

COMPUTER SECURITY

CLASSICAL CIPHERS

Willy Sudiarto Raharjo

Teknik Informatika
Universitas Kristen Duta Wacana

Ciphers

An alias for algorithm to perform encryption/decryption

Defined as (K, M, C)

$$E = K \times M \longrightarrow C$$

$$D = K \times C \longrightarrow M$$

$$\forall m \in M, k \in K: D(k, E(k, m)) \longrightarrow m$$

E is often randomized , D is deterministic

m = message, M = message space

k = key, K = key space

Classical Cipher

- Classical

- Substitution
 - Monoalphabetic Substitution
 - Caeasar/ROT13
 - Affine
 - Polyalphabetic substitution
 - Vigenere
 - Polygraphic
 - Playfair
- Transposition

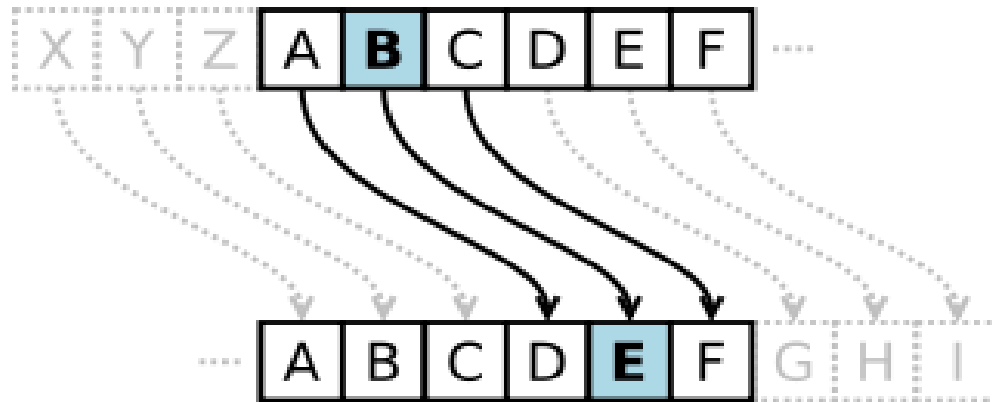
Modern Cipher

- Symetric Key Algorithm
 - Stream Ciphers
 - A5/1
 - RC4
 - One Time Pad
 - Block Ciphers
 - DES
 - 3DES
 - AES
- Asymetric Key Algorithm
 - Diffie-Helman
 - ElGamal
 - Elliptic curve cryptography
 - RSA

Caesar Ciphers

- Each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet

- Eg: shift of 3:



- Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ

- Cipher: DEFGHIJKLMNOPQRSTUVWXYZABC

- Easy to crack using brute force (26 possibilities possible)

- Keyspace $\longrightarrow 26! = 2^{88} \longrightarrow 4.03291461 \times 10^{26}$

Caesar Ciphers

- Can also be done by transforming the letters into numbers
- $A = 0, B = 1, \dots, Z = 25$
- Encryption : $E_n(x) = (x + n) \bmod 26$
- Decryption : $D_n(x) = (x - n) \bmod 26$
- Plaintext
 - DUTA WACANA
- Caesar Ciphers with 5 shift
 - IZYF BFHFSF

Practice

- Plaintext
 - CRYPTOGRAPHY
 - Shift 21 times
- Ciphertext ??
 - XMTKOJB MVKCT
- Ciphertext
 - ZOXQESX
 - Shift 10 times
- Plaintext ??

Affine

- Mono alphabetic substitution cipher
- Simple mathematical formula
 - Modular arithmetic
- Encryption : $E(x) = (ax + b) \bmod m$
- Decryption: $D(x) = a^{-1} (x - b) \bmod m$
 - m = size of message (alphabet in our case, 26)
 - a and b are the keys of this cipher
 - a and m must be coprime

How to get a^{-1}

- $1 = aa^{-1} \pmod m$ (modular multiplicative inverse)
- Only works if a and m are coprime

$$\begin{array}{ll} a^{-1} \equiv x \pmod m & 3^{-1} \equiv x \pmod{11} \\ ax \equiv 1 \pmod m & 3x \equiv 1 \pmod{11} \end{array}$$

- Example
 - $a = 7$ and $m = 26$
 - $7x = 1 \pmod{26}$
 - $a^{-1} = 15$

Affine (Encryption)

