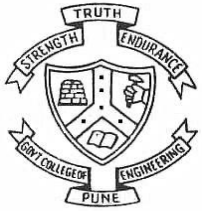
Cryptography and Network Security

Session 5

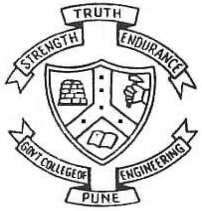
V. K. Pachghare



Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Classical Encryption Techniques

- Playfair Cipher
- Hill Cipher



Playfair Cipher

- Divided the plaintext into a group of two letters each
- Each group is treated as a single unit
- Using the key, for groups of plaintext, corresponding ciphertext groups are generated

Encryption

- Encryption process is divided into three parts:
  - Preparing the Plaintext
  - Preparing the Key
  - Encryption

Preparing the Plaintext

Step 1 Convert this message into lowercase letters and remove punctuations.

We live in a world full of beauty

weliveinaworldfullofbeauty

Step 2 Split the text into a pair of two.

we li ve in aw or ld fu ll of be au ty

If the last group is having only one letter, then append any one letter in that group to make a pair

- If both the letters in a pair are same, then split this pair by adding any letter in between the letters and rearrange the groups.
- we li ve in aw or ld fu **ll** of be au ty
- In this example, one of the pairs having same letters "ll" (shown in bold). Add letter "x" in between the letters, so the group is "lxl". But the group should be of two letters, so shift the last letters of this group to the right by one position and rewrite the groups again.

  we li ve in aw or ld fu **lx l**o fb ea ut **y**

- Here the last group is having only one letter, so append one more letter to complete the pair. Here we append “z” with the last letter “y” as shown below:

  we li ve in aw or ld fu lx lo fb ea ut yz

- Step 3 Now, write the groups such that in one row 5 pairs are there as shown below:
- If j is present all j are replaced with i. (or any letter)

we	li	ve	in	aw
or	ld	fu	lx	lo
fb	ea	ut	yz	

Preparing the Key

- Select the key having any number of letters
- Remove the duplicate letters
- Convert all the letters of the key into uppercase letters
- To prepare the key, 5 × 5 matrix is constructed

- Suppose the key is “another”
- Step 1 Convert the key into uppercase letters, the key becomes

  ANOTHER
- Step 2 Write the letters in the 5 × 5 matrix form, i.e., 5 letters in one row as shown below:

  A N O T H

  E R

- Step 3 The remaining letters of the alphabet which are not present in the key are filled in the alphabetical order as shown below: (we use i for replacement to j, we can use any letter, total count must be 25)

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

Encryption

- Each letter in a pair that is on the **same row** is replaced by the letter to the right. The letter to the right of the rightmost letter is the first letter in the same row. Ex. **RC => BD**

UQ => MS

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

- letters in the same column are replace by the next letter below in the same column. Ex. TK=> CS

WG=>NP

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

- when the letters are neither in the same row nor column, the substitution is based upon their intersection
- first move across (left or right), and then up or down.

Ex. **WE => VR**

CZ => DY

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

PT:- WE LI VE IN AW OR LD FU LX LO FB EA UT YZ

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

CT:- **VR FK AF GO NV NB UL LM IZ IH IE FE SH ZV**

- Finally, perform this transformation for each pair of letters in the modified plaintext and remove the spaces

- The Ciphertext is:

PT:- **WE LI VE IN AW OR LD FU LX LO FB EA UT YZ**

CT:- **VR FK AF GO NV NB UL LM IZ IH IE FE SH ZV**

Decryption

- To decrypt the message, simply reverse the entire process. Break the ciphertext into pairs of letters:

VR FK AF GO NV
NB UL LM IZ IH
IE FE SH ZV

Write down the alphabet square with the key:

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

AF=>VE

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

- Transform the pairs of letters in the opposite direction from that used for encryption:

WE LI VE IN AW
OR LD FU LX LO
FB EA UT YZ

We live in a world full of beauty

Disadvantage

- Cryptanalysis of the Playfair cipher is easy, as the same pair of letters always converted into a same pair of ciphertext.

The Hill Cipher

- The Hill cipher is a polygraphic substitution cipher based on linear algebra
- Each letter is treated as a digit in base 26: A = 0, B =1, and so on.

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

- Consider the message 'COE', and the key below (or “ANOTGERBZ” in letters):
- Ciphertext = Key x Plaintext mod 26

  C = KP mod 26

Encryption

Encryption process is divided into three parts:

- Preparing the Plaintext
- Preparing the Key
- Encryption

Preparing the Plaintext

- First each letter in the message is converted into numbers such as a = 0, b = 1 and so on.
- Then the numbers should be written in columnar form. The number of letters in each column depends on the size of the key matrix.

