INFORMATION SECURITY
LECTURE 5
STREAM & BLOCK CIPHER
PLAYFAIR CIPHER

Khalid Abdullah

MSc computer and Network Security

Computer Science Dept.

University Of Zakho

Last Lecture

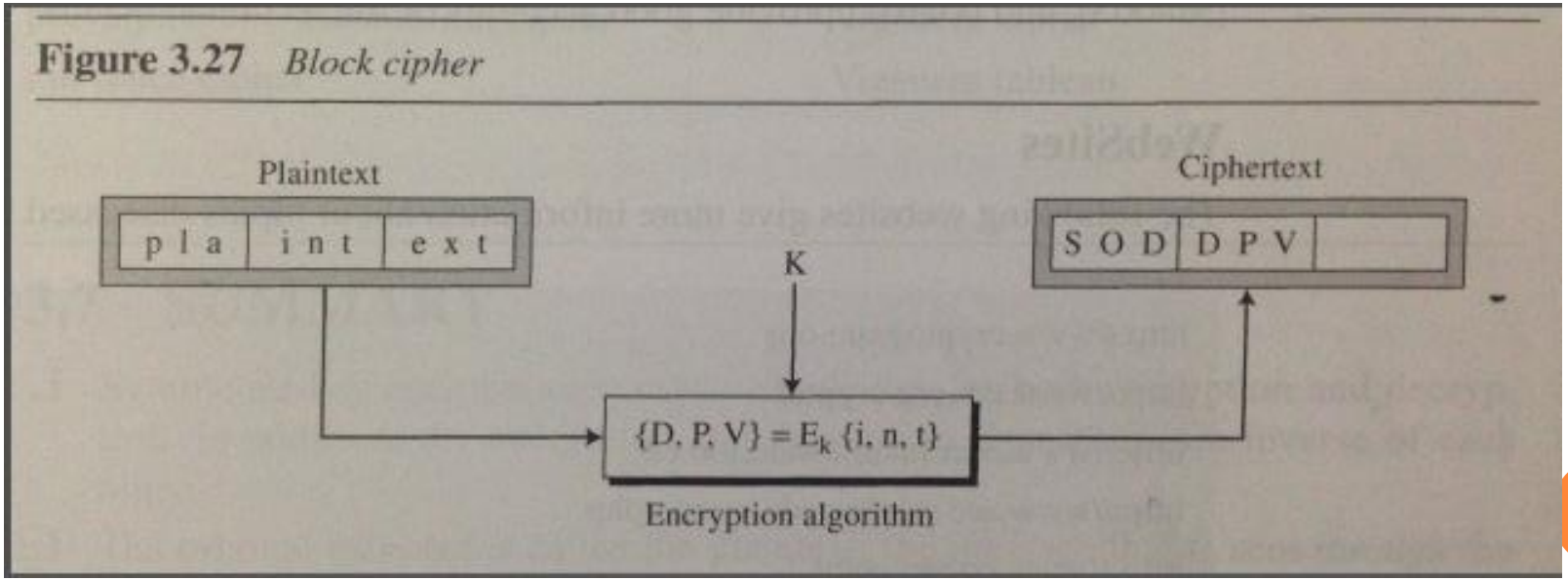
- Transposition ciphers (such as Rail Fence cipher)
- Column transposition cipher
- Double Transposition Cipher

Outline Line

- Stream and Block Cipher
- Playfair Cipher

What is Block Cipher

- In block cipher, a group of plaintext symbols of size m(m>1) are encrypted together creating a group of ciphertext of the same size.
- Single Key is used to encrypt the whole block even the key is made of multiple values.



Block Cipher

- In block cipher, a ciphertext block depends on the whole plaintext block.
- **Playfair cipher** and **Hill cipher** are block cipher.
- most modern ciphers are block ciphers.

- The Data Encryption Standard (DES) is an example of a block cipher, where blocks of 64 bits are encrypted using a 56-bit key.

Formal Definition of a Block Cipher

- Let E be an encipherment algorithm, and let $E_k(b)$ be the encipherment of the message b with key k.
- Let a message $m=b_1b_2...$where each b_i is of a fixed length.
- A **block cipher** is a cipher for which $E_k(m) = E_k(b_1)E_k(b_2)...$

Stream Cipher

- In a **stream cipher**, encryption and decryption are done one sympol (such as a characters or a bit) at a time.
- We have a plaintext stream P, a ciphertext stream C, and the key stream K.

