≈ 100	≈ 1000

Basic operations of secret key ciphers - S-box

Software | **Hardware**

S-box ***n*** **x** ***m***



Substitution

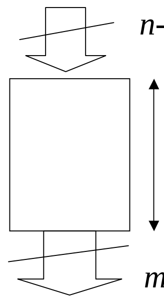
C

```
WORD S[1<<n]=
{ 0x23, 0x34, 0x56
  . . . . . . . . . . . . . .
}
```

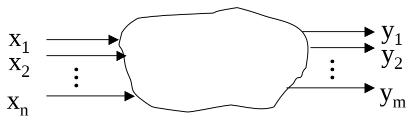
ASM

```
S   DW  23H, 34H,
        56H
        …..
```

ROM



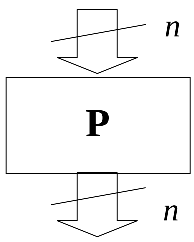
direct logic



Basic operations of secret key ciphers - P-box

Software | **Hardware**

P-box ***n*** **x** ***n***



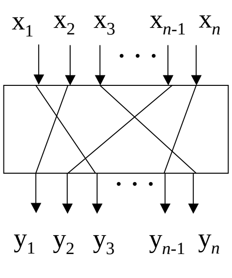
Permutation

C

sequence of instructions
<<, |, &

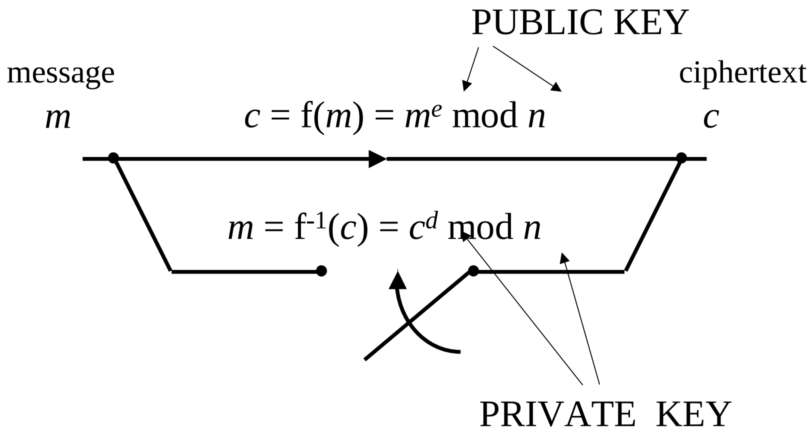
ASM

sequence of instructions
ROL, OR, AND



order of wires

RSA as a trap-door one-way function



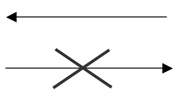
$n = p \cdot q$ $\qquad$ p, q - large prime numbers

