Vernam, Vigenere, Book and Rotor cipher

Vernam Cipher

- **Vernam Cipher** is a method of encrypting alphabetic text.
- It is one of the Transposition techniques for converting a plain text into a cipher text.
- In this mechanism we assign a number to each character of the Plain-Text, like (a = 0, b = 1, c = 2, … z = 25).

One Time Pad

- One-time pad cipher is a type of Vignere cipher which includes the following features −
- It is an unbreakable cipher.
- The key is exactly same as the length of message which is encrypted.
- The key is made up of random symbols.
- As the name suggests, key is used one time only and never used again for any other message to be encrypted.

- Due to this, encrypted message will be vulnerable to attack for a cryptanalyst. The key used for a one-time pad cipher is called **pad**, as it is printed on pads of paper.

Key

- In Vernam cipher algorithm, we take a key to encrypt the plain text which length should be equal to the length of the plain text.

Encryption Algorithm:

1. Assign a number to each character of the plain-text and the key according to alphabetical order.

2. Add both the number (Corresponding plain-text character number and Key character number).

3. Subtract the number from 26 if the added number is greater than 26, if it isn't then leave it.

Example:

- **Plain-Text:** RAMSWARUPK
- **Key:** RANCHOBABA

PT: R A M S W A R U P K

NO: 17 0 12 18 22 0 17 20 15 10

KEY: R A N C H O B A B A

NO: 17 0 13 2 7 14 1 0 1 0

- Now add the number of Plain-Text and Key and after doing the addition and subtraction operation (if required), we will get the corresponding Cipher-Text character number.

  CT-NO: 34 0 25 20 29 14 18 20 16 10

- In this case, there are two numbers which are greater than the 26 so we have to subtract 26 from them and after applying the subtraction operation the new Cipher text character numbers are as follow:

  CT-NO: 8 0 25 20 3 14 18 20 16 10

  New Cipher-Text is after getting the corresponding character from the number.

  CIPHER-TEXT: I A Z U D O S U Q K

- **For the *Decryption* apply the just reverse process of encryption.**

Vigenère Cipher

- Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution.

- A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets .

- The encryption of the original text is done using the *Vigenère square or Vigenère table*.

Vigenere cipher

- The Vigenere cipher is the kind of polyalphabetic cipher.
- It was design by Blaise de Vigenere, a 16th century French mathematician.
- It was used in the American civil war and was once believed to be unbreakable.
- A Vigenere cipher uses a different strategy to create the key stream. The key stream is a repetition of an initial secret key stream of length m, where we have 1<=m<=26.
- The Vigenere cipher is a method of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword.
- The Vigenere cipher uses multiple mixed alphabets, each is a shift cipher.

- The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.
- At different points in the encryption process, the cipher uses a different alphabet from one of the rows.
- The alphabet used at each point depends on a repeating keyword.

Vigenere Cipher

Plain text: $P = P_1 P_2 P_3 \ldots$

Cipher text: $C = C_1 C_2 C_3 \ldots$

Key stream: $K = [(k_1, k_2, \ldots, k_m), (k_1, k_2, \ldots, k_m), \ldots]$

Encryption: $C_i = P_i + k_i$

Decryption: $P_i = C_i - k_i$

Example

- Input :
- Plaintext : GEEKSFORGEEKS
- Keyword : AYUSH
- Output : Ciphertext : GCYCZFMLYLEIM
- For generating key, the given keyword is repeated in a circular manner until it matches the length of the plain text.
- The keyword "AYUSH" generates the key "AYUSHAYUSHAYU"

Example

- We can encrypt the message **"She is listening"** using the 6-character keyword **"PASCAL"**. The initial key stream is **(15,0,18,2,0,11).** The key stream is the repetition of this initial key stream (as many times as needed) .

Use encryption algo: $C_i = P_i + k_i$

Plaintext:	s	h	e	i	s	l	i	s	t	e	n	i	n	g
P's values:	18	07	04	08	18	11	08	18	19	04	13	08	13	06
Key stream:	*15*	*00*	*18*	*02*	*00*	*11*	*15*	*00*	*18*	*02*	*00*	*11*	*15*	*00*
C's values:	**07**	**07**	**22**	**10**	**18**	**22**	**23**	**18**	**11**	**6**	**13**	**19**	**02**	**06**
Ciphertext:	**H**	**H**	**W**	**K**	**S**	**W**	**X**	**S**	**L**	**G**	**N**	**T**	**C**	**G**

Vigenere Table

- Another way to look at Vigenere ciphers is through what is called a Vigenere Tableau, Vigenere Table or Vigenere Square.
- The first row of this table has the 26 English letters. Shows the plain text character to be encrypted.
- Starting with the second row, each row has the letters shifted to the left one position in a cyclic way. For example, when **B** is shifted to the first position on the second row, the letter **A** moves to the end.
- The first column contains the characters to be used by the key.

