Information Protection & Computer Security

Rajendra Kachhwaha
Email: rajendra1983@gmail.com

June 18, 2015

1. Security Architecture, Security Attacks, Security Services.

2-3.Model for Network Security,Basic terms used in Cryptography, Symmetric Cipher Model, Substitution Techniques, Transpositions Techniques.

4.Block Cipher and Stream Ciphers,Component of Modern Block Cipher, Feistel Cipher Structure, Data Encryption Standard (DES)

- Lecture 5.

  Today's Topic: Numerical Problems on:

  Caesar Cipher

  Monoalphabetic Cipher

  Playfair Cipher

  Hill Cipher

  One-Time Pad

  Vigenere Cipher

  Rail fence Cipher

- **Caesar Cipher:**

  Example 1: "welcome to jodhpur" with key=5, converted into "bjqhtrj yt otimuzw"

  Home work: "This is jodhpur national university" with key=4, converted into "xlmw mw nshltyv rexmsrep yrmzivwmxc'.

- **Monoalphabetic Cipher:**

  Example 1: "welcome to jodhpur" with key=ISYVKJRUXEDZQMCTPLOFNBWGAH, converted into "wkzycqk fc ecvutnl".

  Home work: Encryption of "hide the gold" with key=ISYVKJRUXEDZQMCTPLOFNBWGAH would be "uxvk fuk rczv".

- **Playfair Cipher:**

  Example: Using the keyword "MONARCHY"

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

  Example 1: "welcome to jodhpur" is converted into "ug ue no kl af rh fv zm"

  Home work: Encryption of "hide the gold" with the key of "hello world" would be "LFGDNWDPWOAV".

- **Hill Cipher:**

  For m=3, the system can be described as follows:

$$c_1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \bmod 26$$
$$c_2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \bmod 26$$
$$c_3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \bmod 26$$

This can be expressed in term of column vectors and matrices:

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} \bmod 26$$

or

$$\mathbf{C} = \mathbf{KP} \bmod 26$$

where **C** and **P** are column vectors of length 3, representing the plaintext and ciphertext, and **K** is a 3×3 matrix, representing the encryption key. Operations are performed mod 26.

For example, consider the plaintext "paymoremoney" and use the encryption key

$$\mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

The first three letters of the plaintext are represented by the vector $\begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix}$. Then $\mathbf{K}\begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} = \begin{pmatrix} 375 \\ 819 \\ 486 \end{pmatrix} \bmod 26 = \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix}$ = LNS. Continuing in this fashion, the ciphertext for the entire plaintext is LNSHDLEWMTRW.

- **Hill Cipher:**

  Example 1:plaintext: "welcome to jodhpur" with key=(3 2 3 1) (key is:top row, bottom row) is converted into "wsljocyfizwtzkqz".

  Home work: Encryption of "hide the gold" with the key=(3 2 3 1) would be "ldrntmysmbdg".

One-Time Pad:

the letters would first be converted to their numeric equivalents, as shown here.

V	E	R	N	A	M	C	I	P	H	E	R
21	4	17	13	0	12	2	8	15	7	4	17

Next, we must generate random numbers to combine with the letter codes. Suppose the following series of random two-digit numbers is generated.

76 48 16 82 44 03 58 11 60 05 48 88

The encoded form of the message is the sum mod 26 of each coded letter with the corresponding random number. The result is then encoded in the usual base-26 alphabet representation.

Plaintext	V	E	R	N	A	M	C	I	P	H	E	R
Numeric Equivalent	21	4	17	13	0	12	2	8	15	7	4	17
+ Random Number	76	48	16	82	44	3	58	11	60	5	48	88
= Sum	97	52	33	95	44	15	60	19	75	12	52	105
= mod 26	19	0	7	17	18	15	8	19	23	12	0	1
Ciphertext	t	a	h	r	s	p	i	t	x	m	a	b

Thus, the message

VERNAM CIPHER

is encoded as

tahrsp itxmab

Homework: Formulate the decryption process.

$[26 - ([K - C] mod 26)] mod 26$

- **Vigenere Cipher:**

  The Vigenere Cipher is a substitution cipher.

  The Vigenere Cipher uses the table to encipher the plaintext.

  To encipher a message, repeat the key above the plaintext.

  Example 1:plaintext:"welcome to jodhpur" with key="welcome" is converted into "siwecyipsuqrttqv".
  T: welcometojodhpur
  K: welcomewelcomewe
  C: siwecyipsuqrttqv

  Home work:Encryption of "hide the gold" with the key of "helloworld" would be "omophdsxzok".

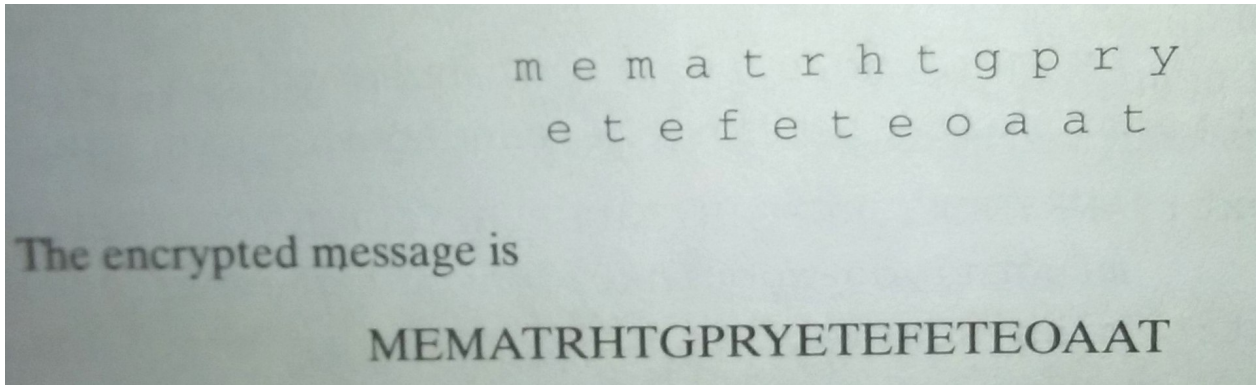
- **Vigenere Cipher: vigenere table**

TABLE 2-1 Vigenère Tableau.

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

- **Rail Fence Cipher:**

  Example: write message out as: "meet me after the toga party".



  Home work:plaintext: "welcome to jodhpur" with key=3 is converted into "woohecmtjdprleou".

  Home work:plaintext: "welcome to jodhpur" with key=5 is converted into "woetjrleoucmdpoh".