$e \cdot d \equiv 1 \mod ((p-1)(q-1))$

RSA keys

PUBLIC KEY $\qquad$ **PRIVATE KEY**

$\{\, e, n \,\}$ $\qquad$ $\{\, d, p, q \,\}$



$n = p \cdot q$ $\qquad$ p, q - large prime numbers

$e \cdot d \equiv 1 \mod ((p-1)(q-1))$

Basic Operations of
the Public Key Cryptosystem RSA

Encryption

public key exponent

ciphertext = **plaintext** **mod** **public key modulus**

k-bits *k*-bits *k*-bits

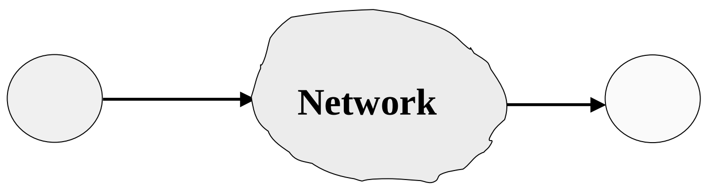
Decryption

private key exponent

ciphertext = **plaintext** **mod** **private key modulus**

k-bits *k*-bits *k*-bits

Hybrid Systems



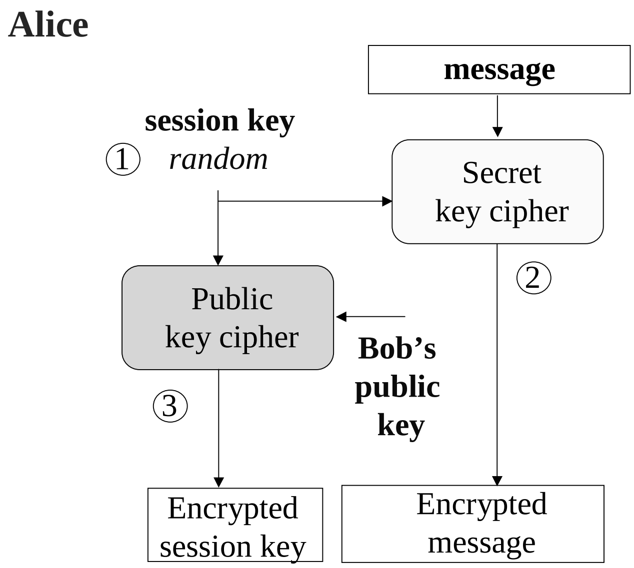
Alice | **Bob**

Bob's public key **session key** *random* | **Bob's private key**

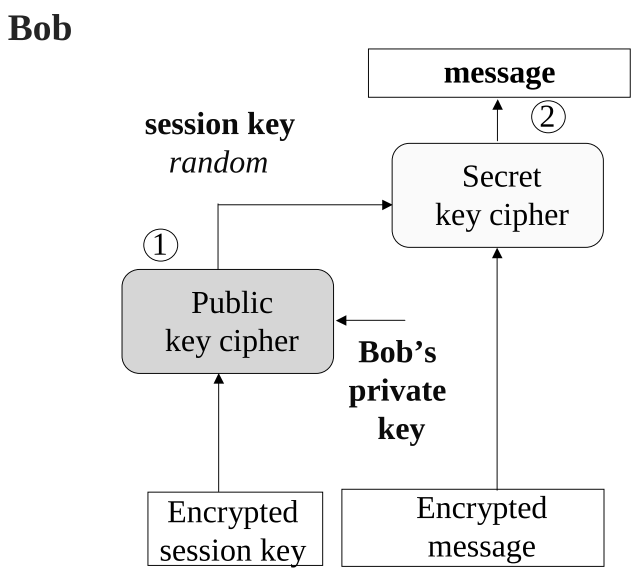
Encrypted session key | Encrypted message | Encrypted session key | Encrypted message

RSA public key DES session key

Hybrid Systems - Sender's Side (2)

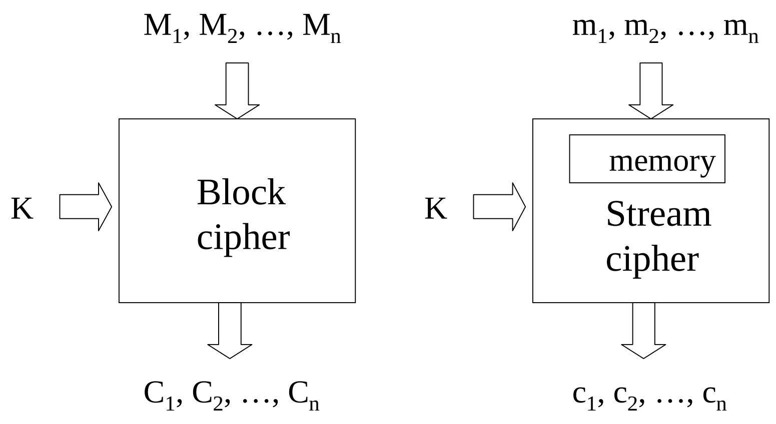


Hybrid Systems - Receiver's Side (2)



