

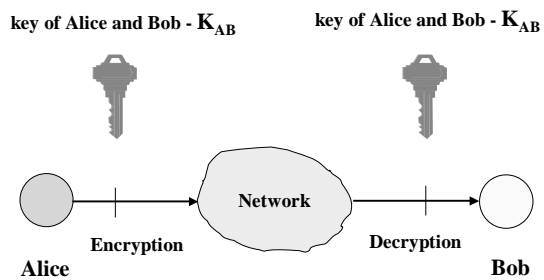
ECE297:11 - Lecture 2

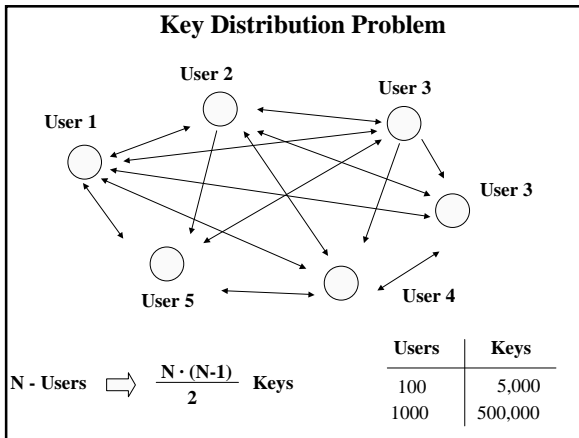
Types of Cryptosystems

**Implementation of
Security Services**

Secret-key vs. public-key ciphers

Secret-key (Symmetric) Cryptosystems



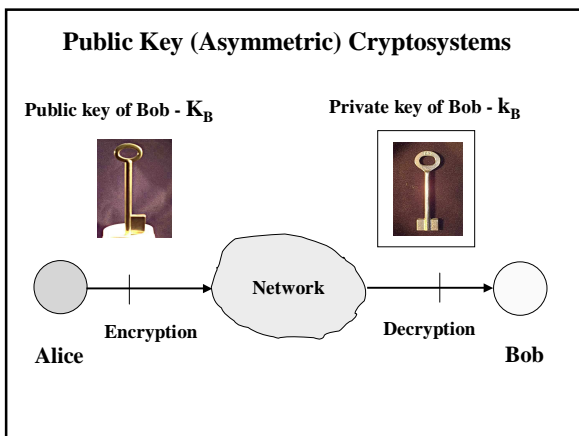


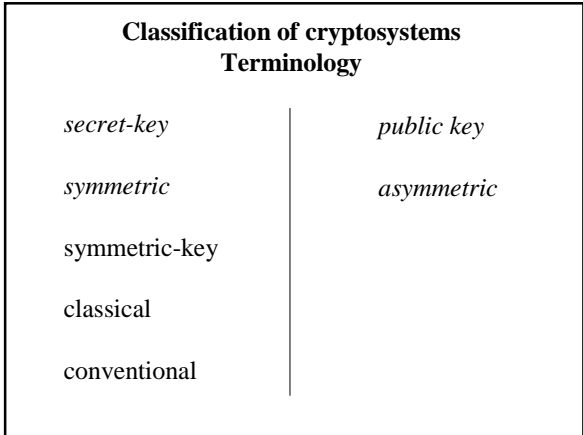
Digital Signature Problem

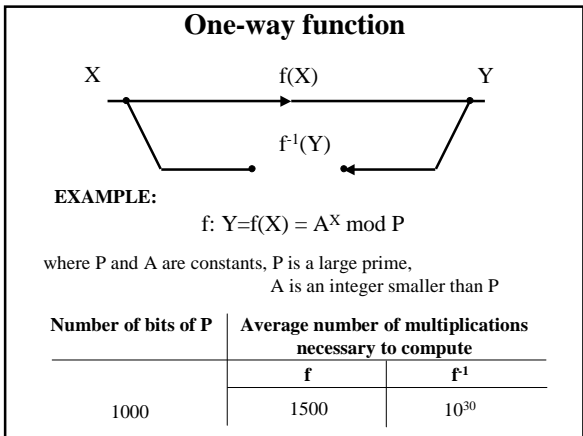
Both corresponding sides have the same information and are able to generate a signature

