

ECE 646 - Lecture 3

Types of Cryptosystems

Implementation of Security Services

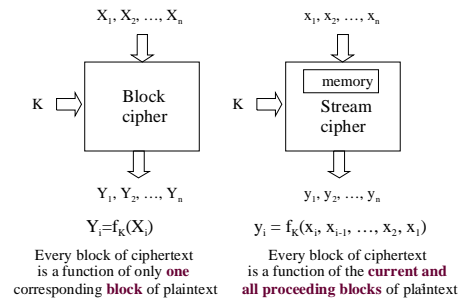
1

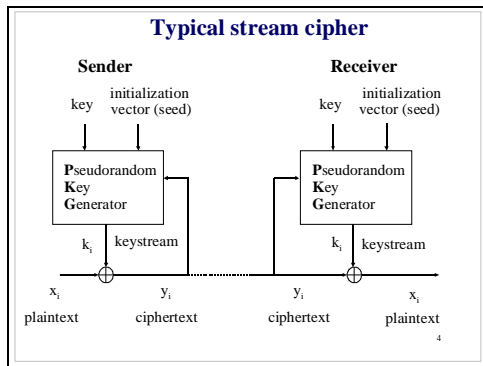
Types of Cryptosystems (1)

Block vs. stream ciphers

2

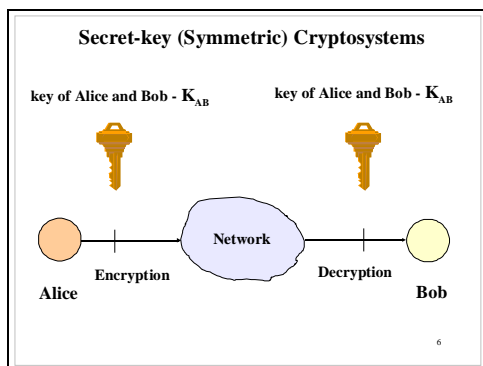
Block vs. stream ciphers





Types of Cryptosystems (2)

Secret-key vs. public-key ciphers



Key Distribution Problem

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

Public key of Bob - K_B

Private key of Bob - k_B

Alice

Encryption

Network

Decryption

Bob

**Classification of cryptosystems
Terminology**

<i>secret-key</i>	<i>public key</i>
<i>symmetric</i>	<i>asymmetric</i>
symmetric-key	
classical	
conventional	

10

One-way function

EXAMPLE: $f: Y=f(X) = A^X \text{ mod } P$

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

11

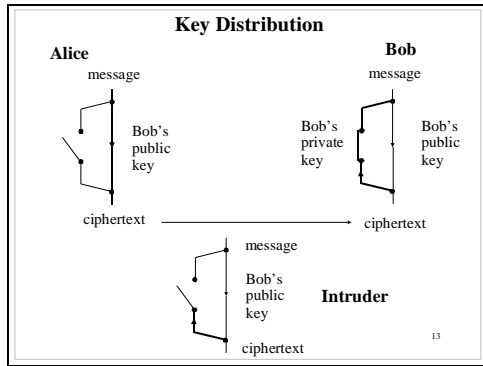
Trap-door one-way function

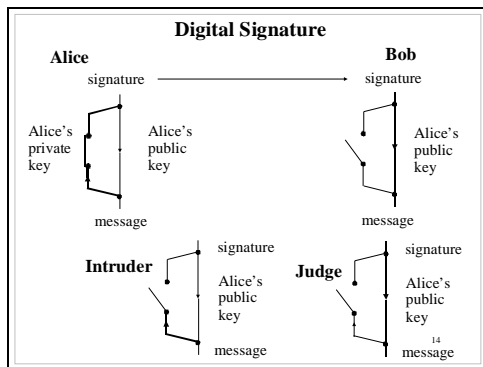
Whitfield Diffie and Martin Hellman
"New directions in cryptography," 1976

