

# Chapter 8 BASIC CRYPTOGRAPHY

## 8.1 What is cryptography?

- Cryptography: science and study of secret writing.
- Cryptanalysis: science and study of breaking ciphers.
- Cryptology: cryptography + cryptanalysis.
- A cryptosystem is a 5-tuple (E, D, M, K, C)

M: set of plaintexts

K: set of keys

C: set of ciphertexts

E: set of encryption functions  $e: M \times K \rightarrow C$

D: set of decryption functions  $d: C \times K \rightarrow M$

- Cipher: secret method of writing that transforms plaintext into ciphertext.
- Encryption (encipherment, scrambling): process of transforming plaintext into ciphertext.
- Decryption (decipherment, descrambling): process of transforming ciphertext into plaintext.

# Chapter 8 BASIC CRYPTOGRAPHY

- **The Caesar cipher**
  - The cipher gets its name because Julius Caesar (100 B.C.? – 44 B.C.) used it to send secret messages.
  - The ciphertext is formed by replacing each letter in the plaintext by the letter three positions to the right in the alphabet.
  - This shift is performed modulo 26.
  - Breaking this cipher is a trivial task!
  - $M = \{ \text{sequences of letters} \}$
  - $K = \{ i \mid i \text{ is an integer and } 0 \leq i \leq 25 \}$
  - $E = \{ E_k \mid k \in K \text{ and for all letters } m \in M, E_k(m) = (m + k) \bmod 26 \}$
  - $D = \{ D_k \mid k \in K \text{ and for all letters } c \in C, D_k(c) = (26 + c - k) \bmod 26 \}$
  - Each  $D_k$  simply inverts the corresponding  $E_k$ .
  - $C = M$  because  $E$  is a set of onto functions.
  - **EXAMPLE**
    - The letter A is in position 0.
    - Plaintext: HELLO (7 4 11 11 14)
    - Ciphertext: KHOOR (10 7 14 14 17)

# Chapter 8 BASIC CRYPTOGRAPHY

- The goal of cryptography is to keep enciphered information secret.
  - Standard cryptographic practice is to assume that the adversary knows the encryption and decryption algorithms but not the cipher key.
- The adversary may use three types of attacks:
  - *ciphertext only*: the adversary has only ciphertext; the goal is to find the plaintext, and possibly the key.
  - *known plaintext*: the adversary has some ciphertext-plaintext pairs; the goal is to find the key.
  - *chosen plaintext*: the adversary is able to acquire the ciphertext corresponding to selected plaintext; the goal is to find the key.
- A good cryptosystem protects against all three types of attacks.

# Chapter 8 BASIC CRYPTOGRAPHY

- **Attacks use both mathematics and statistics.**
- **Mathematical attacks**
  - Based on analysis of underlying mathematics
- **Statistical attacks**
  - Make assumptions about the statistics of the plaintext language.
  - Examine the ciphertext, correlate its properties with the assumptions.
  - The assumptions are collectively called a *model* of the language.
  - Examples: distribution of letters, pairs of letters (digrams), triplets of letters (trigrams), etc.

# Chapter 8 BASIC CRYPTOGRAPHY

<b>E</b> 13.1 %	<b>D</b> 4.1 %	<b>G</b> 1.4 %
<b>T</b> 9.0 %	<b>L</b> 3.6 %	<b>B</b> 1.3 %
<b>O</b> 8.2 %	<b>C</b> 2.9 %	<b>V</b> 1.0 %
<b>A</b> 7.8 %	<b>F</b> 2.9 %	<b>K</b> 0.4 %
<b>N</b> 7.3 %	<b>U</b> 2.8 %	<b>X</b> 0.3 %
<b>I</b> 6.8 %	<b>M</b> 2.6 %	<b>J</b> 0.2 %
<b>R</b> 6.6 %	<b>P</b> 2.2 %	<b>Q</b> 0.1 %
<b>S</b> 6.5 %	<b>Y</b> 1.5 %	<b>Z</b> 0.1 %
<b>H</b> 5.9 %	<b>W</b> 1.5 %	

Letter frequencies in English

## Chapter 8 BASIC CRYPTOGRAPHY

<b>TH</b>	<b>THE</b>
<b>HE</b>	<b>AND</b>
<b>AN</b>	<b>THA</b>
<b>IN</b>	<b>ENT</b>
<b>ER</b>	<b>ION</b>
<b>RE</b>	<b>TIO</b>
<b>ES</b>	<b>FOR</b>
<b>ON</b>	<b>NDE</b>
<b>EA</b>	<b>HAS</b>
<b>TI</b>	<b>NCE</b>

**The 10 most frequent digrams and trigrams in English**

# Chapter 8 BASIC CRYPTOGRAPHY

## 8.2 Classical Cryptosystems

- Classical cryptosystems use the same key for encryption and decryption.
- They are also called symmetric cryptosystems.
- There are two basic types of classical ciphers:
  - Transposition ciphers
  - Substitution ciphers
- A transposition cipher rearranges the characters in the plaintext to form the ciphertext.
  - The letters are not changed.
  - **EXAMPLE:** The rail fence cipher
    - Composed by writing the plaintext in two rows, proceeding down, then across, and reading the ciphertext across, then down.
    - The plaintext “HELLO WORLD” would be written as  
HLOOL  
ELWRD
    - The resulting ciphertext is “HLOOLELWRD.”
- The key to a transposition cipher is a permutation function.
  - The permutation does not alter the frequency of plaintext characters.

# Chapter 8 BASIC CRYPTOGRAPHY

- A transposition cipher can be detected by comparing character frequencies with a model of the language.
  - If character frequencies for 1-grams match those of a model of English, but 2-gram frequencies do not match, the text is probably a transposition cipher!
- Attacking a transposition cipher requires rearrangement of the letters of the ciphertext.
  - This process is called anagramming.
    - Anagramming uses tables of  $n$ -gram frequencies in such a way that the characters in the ciphertext form some  $n$ -grams with highest frequency.
    - This process is repeated, using different  $n$ -grams, until the transposition pattern is found.
- **EXAMPLE**
  - Consider the ciphertext “HLOOLELWRD.”
  - Frequencies of 2-grams beginning with H  
HE: 0.0305, HO: 0.0043, HL, HW, HR, HD < 0.0010
  - Frequencies of 2-grams ending in H  
WH: 0.0026, EH, LH, OH, RH, DH ≤ 0.0002
  - Implies E follows H.

