



SUBSTITUTION TECHNIQUES



- A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.

Caesar Cipher

- The earliest known, and the simplest, use of a substitution cipher was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing **three places** further down the alphabet.



e.g.,

plain text : pay more money

Cipher text: SDB PRUH PRQHB

Note that the alphabet is wrapped around, so that the letter following Z is A.

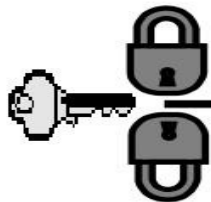
- Plain: a b c d e f g h i j k l m n o p q r s t u v w x y z*
- cipher: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C*



- *For each plaintext letter p , substitute the cipher text letter c such that*
- **$C = E(p) = (p+3) \bmod 26$**
- *A shift may be any amount, so that general Caesar algorithm is*
- **$C = E(p) = (p+k) \bmod 26$**
- *Where k takes on a value in the range 1 to 25. The decryption algorithm is simply*
- **$P = D(C) = (C-k) \bmod 26$**



Monoalphabetic Cipher



Monoalphabetic Cipher

- Rather than just shifting the alphabet
- Could shuffle (jumble) the letters arbitrarily
- Each plaintext letter maps to a different random cipher text letter
- hence key is 26 letters long

Plain: abcdefghijklmnopqrstuvwxyz

Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN

Plaintext: ifwewishtoreplaceletters

Cipher text: WIRFRWAJUHYFTSDVFSFUUFYA



Playfair Cipher



- The Playfair algorithm is based on the use of 5x5 matrix of letters constructed using a keyword. Let the keyword be "**monarchy**".
- The matrix is constructed by filling in the letters of the keyword from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetical order.
- The letter "**i**" and "**j**" count as one letter. Plaintext is encrypted two letters at a time According to the following rules:
- Repeating plaintext letters that would fall in the same pair are separated with a Filler letter such as "x".



Rules



1. Splitting 2 letters as a unit
2. Repeating letter-Filler letter (Eg: balloon- ba lx lo on)
3. Same row | → | Wrap around
4. Same Column | ↓ | wrap around
5. Rectangle | ↔ | Swap



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



Plain Text: me (Same column)

Cipher Text: CL

Plain Text: st (Same Row)

Cipher Text: TL

Plain Text: nt (Rectangle)

Cipher Text: RQ

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



Plain Text:meet me at the school house

Splitting two letters as a unit => me et me at th es ch o x ol ho us ex

Corresponding cipher text => CL KL CL RS PD IL HY AV MP HF XL
IU



Hill Cipher



- Another interesting multiletter cipher is the Hill cipher, developed by the mathematician Lester Hill in 1929.
- The Hill cipher makes use of modulo arithmetic, matrix multiplication, and matrix inverses; hence, it is a more mathematical cipher than others.

A	B	C	D	E	F	G	H	I	J	K	L	M
↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
13	14	15	16	17	18	19	20	21	22	23	24	25