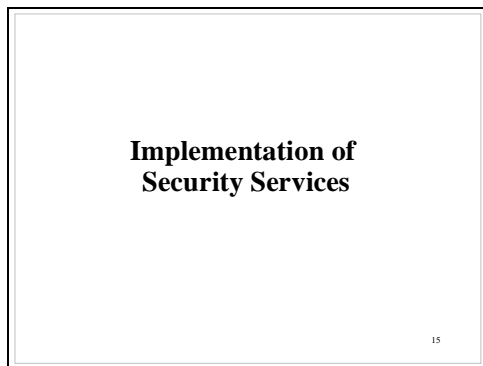
PUBLIC KEY

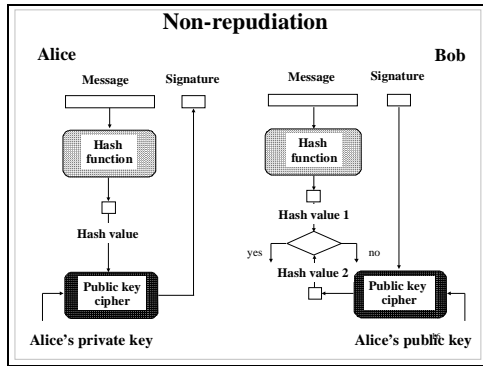
PRIVATE KEY

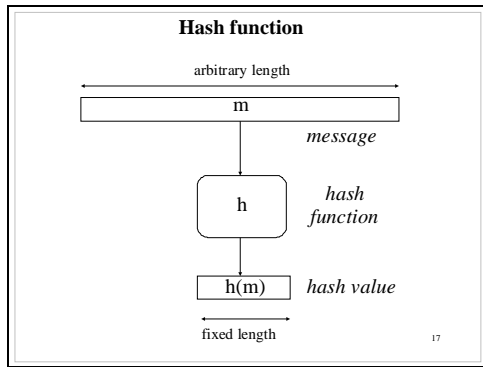
12











- ### Hash functions
- Basic Requirements
 - 1) Public description, no key.
 - 2) $h(m)$ can be applied to any size m .
 - 3) $h(m)$ produces fixed length output.
 - 4) $h(m)$ is easy to compute (hw and sw).

Hash functions

Why not use error correcting codes?

19

Hash functions
Security requirements
It is computationally infeasible

Property	Given	To Find
One-way	$h(m)$	m
Weak collision resistant	m and $h(m)$	$m' \neq m$, such that $h(m') = h(m)$
Strong collision resistant		$m' \neq m$, such that $h(m') = h(m)$

20

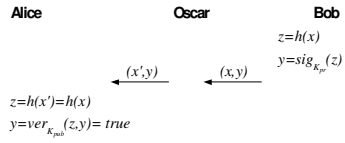
One Way

- Bob sends $E_k(m) || h(m)$ to Alice
- If $h(m)$ is not a one-way function what can Oscar do?

21

Weak collision resistant

- Oscar could replace x with x' .



22

Strong collision resistant

- Oscar could
 - Choose legitimate x_1 and bad x_2 .
 - Alter x_1 and x_2 at "non-visible" locations until $h(x'_1) = h(x'_2)$.
 - Let Bob sign $x'_1 \rightarrow (x'_1, \text{sig}_{k_p}(h(x'_1)))$.
 - Replace $x'_1 \rightarrow x'_2$ and $(x'_2, \text{sig}_{k_p}(h(x'_2)))$

23

Hash functions

Why is there no collision free hash function?

24

Birthday Paradox

- 1st person, P[b'day] = 1
- any person, P[b'day] on a specific date] = $\frac{1}{365}$
- 2nd person, P[b'day \neq 1st person] = $1 - \frac{1}{365} = \frac{364}{365}$
- 3rd person, P[b'day \neq 1st and 2nd] = $1 - \frac{2}{365}$
- P[all 3 have different b'day] = $\left(1 - \frac{1}{365}\right) \left(1 - \frac{2}{365}\right)$
- for 46 ppl: $\left(1 - \frac{1}{365}\right) \left(1 - \frac{2}{365}\right) \dots \left(1 - \frac{45}{365}\right) = 0.052$
- P[no two ppl. have b'day same] = 0.052
i.e. P[two have same b'day] = 94.8% !