- Suppose the key matrix is 2 × 2, then each column of plaintext has two elements only.
- Suppose the key matrix is 3 × 3 matrix, then each column of plaintext has three elements only.
- If the last column contains less elements then append necessary numbers to complete the last column.

Consider the message ‘COE’.

- Since 'C' is 2, 'O' is 14 and 'E' is 4, the message is the vector:

$$P = \begin{bmatrix} 2 \\ 14 \\ 4 \end{bmatrix}$$

Preparing the Key

- Key matrix should be a square matrix.
- i,.e. the size of the key must be a square value.
- For example, size of a matrix should be 4 or 9 or 16 etc.
- Every letter in the key is also assigning the number like message.

- The numbers should be written in row wise.
- The number of letters in each row depends on the size of the key matrix.
- Suppose, the key matrix is 2×2, then each row having two elements only.
- The key matrix is always a square matrix

- Consider the key “ANOTGERBZ”
- Convert it into numbers as: 0 13 14 19 6 4 17 1 25.
- Then write these numbers in a matrix form as:
- Thus the enciphered vector is given by:

$$K = \begin{bmatrix} 0 & 13 & 14 \\ 19 & 6 & 4 \\ 17 & 1 & 25 \end{bmatrix}$$

Encryption

Ciphertext = Key x Plaintext mod 26

C = KP mod 26

$$C = \begin{bmatrix} 0 & 13 & 14 \\ 19 & 6 & 4 \\ 17 & 1 & 25 \end{bmatrix} \begin{bmatrix} 2 \\ 14 \\ 4 \end{bmatrix} = \begin{bmatrix} 238 \\ 138 \\ 148 \end{bmatrix} \text{mod } 26$$

$$C = \begin{bmatrix} 4 \\ 8 \\ 18 \end{bmatrix}$$

Here the numbers are reconverted into the letters, so, 4 = E, 8 = I, 18 = S. So the ciphertext is 'EIS'.

Decryption

- Again we have to perform matrix multiplication.
- $P = K^{-1} C \bmod 26$
- Inverse of the key matrix is calculated using standard methods with extended Euclidean algorithm [Because (1/det)mod 26]

$$P = K^{-1} \times \mathrm{C} \ \mathrm{MOD}\ 26$$

$$K^{-1} = \frac{1}{6453} \begin{bmatrix} -146 & 311 & 32 \\ 407 & 238 & -266 \\ 83 & -211 & 247 \end{bmatrix} \bmod 26$$

$$K^{-1} = \frac{1}{6453} \begin{bmatrix} -16 & 25 & 6 \\ 17 & 4 & -6 \\ 5 & -3 & 13 \end{bmatrix} \bmod 26$$

Here first compute 6453 mod 26 = 5, then find the multiplicative inverse of 5 such that 5 d mod 26 = 1, where d is the multiplicative inverse of 5.

$$K^{-1} = \frac{1}{5}\begin{bmatrix} -16 & 25 & 6 \\ 17 & 4 & -6 \\ 5 & -3 & 13 \end{bmatrix} \bmod 26$$

Extended Euclidean algorithm

Find out the multiplicative inverse of 5 mod 26

$26 = 5(5) + 1$ $\qquad\qquad$ $1 = 26 - 5(5)$

$1 = 26 - 5(5)$
$1 = 26 + 5(-5)]$

-5 is the multiplicative inverse of 5 mod 26 which is equal to (-5 + 26) mod 26 = 21 mod 26

So, 21 is the multiplicative inverse of 5 mod 26

Now replace (1/5) by 21

$$K^{-1} = 21 \begin{bmatrix} -16 & 25 & 6 \\ 17 & 4 & -6 \\ 5 & -3 & 13 \end{bmatrix} \bmod 26$$

$$K^{-1} = \begin{bmatrix} -24 & 5 & 22 \\ 19 & 6 & -22 \\ 1 & -11 & 13 \end{bmatrix} \bmod 26$$

$$K^{-1} = \begin{bmatrix} 2 & 5 & 22 \\ 19 & 6 & 4 \\ 1 & 15 & 13 \end{bmatrix} \bmod 26$$

Now, our ciphertext "EIS" is multiplied by this new key, we get:

$$P = \begin{bmatrix} 2 & 5 & 22 \\ 19 & 6 & 4 \\ 1 & 15 & 13 \end{bmatrix} \begin{bmatrix} 4 \\ 8 \\ 18 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2 \\ 14 \\ 4 \end{bmatrix}$$

The plaintext we get back is 'COE'.

Advantages

- The ciphertext letter generated for a letter in plaintext is not dependent upon only a single plaintext letter but it is a combination of many letters.
- This helps to avoid the letter frequency problem. It is therefore difficult for cryptanalysis and provides more security.

Disadvantage

- This cipher uses linear algebra, which makes easy for a known plaintext attack