# Chapter 8 BASIC CRYPTOGRAPHY

- A substitution cipher changes characters in the plaintext to produce the ciphertext.
- **EXAMPLE: The Caesar cipher**
  - It is a substitution cipher.
  - Susceptible to a statistical ciphertext-only attack.
  - Consider the ciphertext “KHOOR ZRUOG.”
  - Obtain the frequency of each letter in the ciphertext.  
G: 0.1, H: 0.1, K: 0.1, O: 0.3, R: 0.2, U: 0.1, Z: 0.1
  - Let  $\emptyset(i)$  be the correlation of the frequency of each letter in the ciphertext with the character frequencies in English.
  - $p(x)$  is the frequency of character  $x$  in English.
    - $\emptyset(i) = \sum_{0 \leq c \leq 25} f(c)p(c-i)$ , where  $f(c)$  is the frequency of character  $c$ .
    - $\emptyset(i) = 0.1p(6-i) + 0.1p(7-i) + 0.1p(10-i) + 0.3p(14-i) + 0.2p(17-i) + 0.1p(20-i) + 0.1p(25-i)$
    - The correlation should be maximum when the key translates the ciphertext into English.
    - Figure 8-2 shows the values of  $\emptyset(i)$  for the values of  $i$ .
    - When  $i=6$ , the plaintext is “EBIIL TLOIA”
    - When  $i=10$ , the plaintext is “AXEEH PHKEW”
    - When  $i=3$ , the plaintext is “HELLO WORLD” (The correct answer!)

# Chapter 8 BASIC CRYPTOGRAPHY

$i$	$\varphi(i)$	$i$	$\varphi(i)$	$i$	$\varphi(i)$	$i$	$\varphi(i)$
0	0.0482	7	0.0442	13	0.0520	19	0.0315
1	0.0364	8	0.0202	14	0.0535	20	0.0302
2	0.0410	9	0.0267	15	0.0226	21	0.0517
3	0.0575	10	0.0635	16	0.0322	22	0.0380
4	0.0252	11	0.0262	17	0.0392	23	0.0370
5	0.0190	12	0.0325	18	0.0299	24	0.0316
6	0.0660					25	0.0430

Figure 8-2. The values of  $\varphi(i)$  for  $0 \leq i \leq 25$

# Chapter 8 BASIC CRYPTOGRAPHY

- **The Vigenere Cipher**
  - Blaise de Vigenere was a 16<sup>th</sup> century French cryptologist.
  - A popular form of periodic substitution cipher based on shifted alphabets.
  - The key is specified by a sequence of letters:  $K=k_1\dots k_d$ , where  $k_i$  gives the amount of shift in the  $i$ th alphabet, i.e.  $f_i(a)=(a+k_i) \bmod n$ .
  - **EXAMPLE**
    - $M = \text{RENA ISSA NCE}$
    - $K = \text{BAND BAND BAN}$
    - $E_K(M) = \text{SEAD JSFD OCR}$
    - The first letter of each 4-letter group is shifted (mod 26) by 1, the second by 0, the third by 13, and the fourth by 3.
  - **Periodic substitution ciphers can be cryptanalyzed in two steps:**
    - First, the period  $d$  is estimated.
    - The Kasiski method and the Index of Coincidence are two useful tools for this purpose.
    - The work is then reduced to the cryptanalysis of a set of monoalphabetic substitution ciphers.

# Chapter 8 BASIC CRYPTOGRAPHY

- The index of coincidence (IC)
  - Measures the variation in the frequencies of the letters in the ciphertext.
  - Is the probability that two randomly chosen letters from ciphertext will be the same.
  - If the period of the cipher is 1, there will be considerable variation in the letter frequencies, and the IC will be high.
  - As the period increases, the variation is gradually eliminated, and the IC will be low.
  - $IC = [n(n-1)] / \sum_{0 \leq i \leq 25} [F_i(F_i-1)]$ , where  $n$  is length of ciphertext and  $F_i$  the number of times character  $i$  occurs in ciphertext.

Period	1	2	3	4	5	10	large
Expected IC	0.066	0.052	0.047	0.045	0.044	0.041	0.038

Figure 8-4. Indices of coincidences for different periods

# Chapter 8 BASIC CRYPTOGRAPHY

- The Kasiski method (1863)
  - Friedrich W. Kasiski was the name of a Prussian cavalry officer.
  - Analyzes repetitions in the ciphertext to determine the exact period.
  - EXAMPLE

$M =$  TOBEORNOTTOBE

$K =$  HAMHAMHAMHAMH

$E_K(M) =$  AONLODUOFAAONL

- Repetitions in the ciphertext occur when a plaintext pattern repeats at a distance equal to a multiple of the key length.
- If  $m$  ciphertext repetitions are found at intervals  $I_j (1 \leq j \leq m)$ , the period is likely to be some number that divides most of the  $m$  intervals.
- The preceding example has an interval  $I_j = 9$ , suggesting a period of 1, 3, or 9.
- The IC is useful for confirming a period  $d$  found by the Kasiski method.

# Chapter 8 BASIC CRYPTOGRAPHY

## – EXAMPLE

$M =$  THEBOYHASTHEBAG

$K =$  VIGVIGVIGVIGVIG

$E_K(M) =$  OPKWWECIYOPKWIM

- In the ciphertext, the string OPK appears twice.
- The ciphertext repetitions are 9 characters apart.
- Hence, 9 is a multiple of the period.
- The period may be 1, 3, or 9.

# Chapter 8 BASIC CRYPTOGRAPHY

- **EXAMPLE:** Consider the below Vigenere cipher.

ADQYS	MIUSB	OXKKT	MIBHK	IZOOO	EQOOG	IFBAG	KAUMF
VVTAA	CIDTW	MOCIO	EQOOG	BMBFV	ZGGWP	CIEKQ	HSNEW
VECNE	DLAAV	RWKXS	VNSVP	HCEUT	QOIOF	MEGJS	WTPCH
AJMOC	HIUIX						

- Could this be a Caesar cipher (a Vigenere cipher with a key length of 1)?
- The IC = 0.043 (which indicates a key length of 5 or more).
- So, the key may have a length greater than 1.
- We apply the Kasiski method to find out.