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

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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Example:-

- To find the cipher text for the plaintext **“she is listening ”** using the word **“PASCAL”** as the key

  - .we can find **“s”** in the first row**, “p”** in the first column, the cross section is the cross section is the cipher text character **“H”**

  - we can find **“h”** in the first row, **“A”** in the first column, the cross section is the cross section is the cipher text character **“H”**
  - And so on…..

Encryption example:

P.T "TO BE OR NOT TO BE THAT IS THE QUESTION"

Key : RELATIONS

Use Vigenere table method to encrypt plain text to cipher text.

Plaintext: TOBEO RNOTT OBETH ATIST HEQUE STION

Keyword: RELAT IONSR ELATI ONSRE LATIO NSREL

Ciphertext:KSMEH ZBBLK SMEMP OGAJX SEJCS FLZSY

Decrypt example:

“TO BE OR NOT TO BE THAT IS THE QUESTION”

Use Vigenere table method to decrypt cipher text to plain text.

Keyword: RELAT IONSR ELATI ONSRE LATIO NSREL

Ciphertext: KSMEH ZBBLK SMEMP OGAJX SEJCS FLZSY

Plaintext: TOBEO RNOTT OBETH ATIST HEQUE STION

Vigenere Cipher (Crypanalysis)

- This method was actually discovered earlier, in 1854 by Charles Babbage.

- Vigenere-like substitution ciphers were regarded by many as practically unbreakable for 300 years.

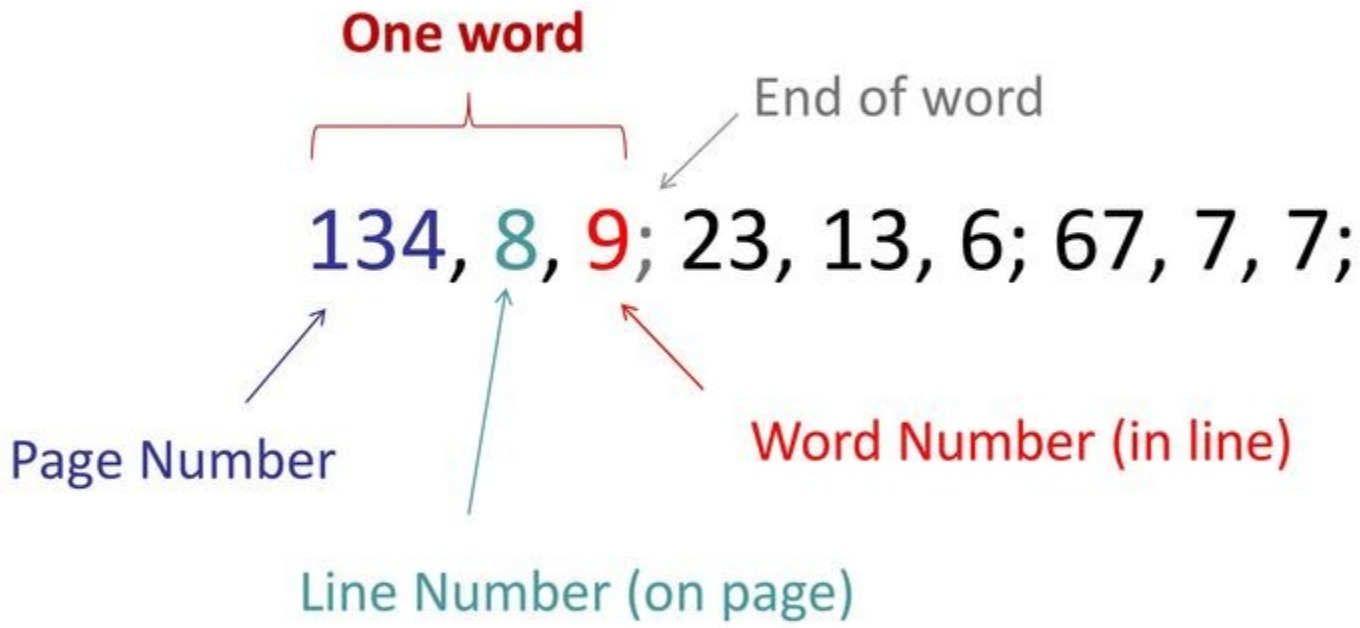
- In 1863, a Prussian major named **Kasiski** proposed a method for breaking a Vigenere cipher that consisted of finding the length of the keyword and then dividing the message into that many simple substitution cryptograms.

