**ADEYEMI ADEBUNMI TESLIMAY**

**16/SCI01/003**

**CSC 418 ASSIGNMENT**

1. **Caesar Cipher** - The Caesar cipher is one of the earliest known and simplest ciphers. It is a type of substitution cipher in which each letter in the plaintext is 'shifted' a certain number of places down the alphabet. For example, with a shift of 1, A would be replaced by B, B would become C, and so on. The method is named after Julius Caesar, who apparently used it to communicate with his generals. To pass an encrypted message from one person to another, it is first necessary that both parties have the 'key' for the cipher, so that the sender may encrypt it and the receiver may decrypt it. For the Caesar cipher, the key is the number of characters to shift the cipher alphabet. E.g-

The text we will encrypt is 'defend the east wall of the castle', with a shift (key) of 1.

plaintext: defend the east wall of the castle

ciphertext: efgfoe uif fbtu xbmm pg uif dbtumf

It is easy to see how each character in the plaintext is shifted up the alphabet. Decryption is just as easy, by using an offset of -1.

plain: abcdefghijklmnopqrstuvwxyz

cipher: bcdefghijklmnopqrstuvwxyza

Obviously, if a different key is used, the cipher alphabet will be shifted a different amount.

1. **Monoalphabetic Cipher** - Monoalphabetic cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process. They work by replacing each letter of the plaintext (and sometimes punctuation marks and spaces) with another letter (or possibly even a random symbol). A monoalphabeticsubstitutioncipher, also known as a simple substitution cipher, relies on a fixed replacement structure. That is, the substitution is fixed for each letter of the alphabet.

e.g if ‘A’ is encrypted as ‘D’, for any number of occurrences in that plaintext, ‘A’ will always get encrypted to ‘D’.

1. **Playfair Cipher** - The Playfair cipher was the first practical digraph substitution cipher. The scheme was invented in 1854 by Charles Wheatstone but was named after Lord Playfair who promoted the use of the cipher. In Playfair cipher unlike traditional cipher we encrypt a pair of alphabets(digraphs) instead of a single alphabet. It was used for tactical purposes by British forces in the Second Boer War and in World War I and for the same purpose by the Australians during World War II. This was because Playfair is reasonably fast to use and requires no special equipment.

E.g

The key is "**monarchy**"

Thus the initial entires are

**'m', 'o', 'n', 'a', 'r', 'c', 'h', 'y'**

followed by remaining characters of

**a-z(except 'j')** in that order

1. **Vigenere 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.

e.g

Input : Plaintext : GEEKSFORGEEKS

Keyword : AYUSH

Output : Ciphertext : GCYCZFMLYLEIM

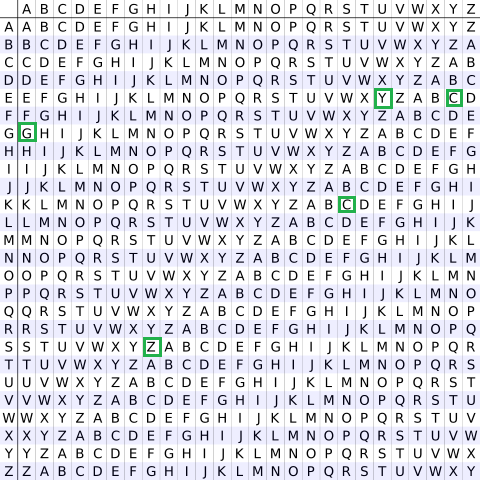
For generating key, the given keyword is repeated

in a circular manner until it matches the length of

the plain text.

The keyword "AYUSH" generates the key "AYUSHAYUSHAYU"

**Encryption**- The first letter of the plaintext, G is paired with A, the first letter of the key. So use row G and column A of the Vigenère square, namely G. Similarly, for the second letter of the plaintext, the second letter of the key is used, the letter at row E and column Y is C. The rest of the plaintext is enciphered in a similar fashion.



**Table to encrypt**

**Decryption** - is performed by going to the row in the table corresponding to the key, finding the position of the ciphertext letter in this row, and then using the column’s label as the plaintext. For example, in row A (from AYUSH), the ciphertext G appears in column G, which is the first plaintext letter. Next we go to row Y (from AYUSH), locate the ciphertext C which is found in column E, thus E is the second plaintext letter.

1. **Polyalphabetic Cipher** - A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The Vigenère cipher is probably the best-known example of a polyalphabetic cipher, though it is a simplified special case.
2. **One Time Cipher** - The One-Time Pad, or OTP is an encryption technique in which each character of the plaintext is combined with a character from a random key stream. Originally described in 1882 by banker Frank Miller (USA), it was re-invented in 1917 by Gilbert Vernam and Joseph Mauborgne. When applied correctly, the OTP provides a truely unbreakable cipher. It is named after the sheets of paper (pads) on which the key stream was usually printed. It is said that the one-time pad is the best cipher anywhere. It is uncrackable as long as you keep the messages short, use shorthand and abbreviations, remove unnecessary letters, never reuse a pad, and have a good enough random source for data.