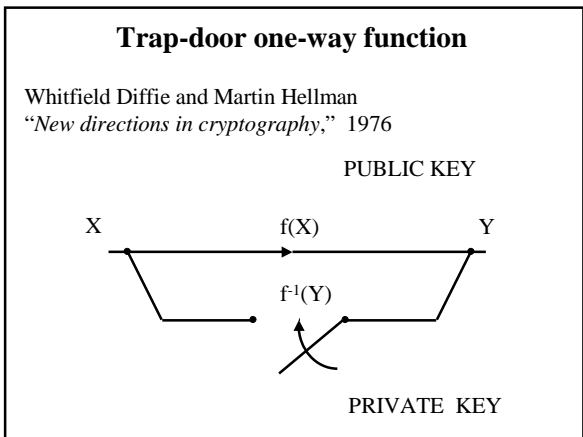
There is a possibility of the

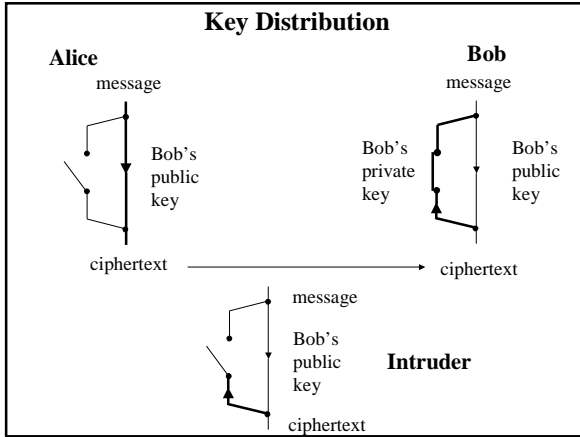
- receiver falsifying the message
- sender denying that he/she sent the message