# Chapter 8 BASIC CRYPTOGRAPHY

Letters	Start	End	Distance	Factors
MI	5	15	10	2, 5
OO	22	27	5	5
OEQOOG	24	54	30	2, 3, 5
FV	39	63	24	2, 2, 2, 3
AA	43	87	44	2, 2, 11
MOC	50	122	72	2, 2, 2, 3, 3
QO	56	105	49	7, 7
PC	69	117	48	2, 2, 2, 2, 3
NE	77	83	6	2, 3
SV	94	97	3	3
CH	118	124	6	2, 3

# Chapter 8 BASIC CRYPTOGRAPHY

- **The longest repetition (OEQOOG) is 6 characters long.**
  - This is unlikely to be a coincidence.
  - The gap between the repetitions is 30.
- **The next longest repetition (MOC) is 3 characters long.**
  - The gap between the repetitions is 72.
  - The greatest common divisor of 30 and 72 is 6.
- **Of the 11 repetitions, 6 have gaps with a factor of 6.**
  - The only factors that occur more in the gaps are 2 and 3.
- **As a first guess, we will try 6.**
  - To verify that this is a reasonable guess, the IC for each alphabet will be computed.

# Chapter 8 BASIC CRYPTOGRAPHY

- The ciphertext message is arranged into 6 columns.
- Each column represents one alphabet.

A	D	Q	Y	S	M
I	U	S	B	O	X
K	K	T	M	I	B
H	K	I	Z	O	O
O	E	Q	O	O	G
I	F	B	A	G	K
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.

# Chapter 8 BASIC CRYPTOGRAPHY

alphabet 1: AIKHOIATTOBGEEERNEOSAI  $\Rightarrow$  IC=0.069  
alphabet 2: DUKKEFUAWEMGKWDWSUFWJU  $\Rightarrow$  IC=0.078  
alphabet 3: QSTIQBMAMQBWQVLKVTMTMI  $\Rightarrow$  IC=0.078  
alphabet 4: YBMZOAFCOOFPHEAXPQEPOX  $\Rightarrow$  IC=0.056 (?)  
alphabet 5: SOIOOGVICOVCSVASHOGCC  $\Rightarrow$  IC=0.124  
alphabet 6: MXBOGKVDIGZINNVVCIJHH  $\Rightarrow$  IC=0.043 (?)

- All indices indicate a single alphabet except #4 and #6.
- Given the statistical nature of the measure, we will assume that there are 6 alphabets.



# Chapter 8 BASIC CRYPTOGRAPHY

	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
1	3	1	0	0	4	0	1	1	3	0	1	0	0	1	3	0	0	1	1	2	0	0	0	0	0	0
2	1	0	0	2	2	2	1	0	0	1	3	0	1	0	0	0	0	0	1	0	4	0	4	0	0	0
3	1	2	0	0	0	0	0	2	0	1	1	4	0	0	0	4	0	1	3	0	2	1	0	0	0	0
4	2	1	1	0	2	2	0	1	0	0	0	0	1	0	4	3	1	0	0	0	0	0	0	2	1	1
5	1	0	5	0	0	0	2	1	2	0	0	0	0	0	5	0	0	0	3	0	0	2	0	0	0	0
6	0	1	1	1	0	0	2	2	3	1	1	0	1	2	1	0	0	0	0	0	0	3	0	1	0	1

Letter frequencies are (H high, M medium, L low):

H	M	M	M	H	M	M	H	H	M	M	M	M	H	H	M	L	H	H	H	M	L	L	L	L	L	L	L
↑				↑																							↑
<b>A</b>				<b>E</b>																							<b>Z</b>

# Chapter 8 BASIC CRYPTOGRAPHY

- First matches characteristics of unshifted alphabet.
- Third matches if I shifted to A.
- Sixth matches if V shifted to A.
- Substituting into the ciphertext (bold are substitutions) produces:

**ADIYS RIUKB OCKKL MIGHK AZOTO EIOOL IFTAG PAUEF**  
**VATAS CIITW EOCNO EIOOL BMTFV EGGOP CNEKI HSSEW**  
**NECSE DDAAA RWCXS ANSNP HHEUL QONOF EEGOS WLPCM**  
**AJEOC IUAX**

# Chapter 8 BASIC CRYPTOGRAPHY

**AJE in the last line suggests ARE.**

**The second alphabet maps A into S.**

**Substituting back produces:**

**ALIYS RICKB OCKSL MIGH S AZOTO MIOOL INTAG PACEF  
VATIS CIITE EOCNO MIOOL BUTFV EGOOP CNESI HSSEE  
NECSE LDAAA RECXS ANANP HHECL QONON EEGOS ELPCM  
AREOC MICAX**

## Chapter 8 BASIC CRYPTOGRAPHY

**MICAX in the last line suggests MICAL.**

**AL is a common ending for adjectives.**

**This means that the fourth alphabet maps O into A:**

**ALIMS RICKP OCKSL AIGHS ANOTO MICOL INTOG PACET  
VATIS QIITE ECCNO MICOL BUTTV EGOOD CNESI VSSEE  
NSCSE LDOAA RECLS ANAND HHECL EONON ESGOS ELDCM  
ARECC MICAL**

## Chapter 8 BASIC CRYPTOGRAPHY

**QI means that U maps into I.**

**In English, Q is always followed by U.**

**The fifth alphabet maps M to A.**

ALIME RICKP ACKSL AUGHS ANATO MICAL INTOS PACET  
HATIS QUITE ECONO MICAL BUTTH EGOOD ONESI VESEE  
NSOSE LDOMA RECLE ANAND THECL EANON ESSOS ELDOM  
ARECO MICAL

# Chapter 8 BASIC CRYPTOGRAPHY

With proper spacing and punctuation, the plaintext message is obtained:

A LIMERICK PACKS LAUGHS ANATOMICAL INTO SPACE  
THAT IS QUITE ECONOMICAL BUT THE GOOD ONES I'VE  
SEEN SO SELDOM ARE CLEAN, AND THE CLEAN ONES SO  
SELDOM ARE COMICAL.

The key is ASIMOV.