  - $P = P_1P_2P_{3,....}$ $C = C_1C_2C_{3,.....}$ $K=(K_1,K_2,K_3, ...)$
  - $C_1 = E_K(P_1)$ $C_2=E_{K2}(P_2)$ $C3=E_{K3}(P_3)$…

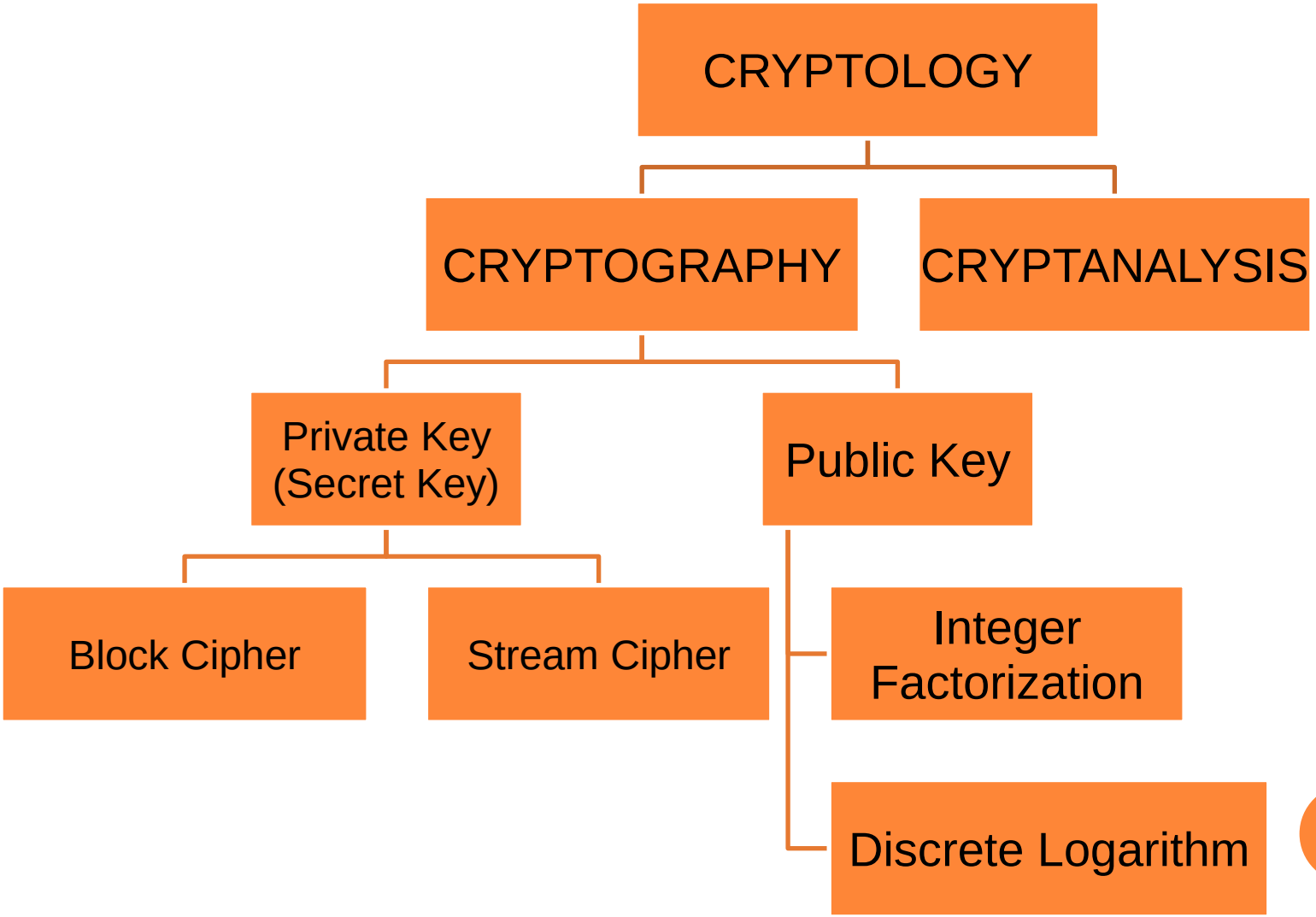
Stream Cipher

- The Vigenère cipher is an example of a stream cipher.
- The one-time pad is also a stream cipher.

Formal Definition of a Stream Cipher

- Let E be an encipherment algorithm, and let $E_k(b)$ be the encipherment of the message b with key k.
- Let a message $m=b_1b_2...$where each b_i is of a fixed length, and let $k = k_1k_2....$
- A **stream cipher** is a cipher for which $E_k(m) = E_{k1}(b_1)E_{k_2}(b_2)...$

Cryptology


CRYPTOLOGY
CRYPTOGRAPHY
CRYPTANALYSIS
Private Key
(Secret Key)
Public Key
Block Cipher
Stream Cipher
Integer
Factorization
Discrete Logarithm

What is the difference between block and stream cipher?