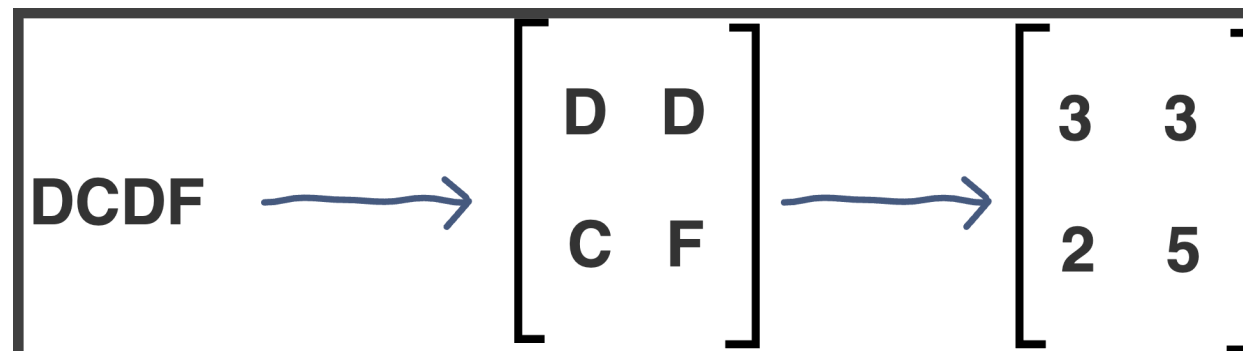
Encryption



$$E(K, P) = (K * P) \text{ mod } 26$$

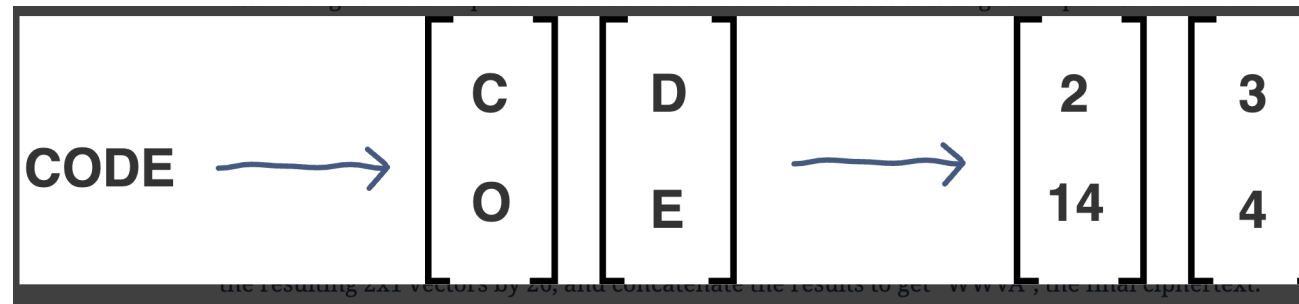
Where K is our key matrix and P is the plaintext in vector form. Matrix multiplying these two terms produces the encrypted ciphertext.

1. Pick a keyword to encrypt your plaintext message. Let's work with the random keyword "DCDF". Convert this keyword to matrix form using your substitution scheme to convert it to a numerical 2x2 key matrix.





2. we will convert our plaintext message to vector form. Since our key matrix is 2×2 , the vector needs to be 2×1 for matrix multiplication to be possible. In our case, our message is four letters long so we can split it into blocks of two and then substitute to get our plaintext vectors.





$$\begin{array}{l} \left[\begin{array}{cc} D & D \\ C & F \end{array} \right] \times \left[\begin{array}{c} C \\ O \end{array} \right] \longrightarrow \left[\begin{array}{cc} 3 & 3 \\ 2 & 5 \end{array} \right] \times \left[\begin{array}{c} 2 \\ 14 \end{array} \right] = \left[\begin{array}{c} 48 \\ 74 \end{array} \right] \% 26 = \left[\begin{array}{c} 22 \\ 22 \end{array} \right] \longrightarrow \left[\begin{array}{c} W \\ W \end{array} \right] \\ \left[\begin{array}{cc} D & D \\ C & F \end{array} \right] \times \left[\begin{array}{c} D \\ E \end{array} \right] \longrightarrow \left[\begin{array}{cc} 3 & 3 \\ 2 & 5 \end{array} \right] \times \left[\begin{array}{c} 3 \\ 4 \end{array} \right] = \left[\begin{array}{c} 21 \\ 26 \end{array} \right] \% 26 = \left[\begin{array}{c} 21 \\ 0 \end{array} \right] \longrightarrow \left[\begin{array}{c} V \\ A \end{array} \right] \end{array} \left. \vphantom{\begin{array}{l} \left[\begin{array}{cc} D & D \\ C & F \end{array} \right] \times \left[\begin{array}{c} C \\ O \end{array} \right] \longrightarrow \left[\begin{array}{cc} 3 & 3 \\ 2 & 5 \end{array} \right] \times \left[\begin{array}{c} 2 \\ 14 \end{array} \right] = \left[\begin{array}{c} 48 \\ 74 \end{array} \right] \% 26 = \left[\begin{array}{c} 22 \\ 22 \end{array} \right] \longrightarrow \left[\begin{array}{c} W \\ W \end{array} \right]} \right\} \text{WWVA}$$