- Plaintext : “AFFINE CIPHER”
- $a = 5$ (must be coprime with m)
- $b = 8$ (any number except 1)
- Encryption function: $y = E(x) = (5x + 8) \pmod{26}$

plaintext:	A	F	F	I	N	E	C	I	P	H	E	R
x:	0	5	5	8	13	4	2	8	15	7	4	17
$5x + 8$	8	33	33	48	73	28	18	48	83	43	28	93
$(5x + 8) \pmod{26}$	8	7	7	22	21	2	18	22	5	17	2	15
ciphertext:	I	H	H	W	V	C	S	W	F	R	C	P

Affine (Decryption)

- Ciphertext : **IHHWVCSWFRCP**
- Decryption function: $D(x) = a^{-1} (x - b) \bmod m$
- Count a^{-1}
- $D(x) = 21(x - 8) \bmod 26$

ciphertext:	I	H	H	W	V	C	S	W	F	R	C	P
y:	8	7	7	22	21	2	18	22	5	17	2	15
$21(y-8)$:	0	-21	-21	294	273	-126	210	294	-63	189	-126	147
$(21(y-8)) \bmod 26$:	0	5	5	8	13	4	2	8	15	7	4	17
plaintext:	A	F	F	I	N	E	C	I	P	H	E	R

Practice

- Plain Text : DUTAWACANA
- $a = 11$
- $b = 6$
- Ciphertext ?

- Ciphertext : RTGTODDYJ
- $a = 17$
- $b = 3$
- Plaintext ?

Vigenère

- Best-known polyalphabetic ciphers
- Using Vigenère table to encrypt/decrypt
- Keyword is repeated to make a key as long as the plaintext
- Example:

Key:	deceptivedeceptivedeceptive
Plaintext:	wearediscoveredsaveyourself
Ciphertext:	ZICVTWQNGRZGVTWAVZHCQYGLMGJ

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

Practice

- Plaintext
 - PERFECTLIFE
 - KEY: BLUE
- Ciphertext ??
- Ciphertext
 - soqmixvikh
 - KEY: WHITE
- Plaintext ??

PlayFair

- Best-known multiple-letter substitution cipher
- Uses 5x5 table or 6x6 table (using 1-9 numeric)
- Steps:
 - Fill the table with the keywords (without duplicates)
 - Fill the rest of the table with remaining alphabets
 - Don't use “Q” or replace “J” with “I”
 - Break the plaintext into digraphs (groups of 2 letters)

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

Keyword = monarchy

Plaintext: H S | E A | A R | M U |
Ciphertext: B P | I M | R M | C M |

PlayFair Rules (encryption)

- Repeating plaintext letters are separated with a filler letter, such as **X**.
- Plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last.
- Plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the row circularly following the last.
- Otherwise, each plaintext letter is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter.

Practice

- Plaintext:
 - LOVEISBLIND
 - Key: TEKNIK
 - FACEBOOK
 - Key: SOCIAL
- Ciphertext ??
 - MG WT NU CH TI CY
 - NF ID HB WC RC
- Ciphertext:
 - RGPSNTTM
 - Key: TEKNIK
 - MDWECSXK
 - Key: SOCIAL
- Plaintext ??
 - PLURKING
 - KEYBOARD

For consistency: remove j from the table

Transposition Ciphers

- Changes the order of the letters of the original message
- Write the message in a series of columns and rows in a grid
- Example: ciphertext
 - uo yn os dn ep ed yx al ag eh tf oy te fa se ht
- Plaintext:
 - the safety of the galaxy depends on you

Simple Matrix Transposition Ciphers

- Plaintext

- troops heading west need more supplies. send general dubois' men to aid

- Generate a 6x10 matrix (free to choose)

T	R	O	O	P	S	H	E	A	D
I	N	G	W	E	S	T	N	E	E
D	M	O	R	E	S	U	P	P	L
I	E	S	S	E	N	D	G	E	N
E	R	A	L	D	U	B	O	I	S
M	E	N	T	O	A	I	D		

- Read the column to get the ciphertext

- TIDIE MRNME REOGO SANOW RSLTP EEEDO
SSSNU AHTUD BIENP GODAE PEIDE LNS