Cryptography and Network Security Chapter 2

Fourth Edition

by William Stallings

Lecture slides by Lawrie Brown

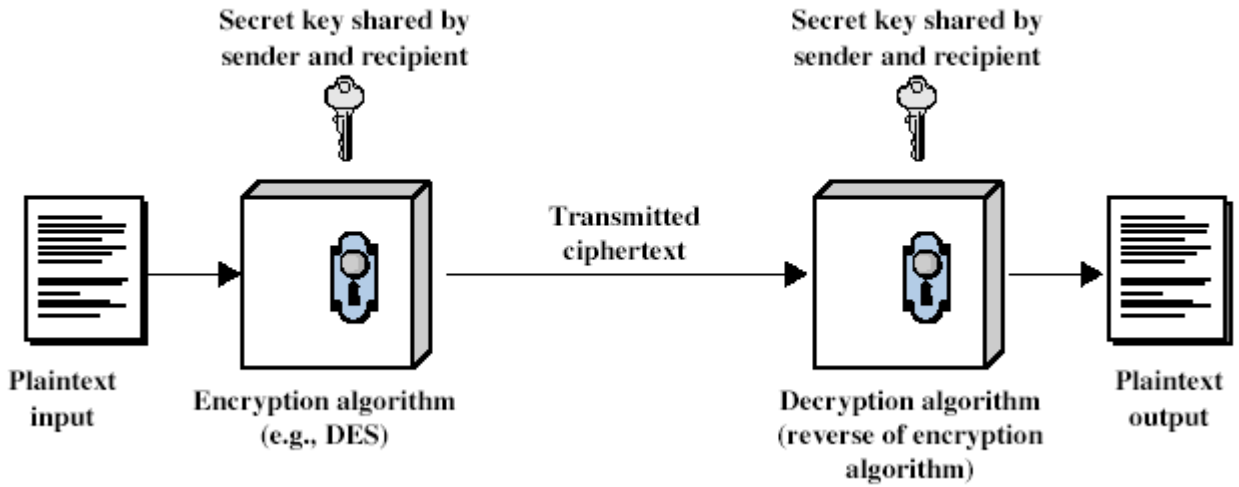
Symmetric Encryption

- or conventional / private-key / single-key
- sender and recipient share a common key
- all classical encryption algorithms are private-key
- was only type prior to invention of public-key in 1970's
- and by far most widely used

Some Basic Terminology

- **plaintext** - original message
- **ciphertext** - coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering ciphertext from plaintext

Symmetric Cipher Model



Requirements

- two requirements for secure use of symmetric encryption:
  - a strong encryption algorithm
  - a secret key known only to sender / receiver
- mathematically have:

  $Y = E_K(X)$

  $X = D_K(Y)$
- assume encryption algorithm is known
- implies a secure channel to distribute key

Cryptography

- characterize cryptographic system by:
  - type of encryption operations used
    - substitution / transposition / product
  - number of keys used
    - single-key or private / two-key or public
  - way in which plaintext is processed
    - A block cipher processes the input one block of elements at a time, producing an output block for each input block.
    - A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along

Cryptanalysis

- objective to recover key not just message
- general approaches:
  - cryptanalytic attack : algorithm + knowledge of text
  - brute-force attack : possible key

Cryptanalytic Attacks

- **ciphertext only**
  - only know algorithm & ciphertext, is statistical, know or can identify plaintext
- **known plaintext**
  - know/suspect plaintext & ciphertext
- **chosen plaintext**
  - select plaintext and obtain ciphertext
- **chosen ciphertext**
  - select ciphertext and obtain plaintext
- **chosen text**
  - select plaintext or ciphertext to en/decrypt

Playfair Cipher

- a manual symmetric encryption technique
- technique encrypts pairs of letters, instead of single letters as in the simple substitution cipher
- significantly harder to break since the frequency analysis used for simple substitution ciphers does not work with it.
- The frequency analysis is possible, but considerably more difficult.