**limerick**: a light or humorous verse form of 5 chiefly anapestic verses of which lines 1, 2, and 5 are of 3 feet and lines 3 and 4 are of 2 feet with a rhyme scheme of *aabba*.

**anapest**: a metrical foot consisting of two short syllables followed by one long syllable or of two unstressed syllables followed by one stressed syllable.

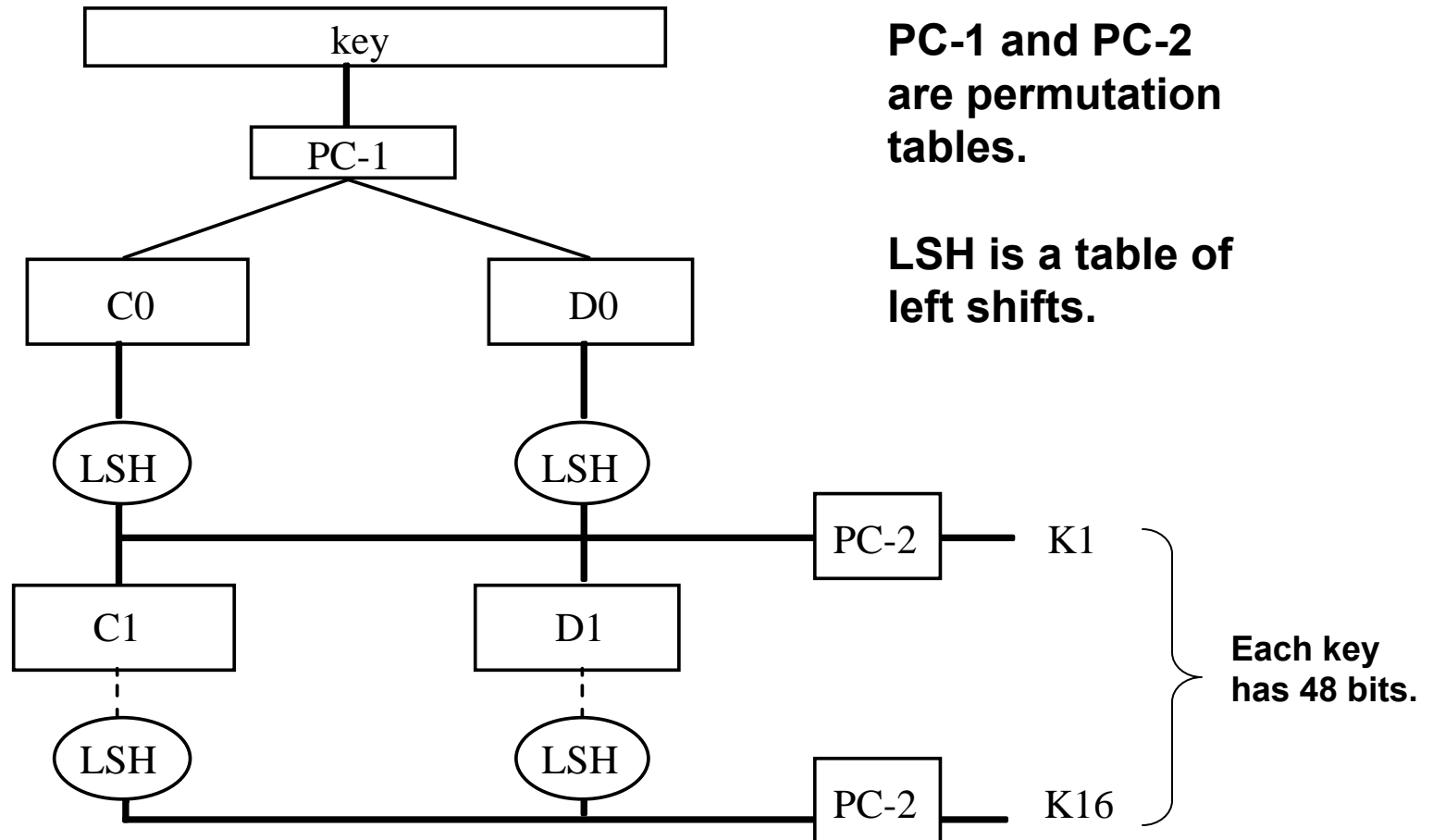
# Chapter 8 BASIC CRYPTOGRAPHY

- **One-time pad**
  - This is a variant of the Vigenere cipher.
  - Provably unbreakable!
  - The key string is chosen at random, and should be at least as long as the message.
  - In most cases, one can only obtain a pseudo random number sequence.
  - Approximations, such as using pseudo random number generators to generate keys, are not random.
  - The distribution of a long key may not be feasible!

# Chapter 8 BASIC CRYPTOGRAPHY

- **Data Encryption Standard (DES)**
  - **A block cipher**
    - encrypts blocks of 64 bits using a 64 bit key
    - outputs 64 bits of ciphertext
  - **A product cipher**
    - basic unit is the bit
    - performs both substitution and transposition on the bits
  - **Cipher consists of 16 rounds (iterations), each with a round key generated from the user-supplied key.**