25

P[no collisions amongst k elements in a group of size n] = $\prod_{i=1}^{k-1} \left(1 - \frac{i}{n}\right)$

Recall: $e^{-x} = 1 - x + \frac{x^2}{2!} - \frac{x^3}{3!} + \dots$

if $x \ll 1$ $e^{-x} \approx 1 - x$

if $n \gg i$ then for $x = \frac{i}{n}$ $x \ll 1$

$$\prod_{i=1}^{k-1} \left(1 - \frac{i}{n}\right) \approx \prod_{i=1}^{k-1} e^{-\frac{i}{n}} = e^{-\frac{1}{n}} e^{-\frac{2}{n}} \dots e^{-\frac{k-1}{n}} = e^{-\frac{1+2+3+\dots+k-1}{n}}$$

Recall: $1+2+3+\dots+k-1 = \frac{k(k-1)}{2}$

P[no collision] $\approx e^{-\frac{k(k-1)}{2n}}$ P[at least one collision] $\approx 1 - e^{-\frac{k(k-1)}{2n}}$

$$1 - \epsilon \approx e^{-\frac{k(k-1)}{2n}} \quad \ln(1 - \epsilon) \approx -\frac{k(k-1)}{2n} \quad k(k+1) \approx -2n \ln(1 - \epsilon) \approx 2n \ln\left(\frac{1}{1 - \epsilon}\right)$$

26

$$k(k+1) \approx 2n \ln\left(\frac{1}{1 - \epsilon}\right) \quad \text{if } k \gg 1, \text{ then } k^2 \approx k(k+1) \approx 2n \ln\left(\frac{1}{1 - \epsilon}\right)$$

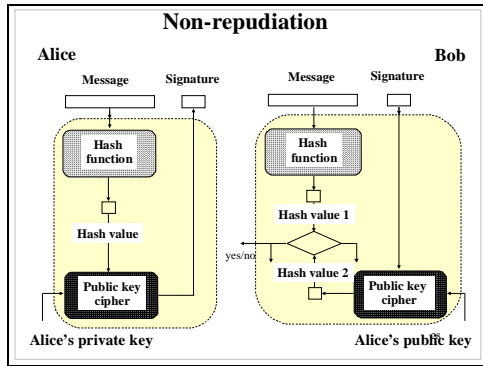
$$k \approx \sqrt{2n \ln\left(\frac{1}{1 - \epsilon}\right)}$$

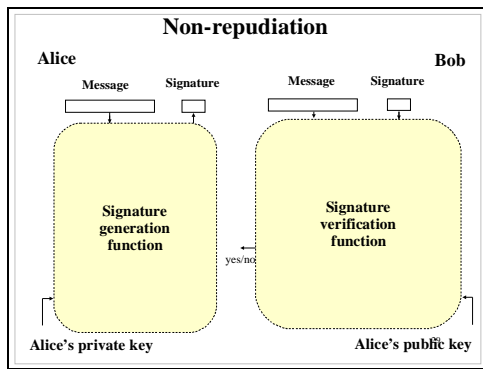
Example:

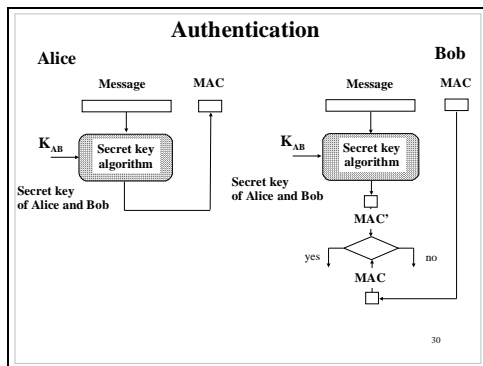
$$k(\epsilon = 0.5) \approx \sqrt{2n \ln\left(\frac{1}{1 - 0.5}\right)} = 1.18\sqrt{n}$$

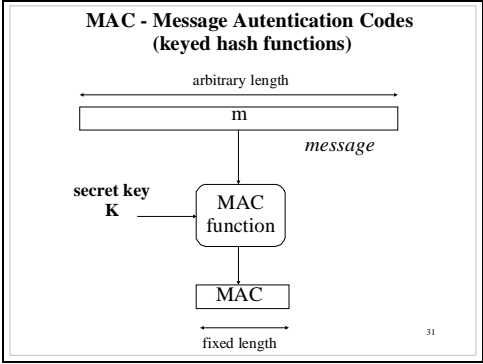
- A collision is found after \sqrt{n} trials with a probability of 50%.
- Hash output space 2^{160} (i.e. 160 bits) then finding collision takes $\sqrt{2^{160}} = 2^{80}$ steps.

