More on ciphers discussed

- Shift cipher is a special case of affine cipher with a=1.
- Both have small key space.
- Substitution cipher has a much larger key space.
- all ciphers discussed so far belong to "mono-alphabetic cryptosystems" . (so what ?)

Polyalphabetic Ciphers

- Plaintext message can be transformed into more then one cipher elements.
- Why it is desirable ?
- all mono-alphabetic cryptosystems can be "attacked" by a simple frequency analysis.
  - How ?
- Example of poly-alphabetic cryptosystems.

Vigenere cipher

- Encrypt m characters at a time.
- $P=C=K=(Z_{26})^m$
- keyword of length m: $\mathbf{k}= (k_1, k_2, \ldots, k_m)$
- plaintext of length m: $\mathbf{x}= (x_1, x_2, \ldots, x_m)$
- ciphertext of length m: $\mathbf{y}= (y_1, y_2, \ldots, y_m)$
- $e_k(x_i) = x_i + k_i \pmod{26}$, i = `position'
- $d_k(y_i) = y_i - k_i \pmod{26}$

Vigenere cipher Example

- Example 1.4 (pages 12-13)
- m=6,
- keyword k=CIPHER=(2,8,15,7,4,17)

t	h	i	s	c	r	y	p	t	o	s	y	s	t	e	m
19	7	8	18	2	17	24	15	19	14	18	24	18	19	4	12
2	8	15	7	4	17	2	8	15	7	4	17	2	8	15	7
21	15	23	25	6	8	0	23	8	21	22	15	20	1	19	19
86	80	88	90	71	73	65	88	73	86	87	80	85	66	84	84
V	P	X	Z	G	I	A	X	I	V	W	P	U	B	T	T

Hill cipher (1929)

- another polyalphabetic cryptosystem
- encrypt m characters at a time.
- $P=C=(Z_{26})^m$
- $K=(Z_{26})^{mxm}$, key **K** is a mxm matrix.
- plaintext of length m: $\mathbf{x}= (x_1, x_2, \ldots, x_m)$
- ciphertext of length m: $\mathbf{y}= (y_1, y_2, \ldots, y_m)$
- $e_k(\mathbf{x}) = \mathbf{x}\,\mathbf{K}$ (mod 26),
- $d_k(\mathbf{y}) = \mathbf{y}\,\mathbf{K}^{-1}$ (mod 26).
- Need matrix multiplication, matrix inverse.

Hill cipher Example

- Example 1.5 (pages 14-16)
- m=2
- Plaintext $\mathbf{x}=(x_1, x_2)$
- Ciphertext $\mathbf{y}=(11x_1+3x_2 , 8x_1 +7x_2)$.
- Find 2x2 matrix **K** ? $\mathbf{y} = \mathbf{x}\,\mathbf{K}$.
- Find matrix inverse $\mathbf{K}^{-1}$?
  - $\mathbf{x}=\mathbf{y}\,\mathbf{K}^{-1}$ (mod 26).

Hill cipher Example

- Inverse of 2x2 matrix (mod 26) should be easy. [Formula ?]
- plaintext: july= [(9,20), (11,24)]
- ciphertext: [(9,20)**K**, (11,24)**K**] mod 26 =[(3,4), (11,22)] = DELW [check!]
- Q: Inverse of mxm matrix (mod 26) ?
- A: Theorem 1.3, Example 1.6 (p 17)

Affine-Hill cipher

- Ex 1.24 (page 42): multi-dim affine cipher.
- $P=C= (Z_{26})^m$
- $K= (Z_{26})^m \times (Z_{26})^{mxm}$,
  - key **A** is a mxm matrix.
  - with another key vector $\mathbf{b}= (b_1, b_2, \ldots, b_m)$
- plaintext of length m: $\mathbf{x}= (x_1, x_2, \ldots, x_m)$
- ciphertext of length m: $\mathbf{y}= (y_1, y_2, \ldots, y_m)$
- $e_k(\mathbf{x}) = \mathbf{x}\ \mathbf{A} + \mathbf{b}$ (mod 26),
- $d_k(\mathbf{y}) = (\mathbf{y-b})\ \mathbf{A}^{-1}$ (mod 26).

Permutation Cipher

- Also called Transposition Cipher
- Instead of replacing one text with another text, it alters the position of a block of m characters using a (secret) permutation table.

Permutation Cipher

- e. g. 1.7. (page 19) m=6: divide plaintext into blocks of 6 characters.
- permutation table as given.
- x -> п(x), x is the position, not the character.

x	1	2	3	4	5	6
$\pi(x)$	3	5	1	6	4	2

Example 1.7 (Permutation)

x	1	2	3	4	5	6
$\pi(x)$	3	5	1	6	4	2

p-1	p-2	p-3	p-4	p-5	p-6
s	h	e	s	e	l
l	s	s	e	a	s
h	e	l	l	s	b
y	t	h	e	s	e
a	s	h	o	r	e

Plaintext:

she sells seashells by the sea shore

Ciphertext:

eeslsh salses lshble hsyeet hraeos

Q-1	Q-2	Q-3	Q-4	Q-5	Q-6
p-3	p-5	p-1	p-6	p-4	p-2
e	e	s	l	s	h
s	a	l	s	e	s
l	s	h	b	l	e
h	s	y	e	e	t
h	r	a	e	o	s

Permutation "this is a final"

- thisis → [3(i)5(i)1(t)6(s)4(s)2(h)] =IITSSH
- afinal → [3(i)5(a)1(a)6(l)4(n)2(f)] =IAALNF
- IITSSH → [3(T)6(H)1(I)5(S)2(I)4(S)]=thisis
- IAALNF → [3(A)6(F)1(I)5(N)2(A)4(L)]=afinal

x	1	2	3	4	5	6
$\pi(x)$	3	5	1	6	4	2
$\pi^{-1}(x)$	3	6	1	5	2	4

Permutation vs. Hill Cipher

- textbook (page 20) : permutation cipher is a special case of Hill cipher with mxm matrix K defined according to the permutation matrix
  - **K** = (k_{ij}) , k_{ij} = 1 if i=π(j).
  - Inverse matrix of **K** is the permutation matrix corresponding to $π^{-1}$(x).
- Q: true ? verify ?