# Chapter 8 BASIC CRYPTOGRAPHY

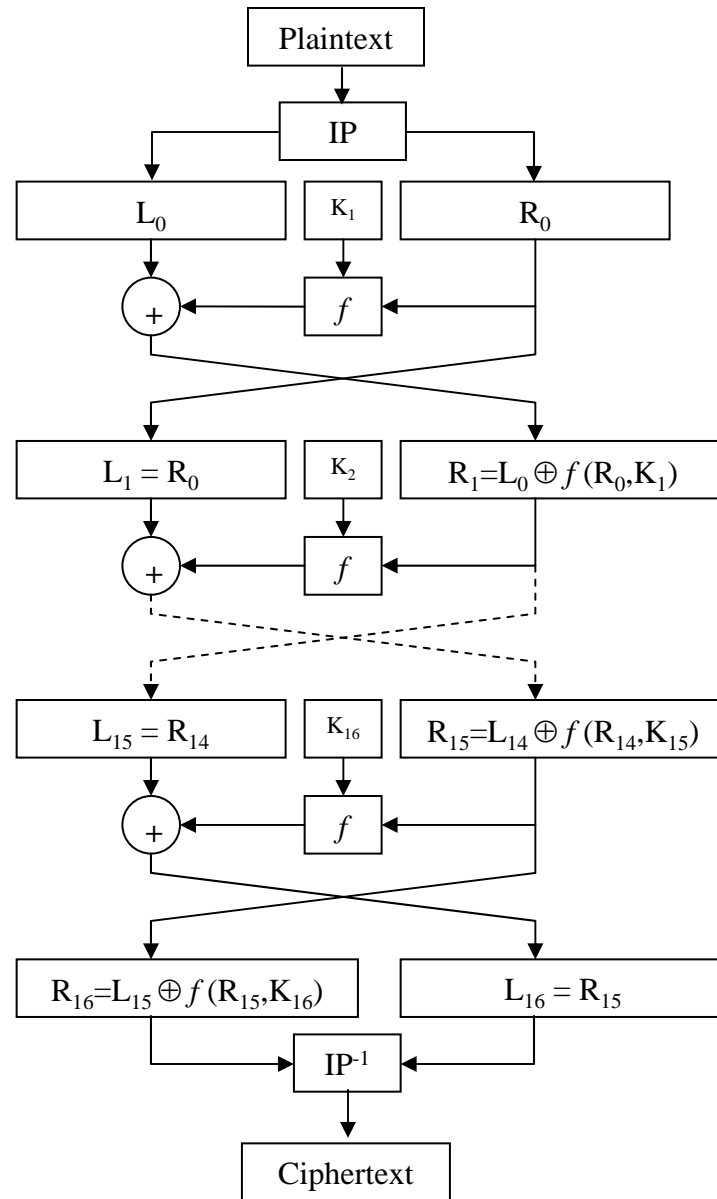


# Chapter 8 BASIC CRYPTOGRAPHY

PC1						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
above for $C_i$ ; below for $D_i$						
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	5	5	28	20	12	4

PC2					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

# Chapter 8 BASIC CRYPTOGRAPHY



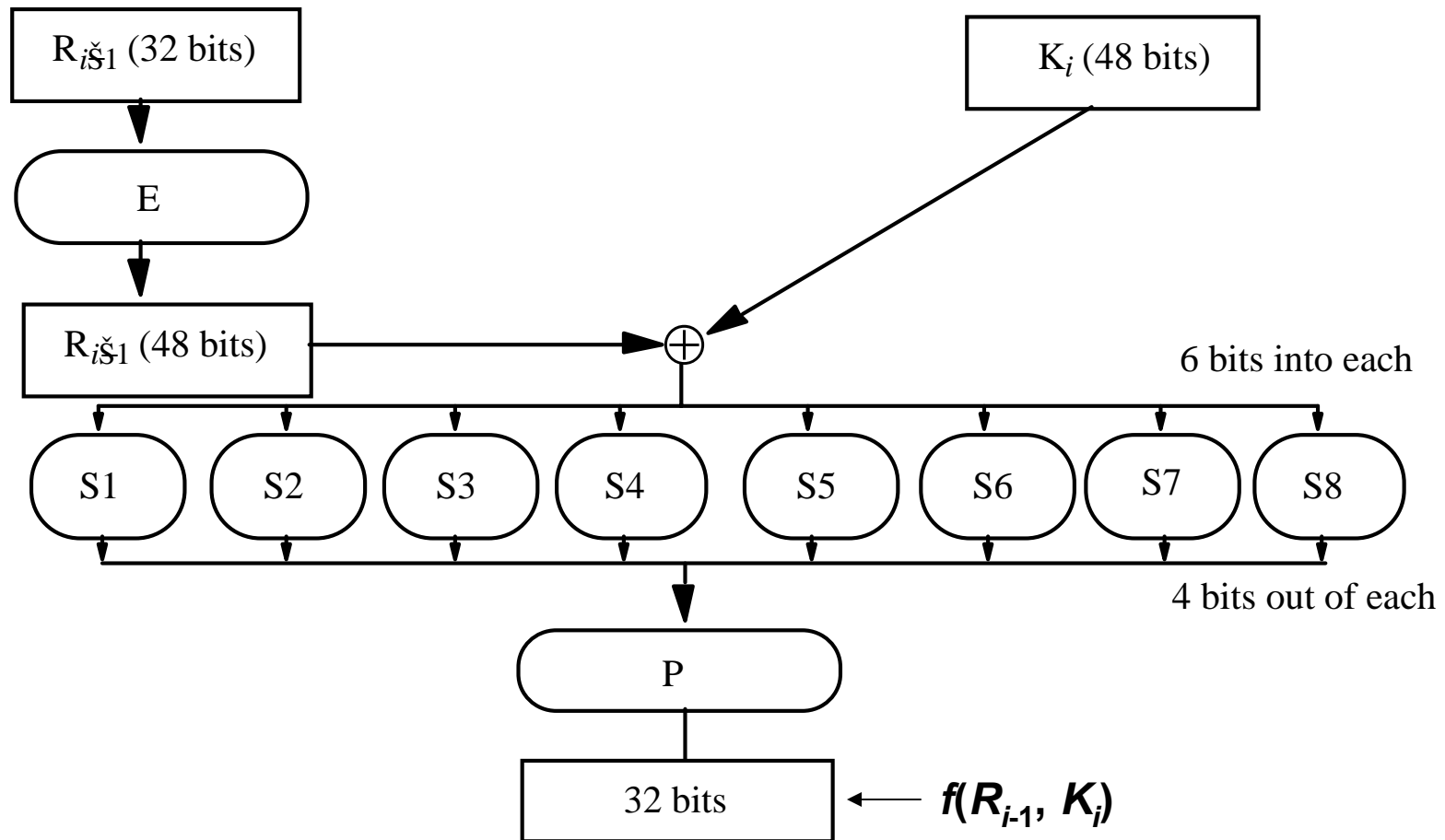
# Chapter 8 BASIC CRYPTOGRAPHY

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP <sup>-1</sup>							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

# Chapter 8 BASIC CRYPTOGRAPHY

## Calculation of $f(R_{i-1}, K_i)$



# Chapter 8 BASIC CRYPTOGRAPHY

E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

P			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

# Chapter 8 BASIC CRYPTOGRAPHY

- **4 weak keys**
  - A DES weak key is a key  $K$  such that  $E_K(E_K(x)) = x$  for all  $x$ .
- **6 pairs of semi-weak keys**
  - A pair of DES semi-weak keys is a pair  $(K_1, K_2)$  with  $E_{K_1}(E_{K_2}(x)) = x$ .
- **Complementation property:  $DES_K(m) = c \Rightarrow DES_K(\hat{m}) = \hat{c}$** 
  - This property does not represent a serious weakness in DES.