Book Cipher

6. Book Cipher

- This particular cipher involves the use of some key, essentially in a book.
- Both the parties should have the same book and the same edition to successfully decipher the code.
- **Locations in the book are used to replace the plain text of the message.**
- The ease of decoding depends on the how well the key has been chosen.
- Also the book should be inconspicuous and of the genre which is similar to the type of messages required to be sent.

Book Cipher


One word
End of word
134, 8, 9; 23, 13, 6; 67, 7, 7;
Page Number
Line Number (on page)
Word Number (in line)

Your turn…

166, 18, 6; 105, 28, 3; 61, 25, 5;

"Plague affected Michigan"

Book Cipher - Example

The Verse of the Rings (from Lord of the rings) as our key:

Three Rings for the Elven-kings under the sky,
Seven for the Dwarf-lords in their halls of stone,
Nine for Mortal Men doomed to die,
One for the Dark Lord on his dark throne,
In the Land of Mordor where the Shadows lie,
One ring to rule them all, one ring to find them,
One ring to bring them all and in the darkness bind them
In the Land of Mordor where the Shadows lie.

Then this book code:

6:10 8:2 4:4 3:4

would be translated as:

Row number	Word number	Word
6	10	FIND
8	2	THE
4	4	DARK
3	4	MEN

Alternatively, instead of whole words, the book cipher could use just the first letter of each word.

The example code would then translate to FTDM.

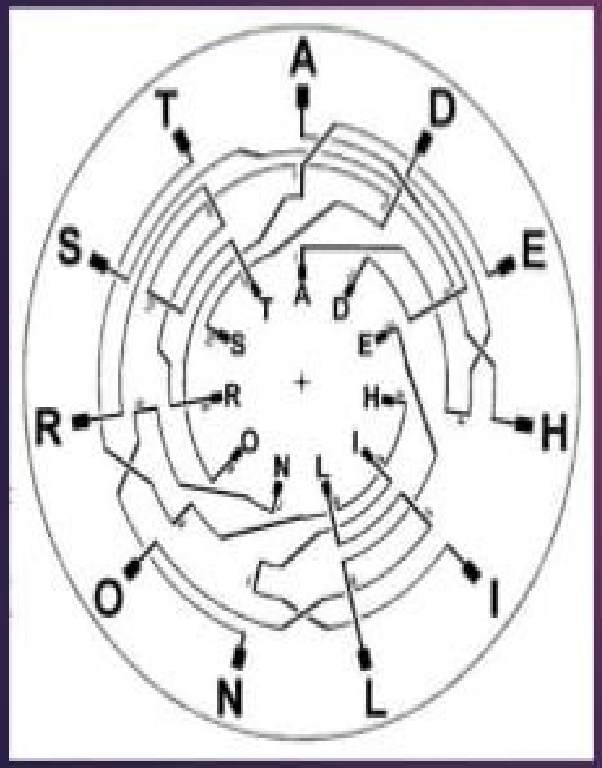
The advantage of translating letter by letter is that you can encode many more different words.