Stream cipher

- Block cipher (textbook definition): plaintext are encrypted using the same key K.
  - (other popular definition): group of plaintext symbols (block) transformed into one block of cipher symbols
- Stream cipher: (textbook definition): plaintext are encrypted using the a keystream.
  - (other popular definition): each plaintext symbol immediately transformed into one cipher symbol.

Snychronous Stream cipher

- Six-tuples: (P, C, K, L, E, D)
- P: finite set of possible plaintexts
- C: finite set of possible ciphertexts
- K: keyspace, finite set of possible keys
- L: keystream alphabets,
  - g: K → L, keystream generator, z_i =g(.) ε L.
- E: set of e_z(m): encryption P → C, z ε L
- D: set of d_z(c): decryption C → P such that $d_z(e_z(m))$ = m.

Stream vs. block cipher (textbook definition)

- block cipher is a special case of stream cipher with a constant key stream.
- Vigenere cipher is another special case of stream cipher with a periodic key stream. [larger period m is preferred. why ?]
  - $(k_1, k_2, \ldots, k_m)\ldots(k_1, k_2, \ldots, k_m)$
  - keystream generator: $z_i = k_i$, $1 \le i \le m$; $z_i = z_{i-m}$, $i>m$.
  - Q: how to generate a long period key stream ?

stream and block cipher (other popular definition)

- Speed of transformation
  - stream cipher is faster
- Problem of error propagation
  - block cipher tends to propagate its errors.
- Diffusion of plaintext information
  - block cipher is much better.
- Immunity to insertion of symbols.
  - block cipher is much better.

keystream generator (LFSR)

- Consider only binary alphabets.
- $P=C=L=Z_2 = \{0, 1\}$.
- $K= (Z_2)^m$, m="degree" or "order" of the recurrence equation
- $z_{i+m} = c_0 z_i + c_1 z_{i+1} + \ldots + c_{m-1} z_{i+m} \bmod 2$
- $z_{i+m} = c_0 z_i \oplus c_1 z_{i+1} \oplus \ldots \oplus c_{m-1} z_{i+m}$
  - $c_0 = 1$, other c_i is 0 or 1.
  - Max period = 2^m-1. How to choose ?

keystream generator example

- e.g. 1.8 (page 23)
- m=4, linear recurrence equation

  $z_{i+4} = z_i + z_{i+1} \bmod 2.$
- initial stream (1,0,0,0):
  - 100010011010111… (show!, period ?)
- initial stream (1,1,1,1):
  - 1111… (complete it!)

keystream generator e.g. 1.8

i	z(i)	z(i+1)	z(i+2)	z(i+3)	z(i+4)
0	1	0	0	0	1
1	0	0	0	1	0
2	0	0	1	0	0
3	0	1	0	0	1
4	1	0	0	1	1
5	0	0	1	1	0
6	0	1	1	0	1
7	1	1	0	1	0
8	1	0	1	0	1
9	0	1	0	1	1
10	1	0	1	1	1
11	0	1	1	1	1
12	1	1	1	1	0
13	1	1	1	0	0
14	1	1	0	0	0
15	1	0	0	0	1
16	0	0	0	1	0
17	0	0	1	0	0

period length=15=2^m-1

keystream generator period

i	z(i)	z(i+1)	z(i+2)	z(i+3)	z(i+4)
0	1	1	1	1	0
1	1	1	1	0	0
2	1	1	0	0	0
3	1	0	0	0	1
4	0	0	0	1	0
5	0	0	1	0	0
6	0	1	0	0	1
7	1	0	0	1	1
8	0	0	1	1	0
9	0	1	1	0	1
10	1	1	0	1	0
11	1	0	1	0	1
12	0	1	0	1	1
13	1	0	1	1	1
14	0	1	1	1	1
15	1	1	1	1	0
16	1	1	1	0	0
17	1	1	0	0	0

period length=15=2^m-1

Autokey Cipher

- non-synchronous stream cipher.
  - z_i in the key stream depends on its prious plaintexts or ciphetexts.
- Autokey Cipher:
- $P=C=K=L=Z_{26}$.
- $z_1=K$. For $i>1$, $z_i = x_{i-1}$.
- $e_z(x) = (x+z) \bmod 26$.
- $d_z(x) = (y-z) \bmod 26$.

Example 1.9 (pages 24-25)

plain	r	e	n	d	e	z	v	o	u	s
code	17	4	13	3	4	25	21	14	20	18
key	8	17	4	13	3	4	25	21	14	20
e(x)	25	21	17	16	7	3	20	9	8	12
cipher	Z	V	R	Q	H	D	U	J	I	M

y	25	21	17	16	7	3	20	9	8	12
d(y)	17	4	13	3	4	25	21	14	20	18
	25-K	21-17	17-4	16-13	7-3 mod 26	3-4 mod 26	20-25 mod 26	9-21 mod 26	8-14 mod 26	12-20 mod 26
plain	r	e	n	d	e	z	v	o	u	s

Summary and HW1

- What we have learned so far ?
- Various ciphers ?
- Mathematical tools ?

- HW1: 1.1, 1.5, 1.10, 1.15, 1.16, 1.18, 1.23.