WEAK KEY			
0101	0101	0101	0101
FEFE	FEFE	FEFE	FEFE
1F1F	1F1F	OEOE	OEOE
E0E0	E0E0	F1F1	F1F1

SEMI-WEAK KEY PAIR							
01FE	01FE	01FE	01FE	FE01	FE01	FE01	FE01
1FE0	1FE0	OEF1	OEF1	E01F	E01F	F10E	F10E
01E0	01E0	01F1	01F1	E001	E001	F101	F101
1FFE	1FFE	0EFE	0EFE	FE1F	FE1F	FE0E	FE0E
011F	011F	010E	010E	1F01	1F01	0E01	0E01
EOFE	EOFE	F1FE	F1FE	FEE0	FEE0	FEF1	FEF1

# Chapter 8 BASIC CRYPTOGRAPHY

## Differential Cryptanalysis (Biham and Shamir)

- A chosen plaintext attack
- Requires  $2^{47}$  {plaintext, ciphertext} pairs
- This is considerably fewer than the trial-and-error approach.

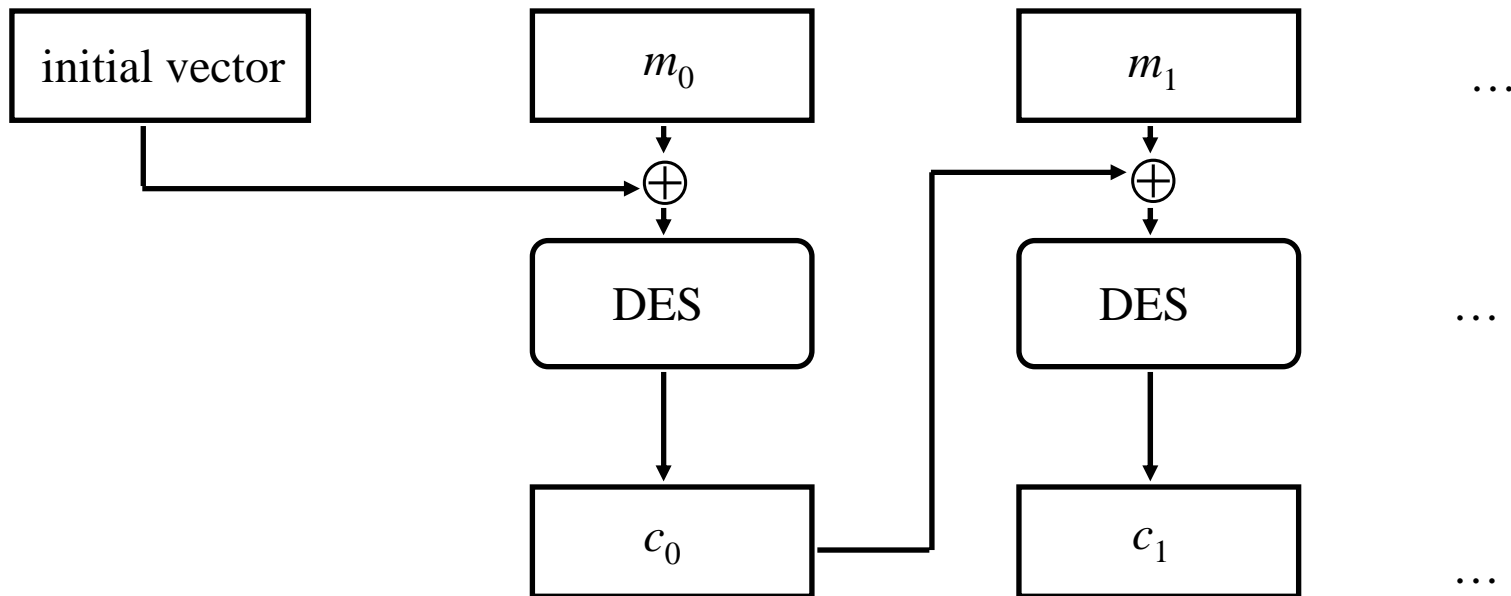
## Linear cryptanalysis (Matsui)

- A known plaintext attack
- Requires  $2^{43}$  {plaintext, ciphertext} pairs on the average.

# Chapter 8 BASIC CRYPTOGRAPHY

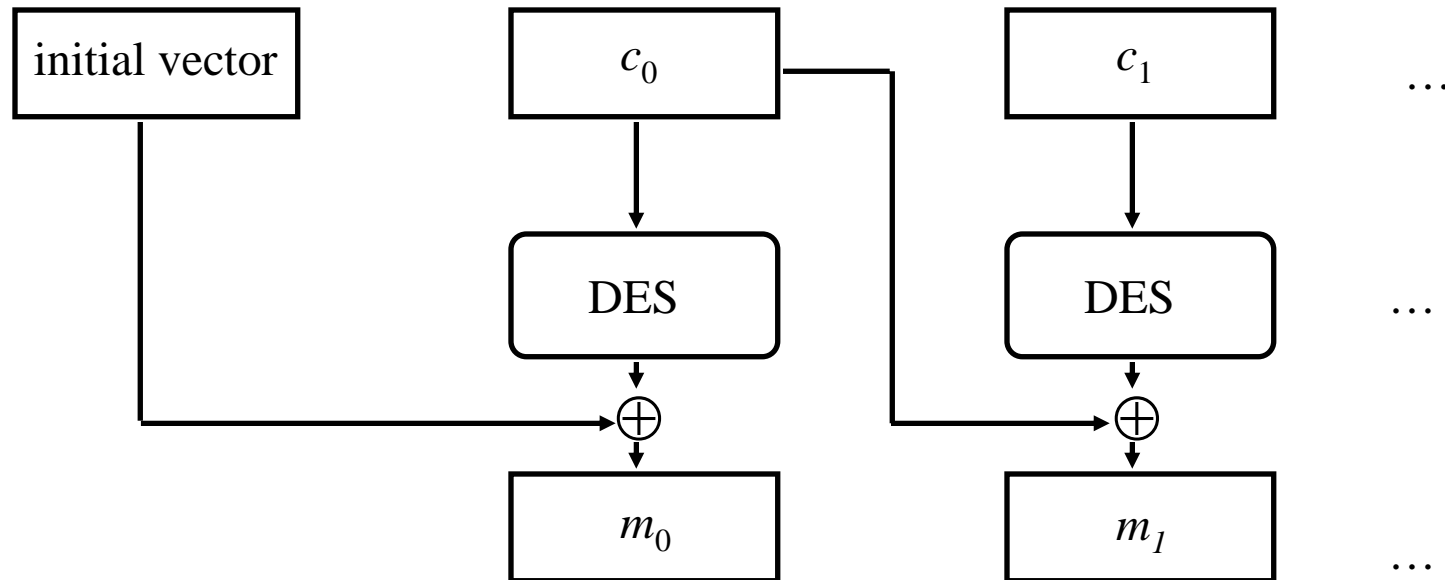
- **Modes of DES**
  - Electronic code book (ECB) mode
  - Cipher feedback (CFB) mode
  - Output feedback (OFB) mode
- **Triple DES**
  - Encrypt with  $K_1$
  - Decrypt with  $K_2$
  - Encrypt with  $K_3$
- **NIST has selected Rijndael as the Advanced Encryption Standard (AES).**
  - Proposed by Joan Daemen and Vincent Rijmen.
  - The AES can use 128, 192, and 256 bit keys.
  - The AES operates on blocks of 128 bits.