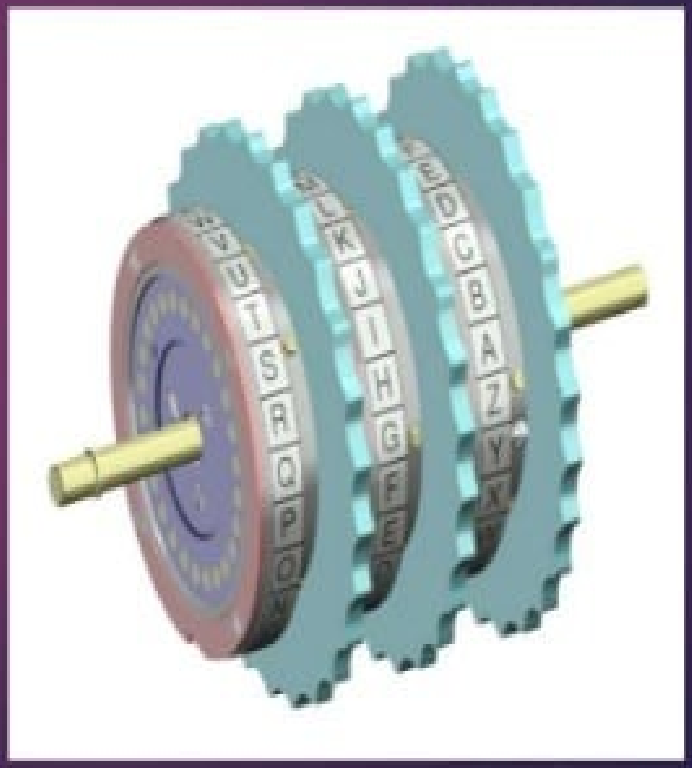
- A book cipher is an example of a homophonic substitution cipher, since the same word or letter can be encoded in different ways.
- For example, the word *THE* could have been translated into 1:4, 2:3 or any of the other places where it has been used.
- An Ottendorf cipher is a book cipher consisting of three parts. Usually in one of these formats:
  - page number - word number - letter number
  - line number - word number - letter number
- A spy operating in enemy territory would probably choose a book that would draw as little attention as possible if seen in their home.
- It is also an advantage if the book isn't too widely available, so that a cryptanalyst likely wouldn't possess it.

Rotor Cipher

- Electric rotor machines were mechanical devices that allowed to use encryption algorithms that were much more complex than ciphers, which were used manually.
- Rotor machines work by executing several monoalphabetic substitutions one after each other.
- These substitutions change with each position in the text, so we have a polyalphabetic cipher.
- The single monoalphabetic substitutions are performed by a rotor.

A Rotor





Example

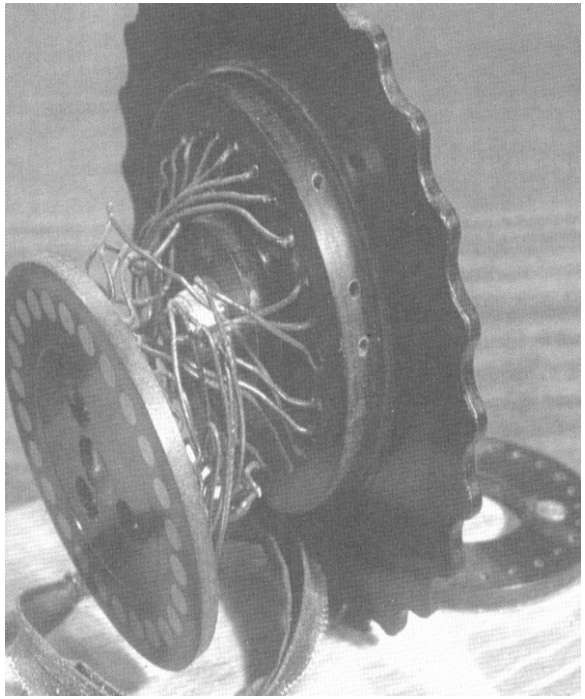
Starting Configuration Of Rotor

	A	B	C	D	E	F	G
A	0	0	1	0	0	0	0
B	0	1	0	0	0	0	0
C	0	0	0	1	0	0	0
D	0	0	0	0	1	0	0
E	1	0	0	0	0	0	0
F	0	0	0	0	0	0	1
G	0	0	0	0	0	1	0

