Traditional Symmetric Key Cipher

AIF 183119 Keamanan Informasi
Universitas Katolik Parahyangan
Mariskha Tri Adithia MSc, PDEng

Overview

- Substitution cipher
  - Caesar
  - Vigenere
  - Playfair
- Transposition cipher

Substitution cipher

- Replaces one symbol with another
- 2 types
  - Monoalphabetic
  - Polyalphabetic

Monoalphabetic

- The relationship between a symbol in the plaintext to a symbol in the ciphertext is always one-to-one

Monoalphabetic
Caesar Cipher

- The oldest substitution cipher
- The original: each letter was substituted with the 3rd letter after it

Example:

- Plaintext:

AWASI ASTERIX DAN TEMANNYA OBELIX

- Then the ciphertext:

DZDVL DVWHULA GDQ WHPDQQBA REHOLA

Monoalphabetic

Caesar Cipher (2)

The original:

$C = E(P) = (P + 3) \bmod 26 \longrightarrow$ encryption

$P = D(P) = (C - 3) \bmod 26 \longrightarrow$ decryption

So, if the letter "A" = 0, then the letter "C" is encrypted to "F"

Monoalphabetic

Caesar Cipher (3)

The improvement:

$C = E(P) = (P + k) \bmod 26$ → encryption

$P = D(P) = (C - k) \bmod 26$ → decryption

Exercise

- Encrypt the following plaintext using a key = 12

  Plaintext: I am a very honest person

Discussion

- What are the weaknesses of the cipher?
- How to attack it?

Caesar Cipher
Statistical attack

Frequency of Occurrence of Letters in English

The following table is from Fletcher Pratt, *Secret and Urgent: The Story of Codes and Ciphers*, Blue Ribbon Books, 1939.

Rank	Letter	Frequency of occurrence in 1000 words	Frequency of occurrence in 1000 letters
1	E	591	131.05
2	T	473	104.68
3	A	368	81.51
4	O	360	79.95
5	N	320	70.98
6	R	308	68.32
7	I	286	63.45
8	S	275	61.01
9	H	237	52.59
10	D	171	37.88
11	L	153	33.89
12	F	132	29.24
13	C	124	27.58
14	M	114	25.36
15	U	111	24.59
16	G	90	19.94
17	Y	89	19.82
18	P	89	19.82
19	W	68	15.39
20	B	65	14.40
21	V	41	9.19
22	K	19	4.20
23	X	7	1.66
24	J	6	1.32
25	Q	5	1.21
26	Z	3	.77

Caesar Cipher
Statistical attack (2)

How?

1. Find a letter occurs the most in the ciphertext
2. Correspond it with the letter that occur the most according to the table
3. Find the key based on that determined letter

Discussion

Ciphertext:
xlilsywimwrsajsvwepijsvjsyvqmppmsrhs
ppevwmxmwasvxlqsvilyvvcfijsvixliwippvi
gimziwqsvisjjivw

Find the plaintext!

Polyalphabetic
Vigenere Cipher

General scheme:

$$c_i = (p_i + k_r) \bmod 26 \longrightarrow \text{enkripsi}$$

$$p_i = (p_i - k_r) \bmod 26 \longrightarrow \text{dekripsi}$$

Polyalphabetic
Vigenere Cipher (2)

