Department of Electronics

Cryptography

Fall 2019

Hasan Mahmood

hasan@qau.edu.pk

Week 4 (25 & 26 September)

The Playfair and ADFGX Ciphers

- Used in World War I (Weak)
- Repeated letters are removed from the key (playfair -> playfir)
- Start a 5x5 matrix
- i and j being treated as one letter

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

The Playfair and ADFGX Ciphers

- Plaintext: *meet at the schoolhouse*
- Remove the spaces and divide the text into groups of two letters
- *me et at th es ch ox ol ho us ex.* (insert x where double letter appears)
- Use the matrix to encrypt each two letter group

EG MN FQ QM KN BK SV VR GQ XN KU.

Use the reverse to perform decryption. (Frequency attack?)

Now use the matrix to encrypt each two letter group by the following scheme:

- If the two letters are not in the same row or column, replace each letter by the letter that is in its row and is in the column of the other letter. For example, et becomes MN, since M is in the same row as e and the same column as t, and N is in the same row as t and the same column as e.

- If the two letters are in the same row, replace each letter with the letter immediately to its right, with the matrix wrapping around from the last column to the first. For example, me becomes EG.

- If the two letters are in the same column, replace each letter with the letter immediately below it, with the matrix wrapping around from the last row to the first. For example, ol becomes VR.

ADFGX Cipher

- Each plaintext letter is replaced by the label of its row and column
- For example: plaintext *Kaiser Wilhelm* is encrypted as

XA FF GG FA AG DX GX GG FD XX AG FD GA.

	A	*D*	*F*	*G*	*X*
A	*p*	*g*	*c*	*e*	*n*
D	*b*	*q*	*o*	*z*	*r*
F	*s*	*l*	*a*	*f*	*t*
G	*m*	*d*	*v*	*i*	*w*
X	*k*	*u*	*y*	*x*	*h*

ADFGX Substitution Cipher further complexity

- Choose a keyword, for example *Rhein*
- Label column of a matrix bny letters of the keyword
- Put the result of initial step into another matrix:

R	*H*	*E*	*I*	*N*
X	*A*	*F*	*F*	*G*
G	*F*	*A*	*A*	*G*
D	*X*	*G*	*X*	*G*
G	*F*	*D*	*X*	*X*
A	*G*	*F*	*D*	*G*
A				

Now reorder the columns so that the column labels are in alphabetic order:

E	H	I	N	R
F	A	F	G	X
A	F	A	G	G
G	X	X	G	D
D	F	X	X	G
F	G	D	G	A
				A

ADFGX Cipher

- The cipher text becomes:

FAGDFAFXFGFAXXDGGGXGXGDGAA.

- ADFGX Cipher which uses 6x6 matrix
- Allowed all 26 characters plus 10 digits to be used

Block Ciphers

- Change in one letter in the plaintext changes on letter in the cipher text
- In shift, affine and substitution ciphers, encrypted letter comes from one letter in the plaintext
- In Vigenere system, block of letters are used
- Makes the frequency analysis more difficult, but still possible
- Block letters avoid these problems by encrypting block of letters simultaneously
- A change in one character in plaintext block should change potentially all characters in the corresponding ciphertext block. (Playfair cipher)

Block Ciphers

- DES operates on 64 bit
- AES uses blocks of 128 bits
- RSA uses blocks of several hundred bits long (depends on modulus)
- All lengths are long enough to resist against frequency attacks

- Electronics Codebook (ECB) mode (convert one block at a time)
- Ways to use feedback from the blocks of ciphertext in the enycription of subsequent blocks of plaintext, called cipher block chaining (CBC)
- Or Cipher feedback (CFB) mode

Hill Cipher

- Block cipher
- Algebraic method was used for the first time (liner algebra, mod math)
- Algebraic methods are used in modern encryption methods
- Choose an integer *n*, for example, *n=3*
- The key is an *nxn* matrix *M*, whose entries are integers mod 26

$$M = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix}$$

Hill Cipher

- Message is written as a series of row vectors: abc -> (0, 1, 2)
- To encrypt, multiply the vector by the matrix

$$(0, 1, 2)\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \equiv (0, 23, 22) \pmod{26}.$$

- Therefore, the ciphertext is: *AXW*

Hill Cipher

- In order to decrypt, we need the determinany of M to satisfy

$$\gcd(\det(M), 26) = 1.$$

- There is a matrix *N* with integer entries such that *MN=I* (mod 26)
- I is an nxn identity matrix

Hill Cipher

- In this example,
- Det(*M*)=-3
- The inverse of *M* is

$$\frac{-1}{3}\begin{pmatrix} -14 & 11 & -3 \\ 34 & -25 & 6 \\ -19 & 13 & -3 \end{pmatrix}$$

Hill Cipher

- Replace -1/3 by 17
- Reduce mode to 26

$$N = \begin{pmatrix} 22 & 5 & 1 \\ 6 & 17 & 24 \\ 15 & 13 & 1 \end{pmatrix}.$$

- *MN=I* (mod 26)

Hill Cipher Decryption

- Multiply ciphertext with *N*

$$(0, 23, 22)\begin{pmatrix} 22 & 5 & 1 \\ 6 & 17 & 24 \\ 15 & 13 & 1 \end{pmatrix} \equiv (0, 1, 2) \pmod{26}.$$

$$\textit{blockcipher}.$$

This becomes (we add an x to fill the last space)

$$1 \quad 11 \quad 14 \qquad 2 \quad 10 \quad 2 \qquad 8 \quad 15 \quad 7 \qquad 4 \quad 17 \quad 23.$$

Now multiply each vector by M, reduce the answer mod 26, and change back to letters:

$$(1,11,14)M = (199,183,181) \equiv (17, \; 1,25) \pmod{26} = RBZ$$

$$(2,10, \; 2)M = (\; 64, \; 72, \; 82) \equiv (12,20, \; 4) \pmod{26} = MUE,$$

etc.