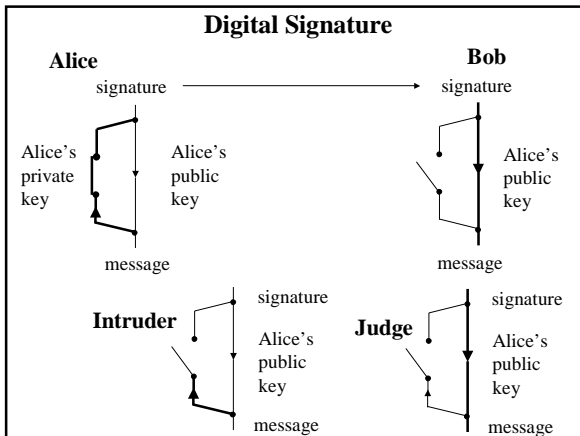




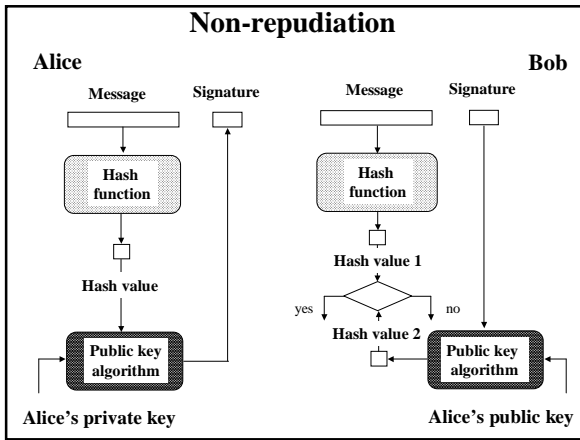


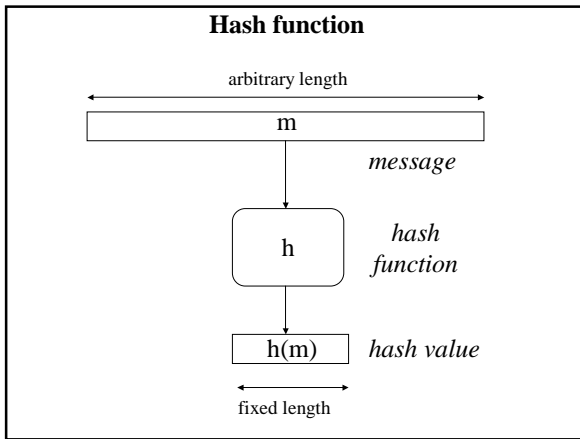






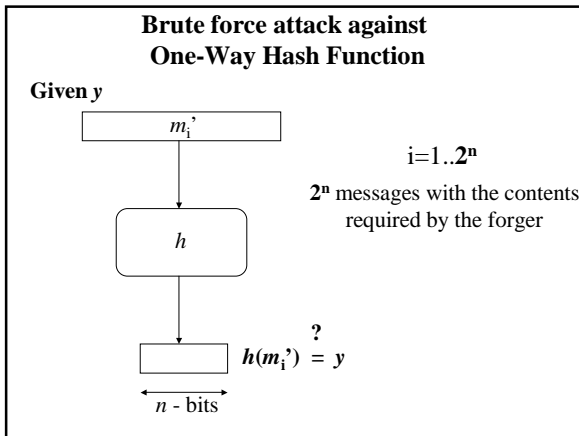
Implementation of Security Services





- ### 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 $h(m') = h(m)$



Creating multiple versions of the required message

I {state} {thereby} that I {borrowed}

{confirm} {-} {received}

{ \$10,000 } from {Mr.} {Kris}

{ten thousand dollars} {Dr.} {Krzysztof}

Gaj on {June 4,} 2002. This {money}

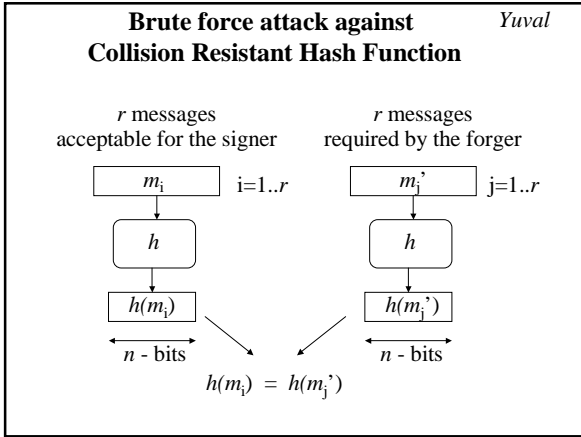
{06 / 04} {sum of money}

{should} be {returned} to {Mr.} Gaj

{is required to} {given back} {Dr.}

by the {end} of {June}

{middle} {July}



Message required by the forger

I {state} {thereby} that I {borrowed}

{confirm} {-} {received}

{ \$10,000 } from {Mr.} {Kris}

{ten thousand dollars} {Dr.} {Krzysztof}

Gaj on {June 4,} 2002. This {money}

{06 / 04} {sum of money}

{should} be {returned}

{is required to} {is required to} {given back} to {Mr.} Gaj

{Dr.}

by the {end} of {June}

{middle} {July} .

Message acceptable for the signer

I {state} {thereby} that on {June 4,} 2001

{confirm} {-} {received}

I {borrowed} from {Mr.} {Kris}

{received} {Dr.} {Krzysztof} a {book}

on {fast} {implementations} of {ciphers}

{efficient} {realizations} {cryptosystems} .

This {text} {should}

{book} {is required to} be {returned}

to {Mr.} Gaj by the {end} of {November}

{Dr.} {middle} {December} .

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

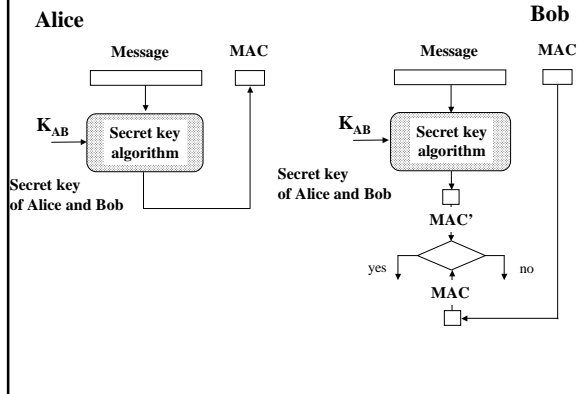
1. one of the students shares the teacher's birthday (day and month)?