Plaintext: THIS PLAINTEXT

Key: sony

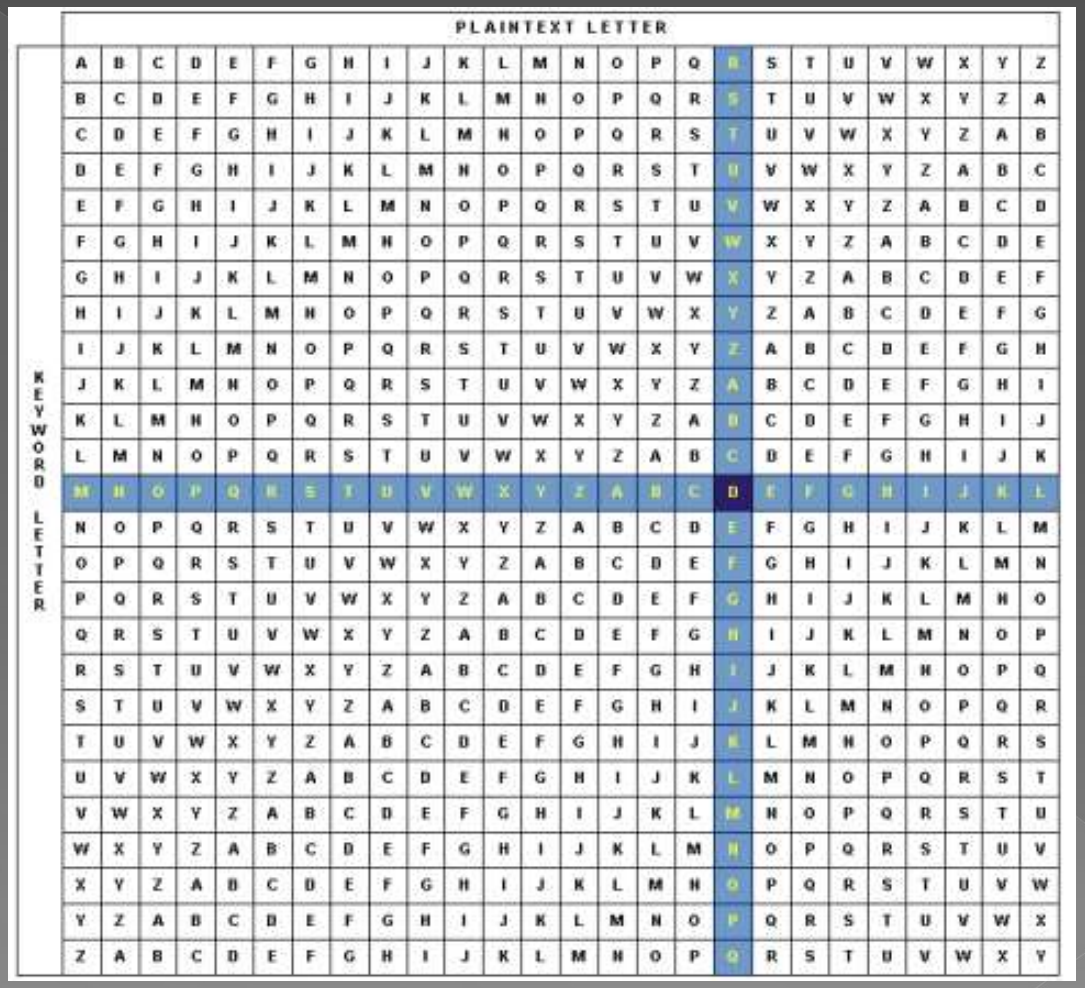
T	H	I	S	P	L	A	I	N	T	E	X	T
s	o	n	y	s	o	n	y	s	o	n	y	s

$$c_1 = (T + s) \bmod 26 = (19 + 18) \bmod 26 = 11 = 'L'$$

Ciphertext: LVVQ HZNGFHRVL

Note: 'A'=0, 'B'=1, …

Polyalphabetic
Vigenere Cipher (3)



KEYWORD LETTER	PLAINTEXT 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
	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Discussion

Determine the plaintext of the following ciphertext:

CSASTP KV SIQUT GQU

CSASTPIUAQJB

With the key “abcd”

Polyalphabetic
Playfair Cipher

- Founded by Sir Charles Wheatstone in 1854.
- Promoted by Baron Lyon Playfair.
- Used by the English army in WW I

Polyalphabetic
Playfair Cipher (2)

1. Replace every letter “J” with the letter “I”
2. Write the plaintext in pairs
3. If there are pairs with containing the same letters, put the letter “Z” in between.
4. If the plaintext length is odd, add the letter “Z” at the last place.

Polyalphabetic
Playfair Cipher (3)

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

- In the same row, use the letter right to each
- In the same column, use the letter beneath each
- Not in the same row or column, use the letter in the same row but also in the same column with the other letter

Polyalphabetic
Playfair Cipher (4)

Given a plaintext:

GOOD BROOMS SWEEP CLEAN.

1. Doesn't contain any letter "J"
2. The plaintext in pairs:

   GO OD BR OO MS SW EE PC LE AN
3. Put "Z" in between the same letter:

   GO OD BR OZ OM SZ SW EZ EP CL EA N
3. Add the letter "Z":

   GO OD BR OZ OM SZ SW EZ EP CL EA NZ

Polyalphabetic
Playfair Cipher (5)

- The encryption of the pair **GO** to **FP**

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

Polyalphabetic

Playfair Cipher (6)

- The encryption of the pair **BR** to **EC**

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

- The ciphertext:

  FP UT EC UW PO DV TV BV CM BG CS DY

Discussion

Encrypt the following plaintext:

THE SECRET IS BROKEN

TH ES EC RE TI SB RO KE NZ

NR KE RH CR …

Transposition Cipher

- The letters are the same, the positions change
- Example: written in columns

Transposition Cipher

Contoh:

- Given a plaintext: JURUSAN INFORMATIKA
- Write it horizantally, with length k = 3:

J	U	R
U	S	A
N	I	N
F	O	R
M	A	T
I	K	A

- Write the plaintext in columns:
  JUNFMI USIOAK RANRTA

Questions?