In our case, the ciphertext is

$$RBZMUEPYONOM.$$

Hill Cipher, Cryptanalysis

- Known plaintext attacks
- If we do not know *n*, we can try various values until we find the tight one
- For example:

$$howareyoutoday =$$

$$7\ \ 14\quad 22\ \ 0\quad 17\ \ 4\quad 24\ \ 14\quad 20\ \ 19\quad 14\ \ 3\quad 0\ \ 24$$

corresponding to the ciphertext

$$ZWSENIUSPLJVEU =$$

$$25\ \ 22\quad 18\ \ 4\quad 13\ \ 8\quad 20\ \ 18\quad 15\ \ 11\quad 9\ \ 21\quad 4\ \ 20$$

The first two blocks yield the matrix equation

$$\begin{pmatrix} 7 & 14 \\ 22 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 25 & 22 \\ 18 & 4 \end{pmatrix} \pmod{26}.$$

Unfortunately, the matrix $\begin{pmatrix} 7 & 14 \\ 22 & 0 \end{pmatrix}$ has determinant -308, which is not invertible mod 26 (though this matrix could be used to reduce greatly the number of choices for the encryption matrix). Therefore, we replace the last row of the equation, for example, by the fifth block to obtain

$$\begin{pmatrix} 7 & 14 \\ 20 & 19 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 25 & 22 \\ 15 & 11 \end{pmatrix} \pmod{26}.$$

In this case, the matrix $\begin{pmatrix} 7 & 14 \\ 20 & 19 \end{pmatrix}$ is invertible mod 26:

$$\begin{pmatrix} 7 & 14 \\ 20 & 19 \end{pmatrix}^{-1} \equiv \begin{pmatrix} 5 & 10 \\ 18 & 21 \end{pmatrix} \pmod{26}.$$

We obtain

$$M \equiv \begin{pmatrix} 5 & 10 \\ 18 & 21 \end{pmatrix} \begin{pmatrix} 25 & 22 \\ 15 & 11 \end{pmatrix} \equiv \begin{pmatrix} 15 & 12 \\ 11 & 3 \end{pmatrix} \pmod{26}.$$

Claude Shannon foundations of cryptography

- Two properties

1. Diffusion
    - If we change a character of the plaintext, then several characters of the ciphertext should change
    - If we change a character of ciphertext, then several characters of the plaintext should change (Property exhibited by Hill cipher)
    - Frequency statistics of letters, diagrams, etc. in the plaintext are diffused over several characters in the cyphertext (more ciphertext is needed to do a meaningful statistical attack)

Claude Shannon foundations of cryptography

- Confusion
  - Key does not relate in a simple way to the ciphertext
  - Each character of the ciphertext should depend on several parts of the key
  - Hill cipher with *nxn* matrix, plaintext-ciphertext pair of length n^2 (difficult to solve)
  - If we change one character of the ciphertext one column of the matrix can change completely
  - It is desirable to have the entire key change
  - Vigenere and substitution ciphers do not have the properties of diffusion and confusion (Frequency analysis possible)
  - Modern ciphers, both properties are present
  - Error propagation (advantage/disadvantage?)

One Time Pads

- Unbreakable system, represent the message as 0s and 1s
- The key is a random sequence of 0s and 1s of the same length
- Once a key is used, it is discarded and never used again (only for decryption)
- Encryption consists of adding the key to the message mod 2 bit by bit (exclusive OR)

$$
\begin{array}{rr}
\text{(plaintext)} & 00101001 \\
\text{(key)} + & \underline{10101100} \\
\text{(ciphertext)} & 10000101
\end{array}
$$

Pseudo-random Bit Generation

- One time pad requires long key
- Natural randomness in nature (thermal noise for example)
- Pseudo random no. generator (rand () function in C language, seed)
- $x_n = ax_{n-1} + b \pmod{m}$
- Only useful for experimental purpose, because the sequence is predictable

Blum-Blum-Shub (BBS) Pseudo-random bit generator (quadratic residue generator)

- Generate two large prime numbers *p* and *q*
- We set $n=pq$ and choose a random integer x
- Initial seed is set to $x_0=x^2$ (mod n)
- The BBS generator produces a sequence of random bits $b_1, b_2, \ldots$ by

1. $x_j \equiv x_{j-1}^2 \pmod{n}$
2. b_j is the least significant bit of x_j.

Example. Let

$$p = 24672462467892469787 \text{ and } q = 39673684567834589803,$$

$$n = 978847614085311079416885521741371578196 1.$$

Take $x = 873245647888478349013$. The initial seed is

$$\begin{aligned} x_0 &\equiv x^2 \pmod{n} \\ &\equiv 88452987104787800970899177460101228631 72. \end{aligned}$$

The values for $x_1, x_2, \cdots x_8$ are

$$
\begin{aligned}
x_1 &\equiv 71188942811313295227459624554981238 22408 \\
x_2 &\equiv 314517460888889316415138015206070 4518227 \\
x_3 &\equiv 489800778230715623327223318555748 99430355 \\
x_4 &\equiv 393545781893511292234709354618967 2310389 \\
x_5 &\equiv 67509951151009704890176130319874 0246040 \\
x_6 &\equiv 428991482877174013354619065826651 5171326 \\
x_7 &\equiv 443106671145437826089038638559381 7521668 \\
x_8 &\equiv 733687612419504639741423533367500 5372436.
\end{aligned}
$$

Taking the least significant bit of each of these, which is easily done by checking whether the number is odd or even, produces the sequence $b_1, \cdots, b_8 = 0, 1, 1, 1, 0, 0, 0, 0$. ∎