Playfair Key Matrix

- a 5X5 matrix of letters based on a keyword
- fill in letters of keyword (sans duplicates)
- fill rest of matrix with other letters where assuming that I and J are interchangeable
- eg. using the key “playfair example”

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

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

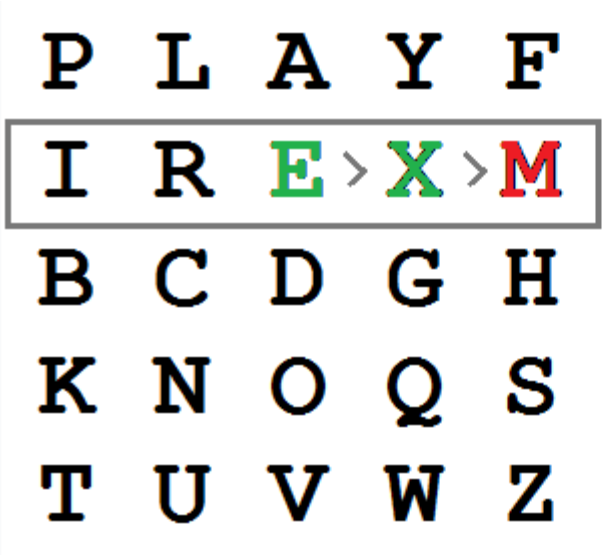
Encrypting and Decrypting

- Encrypting the message "Hide the gold in the tree stump“
- plaintext is encrypted two letters at a time
  1. if a pair is a repeated letter, insert filler like 'X’
     - eg. "balloon" encrypts as "ba lx lo on"

- **HI DE TH EG OL DI NT HE TR EX ES TU MP**

Encrypting and Decrypting

- if both letters fall in the same row, replace each with letter to right (wrapping back to start from end)
- RM -> EI
- EX -> XM
- XE -> MX



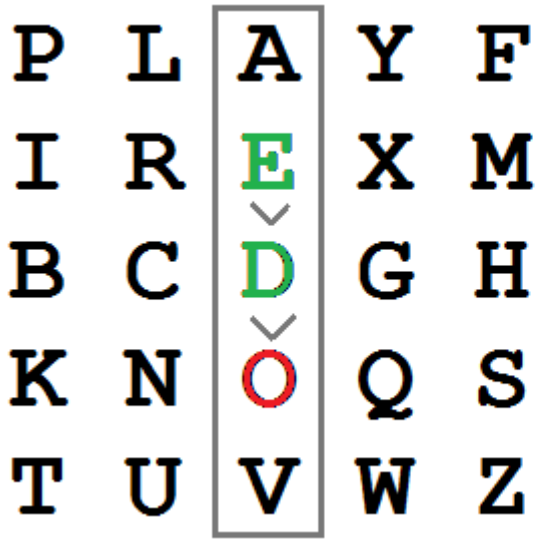
EX

Shape: Row
Rule: Pick Items to Right of Each Letter, Wrap to Left if Needed

XM

Encrypting and Decrypting

- if both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom)
- EV -> DA
- Jo yx -> EK XG -> IO YX / Joyx



DE

Shape: Column
Rule: Pick Items Below Each Letter, Wrap to Top if Needed

OD

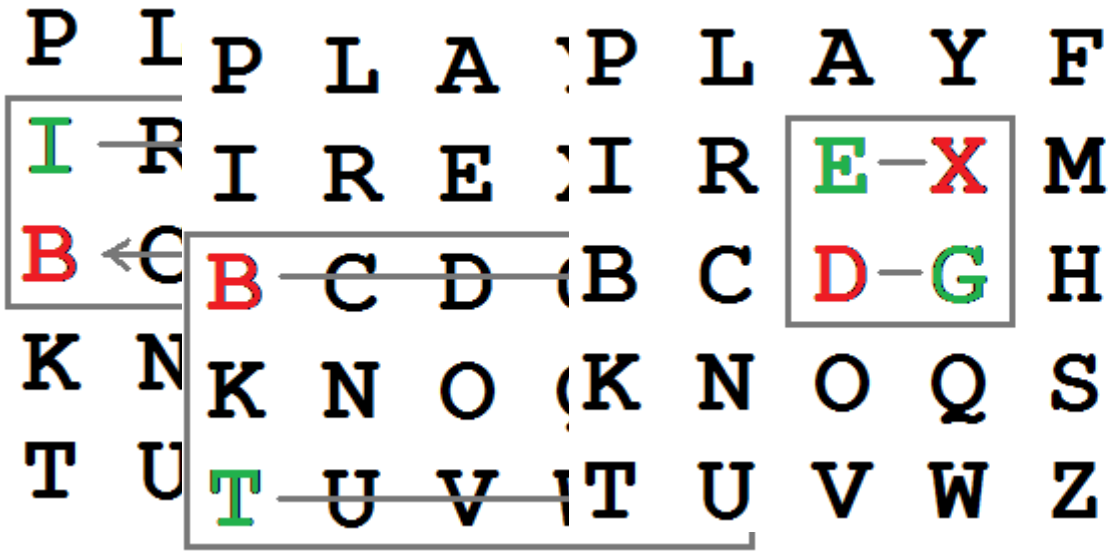
BSSE SECOND BATCH

b	s	e	c	o
n	d	a	t	h
f	g	l	k	l
m	p	q	r	u
v	w	x	y	z

Plaintext: Software Engineering
SO FT WA RE EN GI NE ER IN GX
Chipertext: EB KN

Encrypting and Decrypting

- otherwise each letter is replaced by the letter in the same row and in the column of the other letter of the pair