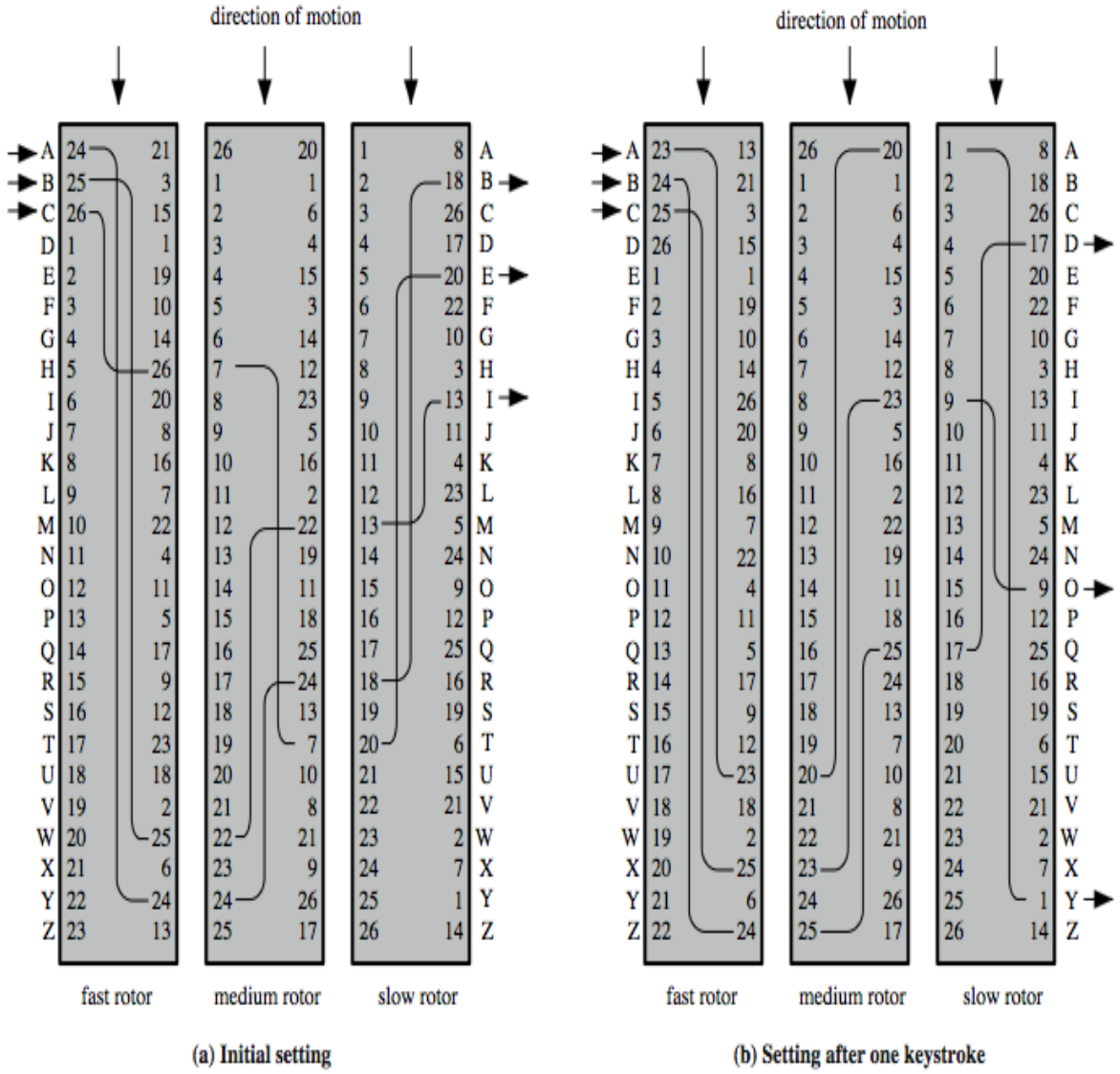
Example


A A A A A A A A A A
B B B B B B B B B B
C C C C C C C C C C
D D D D D D D D D D
E E E E E E E E E E
F F F F F F F F F F
G G G G G G G G G
Rot. 1
Rot. 2
Rot. 3
Rot. 4
Rot. 5

- A rotor is a thick disk that has near its outer circumference on both sides as many electric contacts as letters in the alphabet .
- The contacts of the two sides are pairwise connected by wires in an erratic way.
- with a single cylinder, After each input key is depressed, the cylinder rotates one position, so that the internal connections are shifted accordingly.
- Thus, a different monoalphabetic substitution cipher is defined.



Three Rotor Machine



- With multiple cylinders, the one closest to the operator input rotates one pin position with each keystroke.
- For every complete rotation of the inner cylinder, the middle cylinder rotates one pin position.
- Finally, for every complete rotation of the middle cylinder, the outer cylinder rotates one pin position.
- The result is that there are 26 * 26 * 26 = 17,576 different substitution alphabets used before the system repeats.