Block vs. stream ciphers

Block vs. stream ciphers



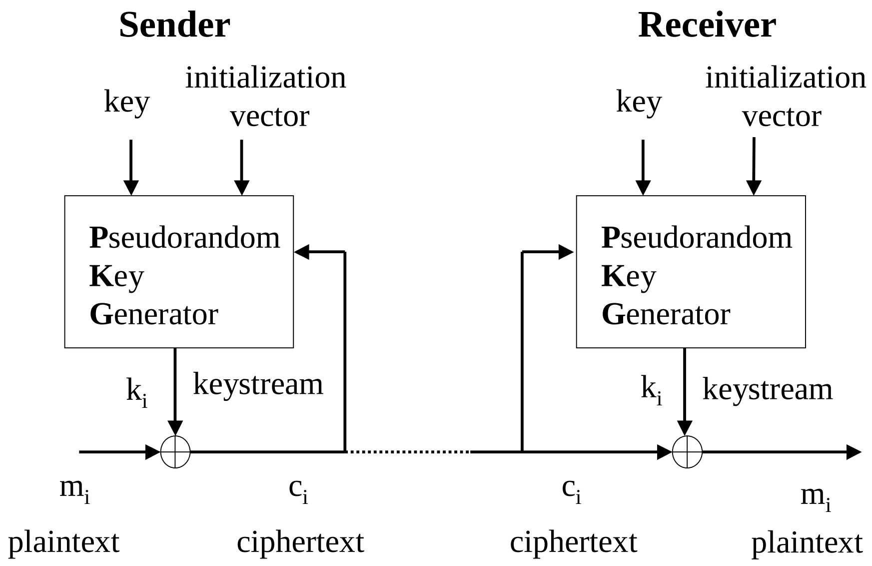
$C_i=f_K(M_i)$

Every block of ciphertext is a function of only **one** corresponding **block** of plaintext

$c_i = f_K(m_i, m_{i-1}, \ldots, m_2, m_1)$

Every block of ciphertext is a function of the **current and all proceeding blocks** of plaintext

Typical stream cipher



Evaluating the security of secret-key ciphers

Classification of attacks (1)

Ciphertext-only attack

Given:

ciphertext

Looked for:

plaintext

or key

Example:

Frequency analysis of letters in the ciphertext
(effective only for most simple historical ciphers)

Classification of attacks (2)

Known plaintext attack

Given:

ciphertext

guessed fragment of the plaintext

Looked for:

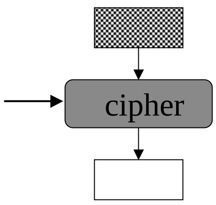
remaining plaintext

or key

Example:

exhaustive key search
(brute-force) attack

successive keys

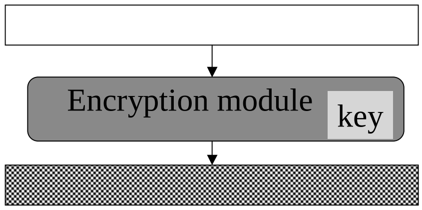


Classification of attacks (3)

Chosen plaintext attack

Given:

Capability to encipher an arbitrarily chosen fragment of the plaintext

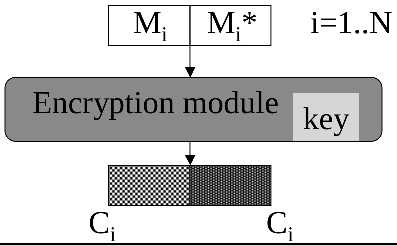


Looked for:

key

Example:

Differential cryptanalysis

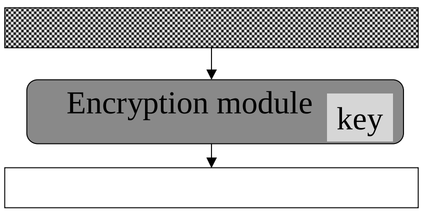


Classification of attacks (4)

Chosen ciphertext attack

Given:

Capability to decipher an arbitrarily chosen fragment of the ciphertext



Looked for:

key