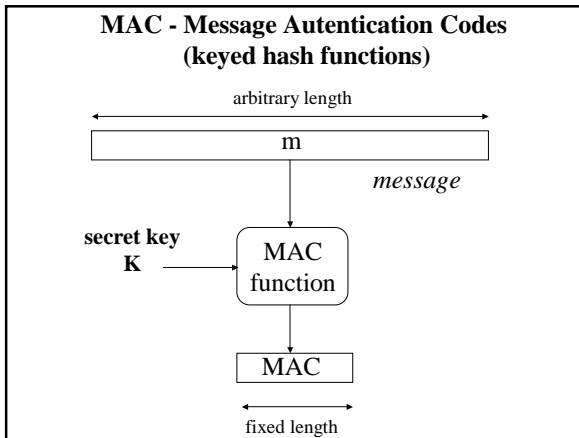
$$\sim 366/2 = 188$$

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

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

Authentication





- 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

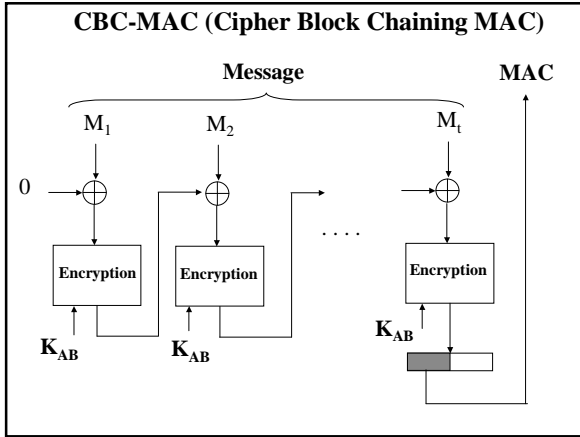
$$m_i, \text{MAC}(m_i) \quad i = 1..k$$

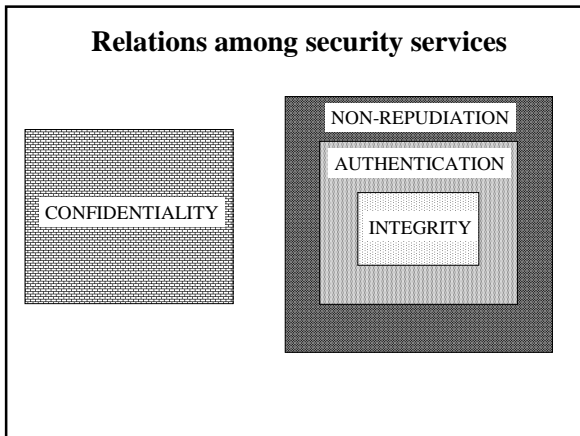
it is computationally impossible to find any new pair