# Chapter 8 BASIC CRYPTOGRAPHY



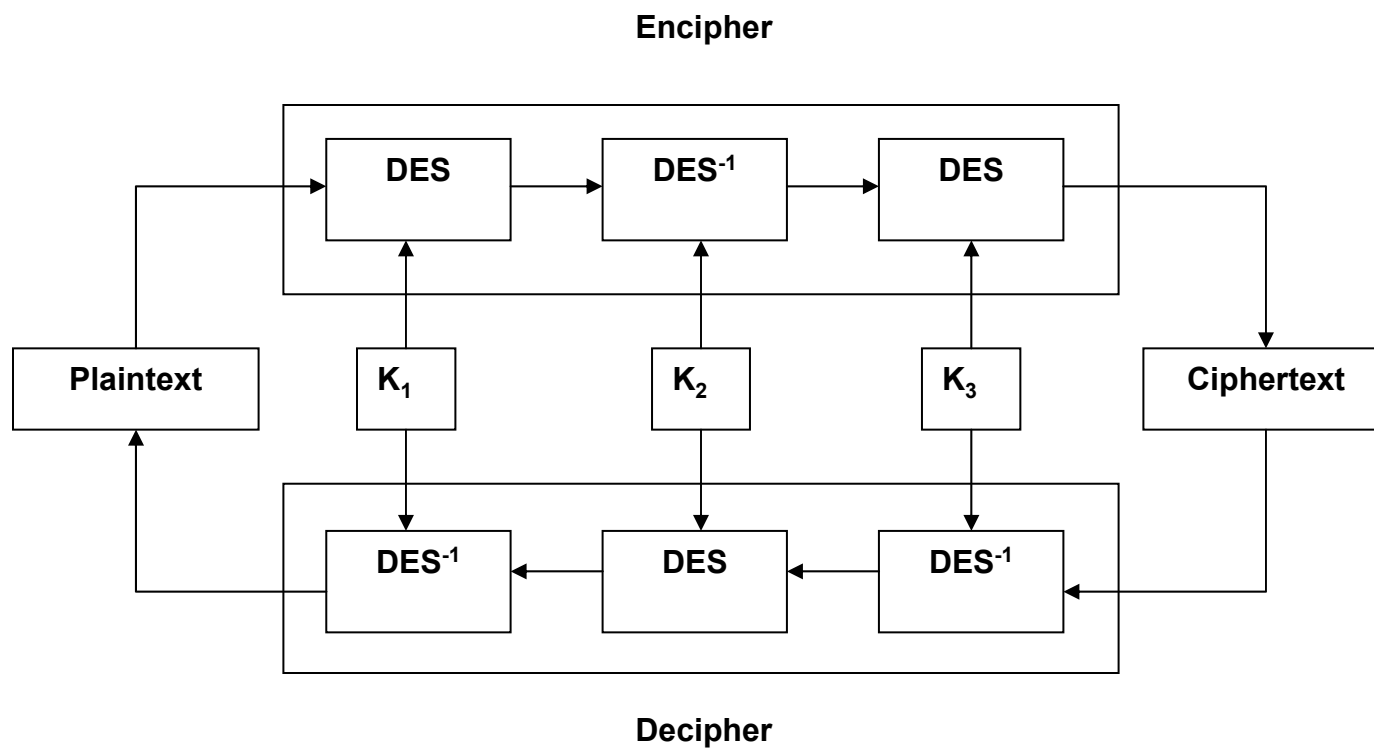
**CBC Mode Encryption**

# Chapter 8 BASIC CRYPTOGRAPHY



**CBC Mode Decryption**

# Chapter 8 BASIC CRYPTOGRAPHY



**Triple-DES encryption and decryption**

# Chapter 8 BASIC CRYPTOGRAPHY

- **Public Key Cryptography**
  - In 1976, Diffie and Hellman introduced a new type of cryptography.
  - Private key should be securely kept by the owner.
  - Public key can be publicly known.
- **A public key cryptosystem must meet the following requirements:**
  - It must be computationally easy to encipher or decipher a message given the appropriate key.
  - It must be computationally infeasible to derive the private key from the public key.
  - It must be computationally infeasible to determine the private key from a chosen plaintext attack.