- A typical stream cipher encrypts plaintext one byte at a time, although a stream cipher may be designed to operate on one bit at a time or on units larger than a byte at a time.
- A block cipher encrypts one block at a time. The block may be of size one byte or more or less. That means we can also encrypt a block of one byte by help of a stream cipher as a stream.

Shannon's building blocks

- **confusion**
  - make relation between statistics of ciphertext and the value of the encryption key as complex as possible
- **diffusion**
  - diffuse statistical property of plaintext digit across a range of ciphertext digits
  - i.e. each plaintext digits affects value of many ciphertext digits

History

- invented by Wheatstone on 26 March 1854,but it was promoted by Lord Playfair

Lord Playfair

History

- Playfair is now regarded as insecure for any purpose because modern hand-held computers could easily break the cipher within seconds
- The first published solution of the Playfair cipher was published in 1914

Playfair Cipher

- The best-known multiple-letter encryption cipher is the playfair, which treats diagrams in the plaintext as single units and translates these units into ciphertext diagrams.

- The Playfair algorithm is based on the use of a 5 x 5 matrix of letters constructed using a keyword.

Encryption Rules

1. Fill the Matrix with the keyword, drop duplicates.
2. Filling in the remainder of the matrix with the remaining letters in alphabetic order.
3. Plaintext is encrypted two letters at a time.
4. The letters I and J count as one letter.
5. Use the Playfair Rules to map the message to the matrix.

How to use it?

- Prepare your Message
- Rules
  - Must be split into PAIRS
  - Separate all duplicated letters by inserting letter “X”
  - Ignore all spaces

Playfair Rules

- 1) If two plaintext letters that located in the same row of the matrix.
  - Replaced by the letter to the right.
  - first element of the first element of the row circularly following the last.
  - Wrapping to the beginning of the row if the plaintext letter is the last character in the row.

2) If both letters are located in same COLUMN

Move each letter down ONE.(replace the letter with the letter beneath it in the same column).

Wrapping to the beginning of the column if the plaintext letter is the last character in the column.

3) If the letters are not on the same row or column, put them in a rectangle forms, Swap (Replace) the letters with the ones on the end of the rectangle.

The order is important- the first letter of the encrypted pair is the one on the same row as the first letter of the plaintext pair.

Preparing the plaintext

- Example 1:
- Prepare specific information
- E.g. I will see you there

- Choose encryption key
- E.g. dream

All the letters should be written

- in capital letter,
- in pairs,
- without punctuation

→ Iw il ls ***ee*** yo ut he re

- double letters which occur in a pair must be divided by an X. And X to the end single letter if appear.
- E.g. ee

- →IW IL LS EX EY OU TH ER EX

Preparing the Key: Alphabet Square

- present with an alphabet square
- 5*5
- No repeat letter
- No Js
- KEY: DREAM→

3 Rules

- letters appear on the same row： **replace them with the letters to their immediate right respectively**
- letters appear on the same column： **replace them with the letters immediately below respectively**

- not on the same row or column:

  replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair.

  The order is important – the first encrypted letter of the pair is the one that lies on the same row as the first plaintext letter.

How to implement playfair cipher

Plaintext is :
iw il ls ex ey ou th er ex

D	R	E	A	M
B	C	F	G	H
i	k	L	N	O
P	Q	S	T	U
V	W	X	Y	Z

- final ciphertext is:

KV KN SX FE AX UZ UG AE FE

PLAYFAIR CIPHER…

- **Example 2:**

  Key: COMPUTER

C	O	M	P	U
T	E	R	A	B
D	F	G	H	I/J
K	L	N	Q	S
V	W	X	Y	Z

Plaintext: SEND HELP SOON

SE ND HE LP SO ON

LB KG FA QO LU ML

Ciphertext: LBKG FAQO LUML

PLAYFAIR CIPHER…

- **Example 3:**

  Key: security

S	E	C	U	R
I/J	T	Y	A	B
D	F	G	H	K
L	M	N	O	P
Q	V	W	X	Z

Plaintext: UNIVERSITY OF ZAKHO

UN IV ER SI TY OF ZA KH OX

CO TQ CS ID YA MH XB DK XU

Ciphertext: COTQCSIDYAMHXBDKXU

Security of Playfair Cipher

- security much improved over monoalphabetic
- since have 26 x 26 = 676 diagrams
- would need a 676 entry frequency table to analyse (verses 26 for a monoalphabetic)
- it can be broken, given a few hundred letters
- since still has much of plaintext structure

Summery

- Steam and Block Cipher
- Stream cipher Vs Block Cipher
- Playfair cipher

What Next

- Use of Passwords
- Key Management
- Hill cipher