EG

Shape: Rectangle
Rule: Pick Same Rows, Opposite Corners

XD

Security of Playfair Cipher

- since have 26 x 26 = 676 digrams
- would need a 676 entry frequency table to analyse
- and correspondingly more ciphertext
- was widely used for many years
  - eg. by US & British military in WW1
- it **can** be broken, given a few hundred letters
- since still has much of plaintext structure

Hill cipher

- Hill cipher is a substitution cipher based on linear algebra.
- Encryption & decryption
  - Each letter is represented by a number modulo 26.
  - Though this is not an essential feature of the cipher, this simple scheme is often used
  - To encrypt a message, each block of n letters is multiplied by an invertible n × n matrix, against modulus 26.
  - To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.
  - The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n × n matrices (modulo 26).

Letter	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
Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Hill cipher: Encrypting and Decrypting

- Key

$$M = \begin{pmatrix} 2 & 3 \\ 5 & 7 \end{pmatrix}$$

- Plaintext

$$HELP \rightarrow \begin{pmatrix} H \\ E \end{pmatrix}, \begin{pmatrix} L \\ P \end{pmatrix} \rightarrow \begin{pmatrix} 7 \\ 4 \end{pmatrix}, \begin{pmatrix} 11 \\ 15 \end{pmatrix}$$

Hill cipher: Encrypting and Decrypting

- $\begin{pmatrix} 2 & 3 \\ 5 & 7 \end{pmatrix} \begin{pmatrix} 7 \\ 4 \end{pmatrix} \equiv \begin{pmatrix} 26 \\ 63 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 11 \end{pmatrix} \pmod{26}$
- $\begin{pmatrix} 2 & 3 \\ 5 & 7 \end{pmatrix} \begin{pmatrix} 11 \\ 15 \end{pmatrix} \equiv \begin{pmatrix} 67 \\ 160 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 4 \end{pmatrix} \pmod{26}$
- $\begin{pmatrix} 0 \\ 11 \end{pmatrix}, \begin{pmatrix} 15 \\ 4 \end{pmatrix}$
- ALPE
- HELP -> ALPE

Hill cipher: Encrypting and Decrypting

- Key for decryption (inverse matrix)

$$\begin{pmatrix} 2 & 3 \\ 5 & 7 \end{pmatrix}^{-1} \equiv \begin{pmatrix} -7 & 3 \\ 5 & -2 \end{pmatrix} \equiv \begin{pmatrix} 19 & 3 \\ 5 & 24 \end{pmatrix} \mod 26$$

- ALPE -> $\begin{pmatrix} 0 \\ 11 \end{pmatrix}, \begin{pmatrix} 15 \\ 4 \end{pmatrix}$

Hill cipher: Encrypting and Decrypting

- $\begin{pmatrix} 19 & 3 \\ 5 & 24 \end{pmatrix} \begin{pmatrix} 0 \\ 11 \end{pmatrix} \equiv \begin{pmatrix} 33 \\ 264 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 4 \end{pmatrix} \pmod{26}$
- $\begin{pmatrix} 19 & 3 \\ 5 & 24 \end{pmatrix} \begin{pmatrix} 15 \\ 4 \end{pmatrix} \equiv \begin{pmatrix} 297 \\ 171 \end{pmatrix} \equiv \begin{pmatrix} 11 \\ 15 \end{pmatrix} \pmod{26}$
- HELP

Presentation Topics

1. Polygraphic substitution: **Razu Biswas, Nayeem Khan**
2. Monoalphabetic cipher: **Anupa Das, Sanzida Nitu**
3. Digital signature: **Prosanto Deb, Joy Bhowmik**
4. Digital currency: **Nadia Islam, Ayesha Nasrin Ripa**
5. Secret sharing: **Abdullah Al Tahmid, Sanjatul Hasan**
6. Steganography: **Shahriar Ahmed, Alamgir Hossain**