27









- MAC functions**
Basic requirements
1. Public description, SECRET key parameter
 2. Compression
arbitrary length input → fixed length output
 3. Ease of computation
- 32

MAC functions
Security requirements

Given zero or more pairs

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

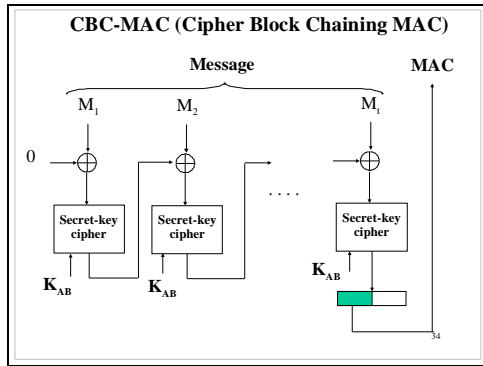
it is computationally impossible to find any new pair

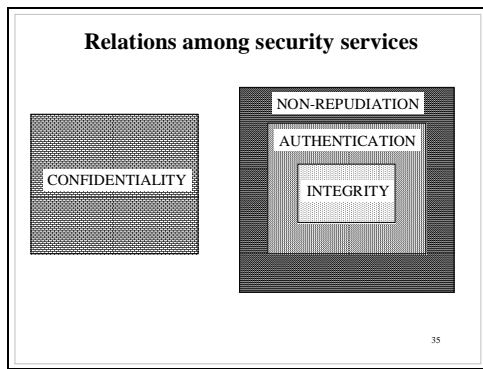
$m', \text{MAC}(m')$

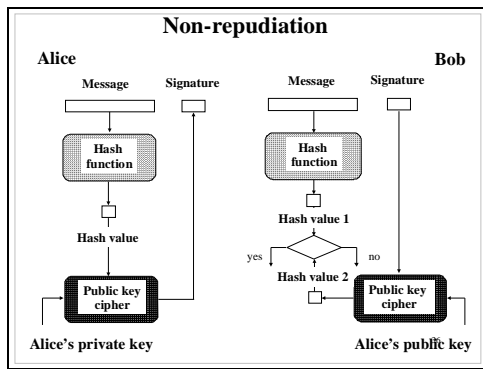
such that

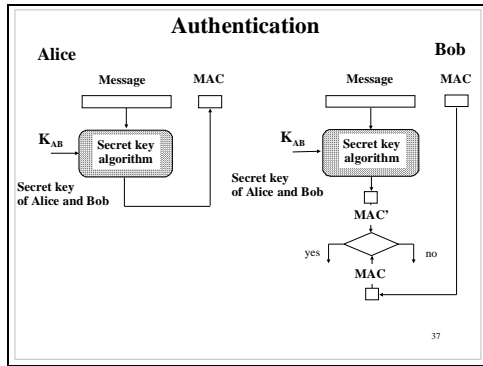
$m' \neq m_i \quad i = 1..k$

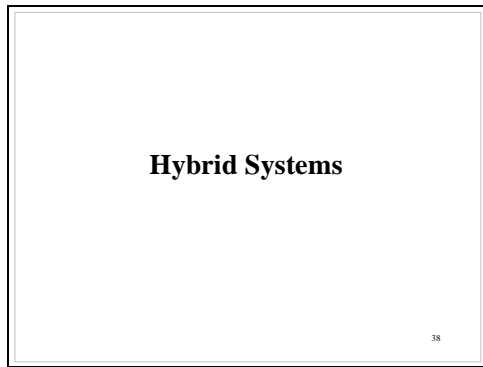
33

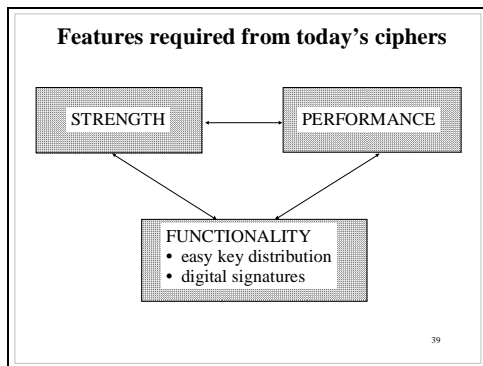


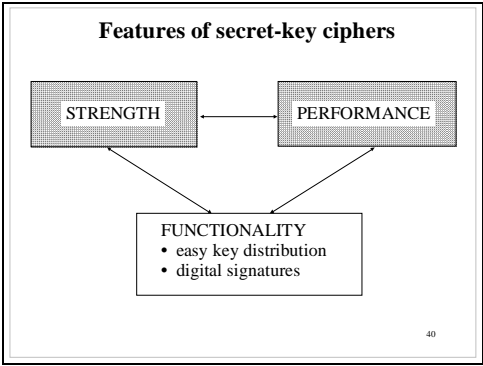


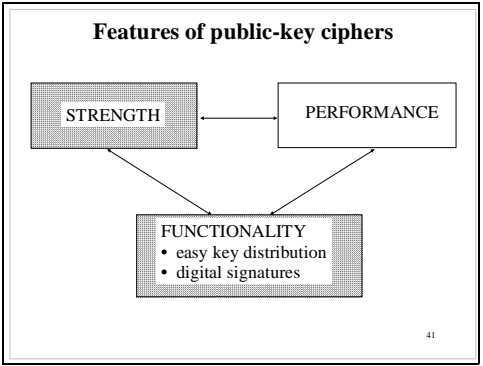










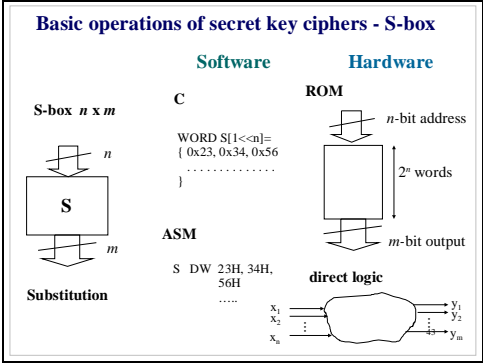


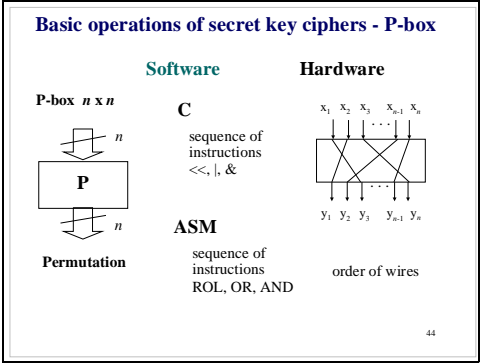
Average Decryption Speed