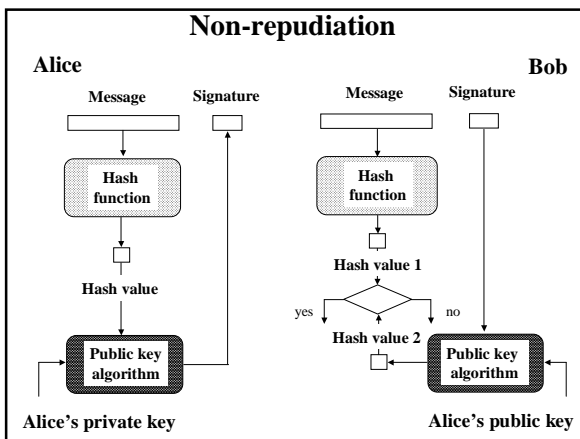
$$m', \text{MAC}(m')$$

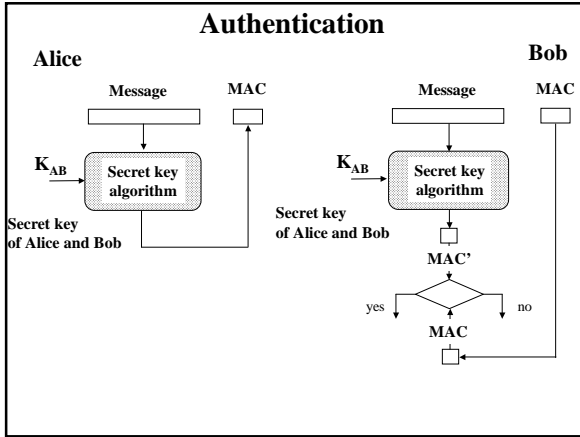
Such that

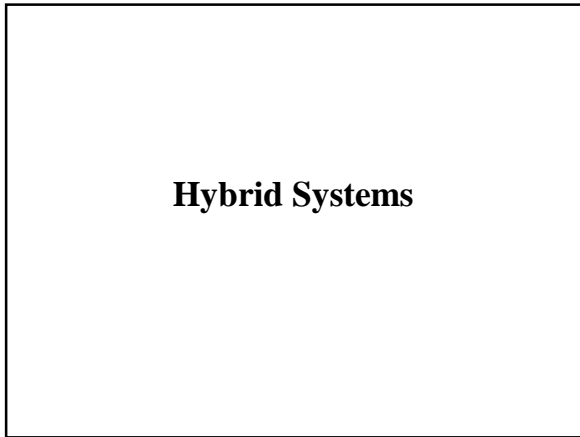
$$m' \neq m_i \quad i = 1..k$$

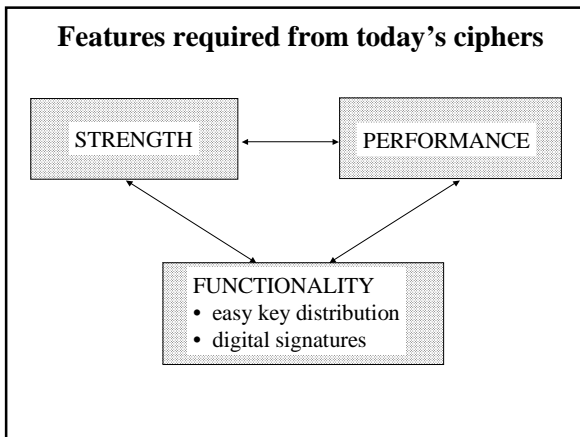


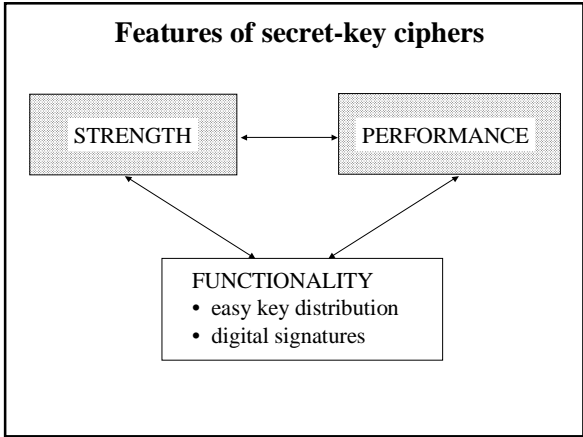


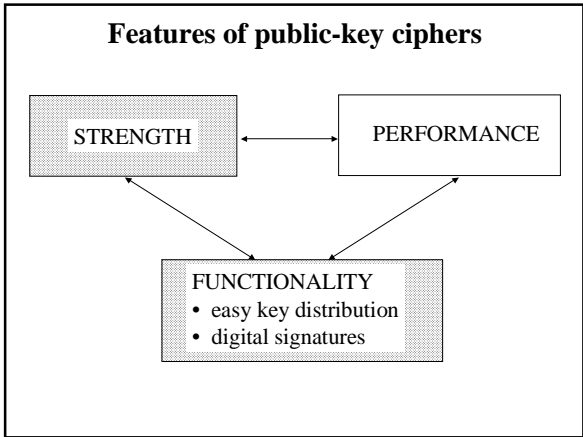






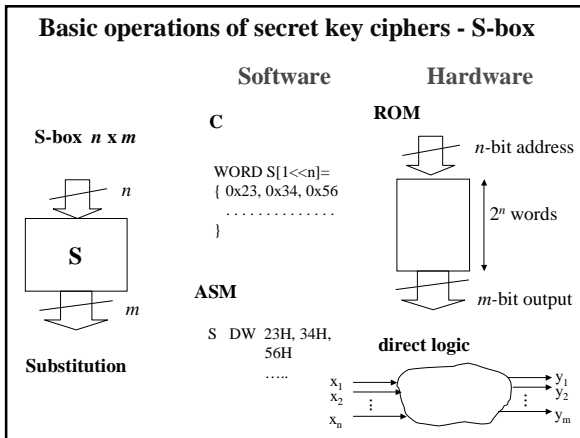