# Chapter 8 BASIC CRYPTOGRAPHY

- **RSA (Rivest, Shamir, Adleman)**
  - Exponentiation cipher
  - Provides both confidentiality and authentication
- **The RSA Problem:** Given a positive integer  $n$  that is a product of two distinct odd primes  $p$  and  $q$ , a positive integer  $e$  such that  $\gcd(e, (p-1)(q-1)) = 1$ , and an integer  $c$ , find an integer  $m$  such that  $m^e \equiv c \pmod{n}$ .
- **Choose two large prime numbers  $p, q$** 
  - Let  $n = pq$  and  $\phi(n) = (p-1)(q-1)$
  - Choose  $e < n$  such that  $e$  is relatively prime to  $\phi(n)$ .
  - Compute  $d$  such that  $ed \pmod{\phi(n)} \equiv 1$
- **Public key:  $(e, n)$ ; private key:  $d$**
- **Encipher:  $c = m^e \pmod{n}$**
- **Decipher:  $m = c^d \pmod{n}$**

# Chapter 8 BASIC CRYPTOGRAPHY

## CONFIDENTIALITY

- Take  $p = 7$ ,  $q = 11$ , so  $n = 77$  and  $\phi(n) = 60$
- Alice chooses  $e = 17$ , making  $d = 53$
- Bob wants to send Alice secret message HELLO (07 04 11 11 14).  
 $07^{17} \bmod 77 = 28$ ,  $04^{17} \bmod 77 = 16$ ,  $11^{17} \bmod 77 = 44$ ,  $11^{17} \bmod 77 = 44$ ,  $14^{17} \bmod 77 = 42$
- Bob sends 28 16 44 44 42
- Alice receives 28 16 44 44 42
- Alice uses private key,  $d = 53$ , to decrypt message:  
 $28^{53} \bmod 77 = 07$ ,  $16^{53} \bmod 77 = 04$ ,  $44^{53} \bmod 77 = 11$ ,  $44^{53} \bmod 77 = 11$ ,  $42^{53} \bmod 77 = 14$
- Alice translates message to letters to read HELLO.
  - No one else could read it, as only Alice knows her private key and that is needed for decryption.

# Chapter 8 BASIC CRYPTOGRAPHY

## INTEGRITY/AUTHENTICATION

- Take  $p = 7$ ,  $q = 11$ , so  $n = 77$  and  $\phi(n) = 60$
- Alice chooses  $e = 17$ , making  $d = 53$
- Alice wants to send Bob message HELLO (07 04 11 11 14) in such a way that Bob will be sure that Alice sent it (no changes in transit, and authenticated).

$$07^{53} \bmod 77 = 35, 04^{53} \bmod 77 = 09, 11^{53} \bmod 77 = 44, 11^{53} \bmod 77 = 44, 14^{53} \bmod 77 = 49$$

- Alice sends 35 09 44 44 49
- Bob receives 35 09 44 44 49
- Bob uses Alice's public key,  $e = 17$ ,  $n = 77$ , to decrypt message:

$$35^{17} \bmod 77 = 07, 09^{17} \bmod 77 = 04, 44^{17} \bmod 77 = 11, 44^{17} \bmod 77 = 11, 49^{17} \bmod 77 = 14$$

- Bob translates message to letters to read HELLO.
  - Alice sent it as she is the only one to have the private key, so no one else could have enciphered it.

# Chapter 8 BASIC CRYPTOGRAPHY

## CONFIDENTIALITY & AUTHENTICATION

- Alice wants to send Bob message HELLO both enciphered and authenticated (integrity-checked).
  - Alice's keys: public (17, 77); private: 53
  - Bob's keys: public: (37, 77); private: 13
- Alice enciphers HELLO (07 04 11 11 14):
  - $(07^{53} \bmod 77)^{37} \bmod 77 = 07$
  - $(04^{53} \bmod 77)^{37} \bmod 77 = 37$
  - $(11^{53} \bmod 77)^{37} \bmod 77 = 44$
  - $(11^{53} \bmod 77)^{37} \bmod 77 = 44$
  - $(14^{53} \bmod 77)^{37} \bmod 77 = 14$
- Alice sends 07 37 44 44 14

# Chapter 8 BASIC CRYPTOGRAPHY

## CRYPTOGRAPHIC CHECKSUMS

- **Mathematical function to generate a set of  $k$  bits from a set of  $n$  bits (where  $k \leq n$ ).**
- **Example: ASCII parity bit**
  - ASCII has 7 bits; 8th bit is “parity”
  - Even parity: even number of 1 bits
  - Odd parity: odd number of 1 bits
  - Assume Alice sends Bob the letter “A”(0111101).
  - Alice uses even parity (six 1 bits).
  - Bob receives “10111101.”

↑  
Parity bit

# Chapter 8 BASIC CRYPTOGRAPHY

- **Cryptographic checksum  $h: A \rightarrow B$ :**
  1. For any  $x \in A$ ,  $h(x)$  is easy to compute
  2. For any  $y \in B$ , it is computationally infeasible to find  $x \in A$  such that  $h(x) = y$
  3. It is computationally infeasible to find two inputs  $x, x' \in A$  such that  $x \neq x'$  and  $h(x) = h(x')$
- **A keyed cryptographic checksum function requires a cryptographic key.**
  - The DES in CBC mode can be used as a message authentication code if 64 bits or fewer are required.
  - Because the hash is at most 64 bits, finding 2 inputs to produce the same output would require  $2^{32}$  messages.
- **A keyless cryptographic checksum function does not require a cryptographic key.**
  - Known examples of keyless hash functions are MD5 and SHA-1.
  - SHA-1 produces 160-bit output. MD5 produces 128-bit output.

# Chapter 8 BASIC CRYPTOGRAPHY

- **HMAC**

- A generic term for an algorithm that uses a keyless hash function and a cryptographic key to produce a keyed hash function.
- The need for HMAC arose because keyed hash functions are derived from cryptographic algorithms.
- Let  $h$  be a keyless hash function that takes data in blocks of  $b$  bytes and outputs blocks of  $l$  bytes.
- Let  $k$  be a cryptographic key of length  $b$  bytes.
  - The assumption is that the length of  $k$  is no greater than  $b$ .
  - If it is, use  $h$  to hash it to produce a new key of length  $b$ .
- Let  $k'$  be the key  $k$  padded with bytes containing 0 to make  $b$  bytes.
- Let  $ipad$  be a sequence of bytes containing 00110110 and repeated  $b$  times.
- Let  $opad$  be a similar sequence with the bits 01011100.
- The HMAC- $h$  function with key  $k$  for message  $m$  is:

$$\text{HMAC-}h(k,m) = h(k' \oplus opad \parallel h(k' \oplus ipad \parallel m)) ,$$

where  $\oplus$  is exclusive or, and  $\parallel$  is concatenation.