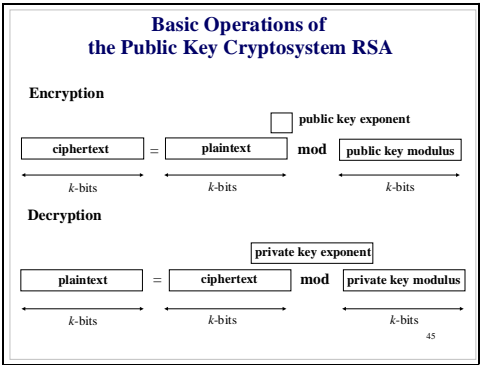
for implementations based on the same technology

	software	hardware
Triple DES deciphering speed		
RSA-1024 deciphering speed	≈ 100	≈ 1000

42







Evaluating the security of secret-key ciphers

49

Classification of attacks (1)

Ciphertext-only attack

Given: ciphertext 


Looked for: plaintext 
or key

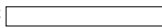
Example:
Frequency analysis of letters in the ciphertext
(effective only for most simple historical ciphers)

50



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 —  

51

Classification of attacks (3)

Chosen plaintext attack

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

Looked for:
 key

Example:
Differential cryptanalysis

52

Classification of attacks (4)

Chosen ciphertext attack

Given:
 Capability to decipher
 an arbitrarily chosen
 fragment of the ciphertext

Looked for:
 key

53