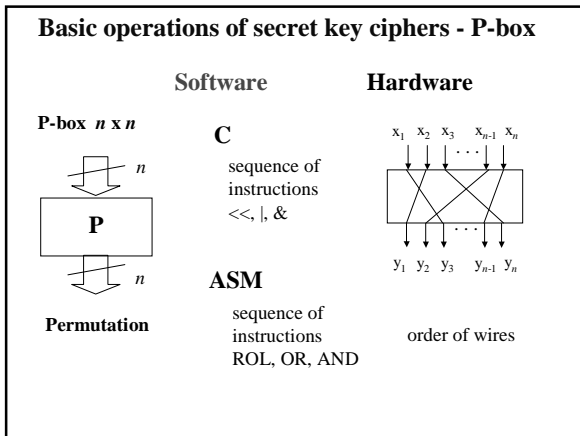


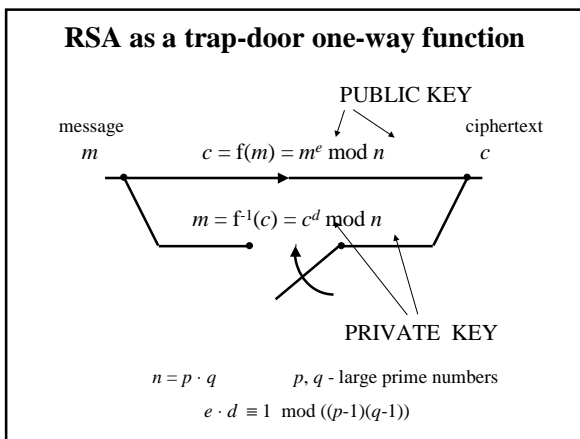


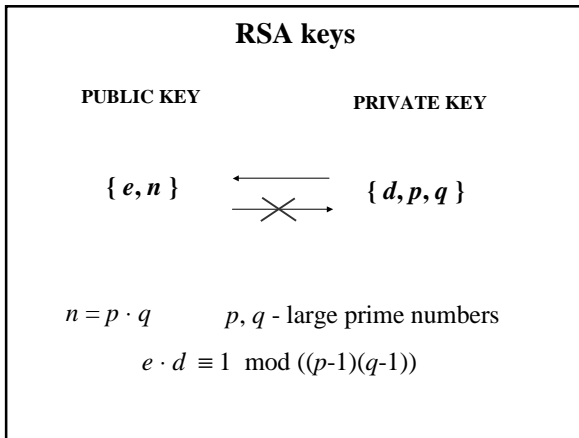
Ciphering and Deciphering Speed
on average
for implementations based on the same technology

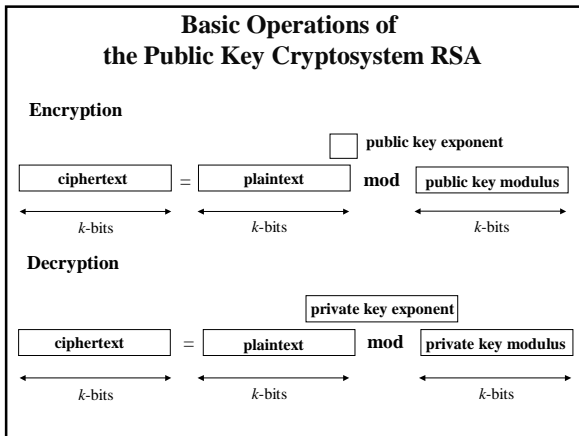
	software	hardware
DES deciphering speed	≈ 100	≈ 1000
RSA deciphering speed		