Decryption



- $D(K, C) = (K^{-1} * C) \bmod 26$

Inverse of a Matrix

If $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ then

 $A^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

Inverse of A **Determinant of A** **Adjoint of A**

Note: A^{-1} exists only when $ad - bc \neq 0$



Polyalphabetic Cipher



Vigenere Cipher

$$C_i = (p_i + k_i) \bmod 26 \text{ (Encryption)}$$

$$p_i = (C_i - k_i) \bmod 26 \text{ (Decryption)}$$

- The first letter of the key is added to the first letter of the plaintext, mod 26
- The second letters are added, and so on through the first m letters of the plaintext.
- For the next m letters of the plaintext, the key letters are **repeated**. This process continues until all of the plaintext sequence is encrypted.



Vigenere Cipher

Key : deceptivedeceptivedeceptive

Plaintext : wearędiscoveredsaveyourself

Ciphertext : ZICVTWQNGRZGVTVAVZHCQYGLMGJ

Key	3	4	2	4	15	19	8	21	4	3	4	2	4
PT	22	4	0	17	4	3	8	18	2	14	21	4	17
CT	25	8	2	21	19	22	16	13	6	17	25	6	21

Key	15	19	8	21	4	3	4	2	4	15	19	8	21	4
PT	4	3	18	0	21	4	24	14	20	17	18	4	11	5
CT	19	22	0	21	25	7	2	16	24	6	11	12	6	9

NESO ACADEMY



$$25 \bmod 26 = 25$$

$$8 \bmod 26 = 8$$

$$39 \bmod 26 = 13$$



Vernam Cipher



- Introduced by Gilbert Vernam in 1918. His system works on binary data (bits) rather than letters.
- Vernam proposed the use of a running loop of tape that eventually repeated the key, so that in fact the system worked with a very long but repeating keyword.

$$E (P_i , K_i) = P_i \text{ (XOR) } K_i$$

$$D (C_i , K_i) = C_i \text{ (XOR) } K_i$$



Plain-Text: O A K

Key: S O N

O ==> 14 = 0 1 1 1 0

S ==> 18 = 1 0 0 1 0

Bitwise XOR Result: 1 1 1 0 0 = 28

Since the resulting number is greater than 26, subtract 26 from it.

28 - 26 = 2 ==> C

CIPHER-TEXT: C



One time pad



One Time Pad algorithm is the improvement of the **Vernam Cipher**

- The key should be **randomly generated as long as the size of the message.**
- The key is to be used to encrypt and decrypt **a single message, and then it is discarded.**
- So encrypting every new message requires a new key of the same length as the new message in one-time pad.

One-Time Pad is the only algorithm that is truly unbreakable and can be used for low-bandwidth channels requiring very high security(**ex. for military uses**).



Transposition Techniques



Rail Fence Technique

- Rail fence is simplest of such cipher, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

Plaintext = meet at the school house

- To encipher this message with a rail fence of depth 2,

- **m e a t e c o l o s**

- **e t t h s h o h u e**

- *The encrypted message is*

Cipher Text=MEATECOLOSETTSHOHUE



Row-Transposition Cipher

- A more complex scheme is to write the message in a rectangle, row by row, and read the message off, **column by column**, but permute the order of the columns. The order of columns then becomes the key of the algorithm.

plaintext = meet at the school house

Key = 4 3 1 2 5 6 7

4	3	1	2	5	6	7
M	E	E	T	A	T	T
H	E	S	C	H	O	O
L	H	O	U	S	E	X

Cipher Text: ESOTCUEEHMHLAHSTOETOX



Stegnography



Steganography is the practice of concealing information within another message or physical object to avoid detection.

Example: **S**imply **e**ncrypt **c**orrect **r**eading **e**xactly **t**wice.

- **Character marking:** Selected letters of printed or typewritten text are over-written in pencil. The marks are ordinarily not visible unless the paper is held at an angle to bright light.
- **Invisible ink:** A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.
- **Pin punctures:** Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light.
- **Typewriter correction ribbon:** Used between lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.