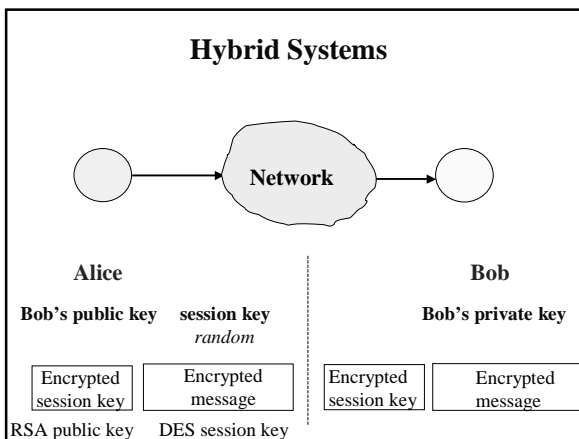






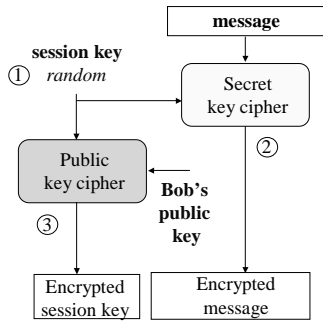






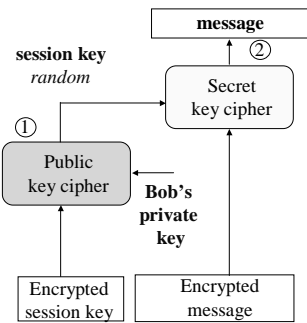
Hybrid Systems - Sender's Side (2)

Alice

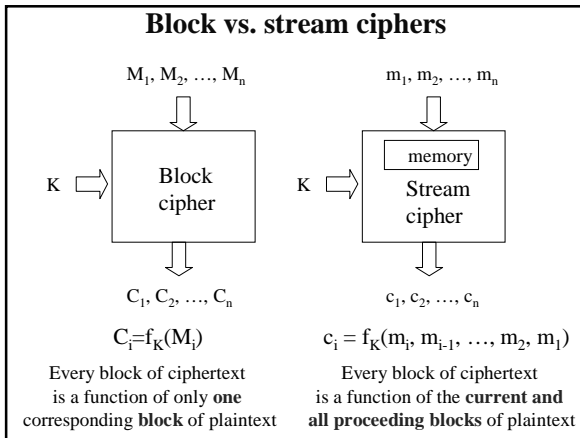


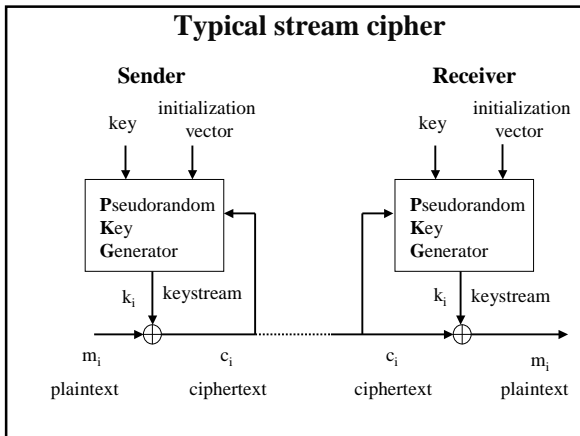
Hybrid Systems - Receiver's Side (2)

Bob



Block vs. stream ciphers



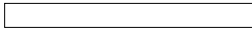


Evaluating the security of secret-key ciphers

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

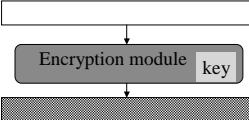
Example:
exhaustive key search (brute-force) attack

successive keys → 

Classification of attacks (3)

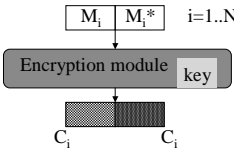
Chosen plaintext attack

Given: Capability to encipher an arbitrarily chosen fragment of the plaintext



Looked for: key

Example: Differential cryptanalysis

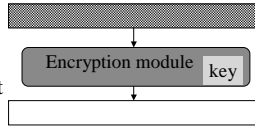


Classification of attacks (4)

Chosen ciphertext attack

Given:

Capability to decipher
an arbitrarily chosen
fragment of the ciphertext



Looked for:

key
