**NAME: DABO LAURA I.**

**MATRIC NUMBER: 16/SCI01/053.**

**COURSE CODE: CSC 418.**

**COURSE TITLE: INFORMATION SYSTEMS SECURITY.**

**ASSIGNMENT TITLE: CRYPTOGRAPHY.**

**START DATE: 11-04-2020.**

**END DATE: 27-04-2020.**

**QUESTION**

Briefly discuss these cryptography methods with a given examples

1. Ceaser Cipher or Shift Cipher.
2. Monoalphabetic cipher or Simple cipher.
3. Playfair cipher.
4. Vigenere cipher.
5. Polyalphabetic cipher.
6. One time cipher.

**ANSWERS**

1. **Ceaser Cipher or Shift Cipher:**

In cryptography, a Caesar cipher, also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption techniques.

It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions between 0 and 25 down the alphabet. For example, with a left shift of 3, transforms A to D, B to E, and so on until W to Z, X to A, Y to B, and Z to C. The method is named after Julius Caesar, who used it in his private correspondence to communicate with his officials.

It is a mono-alphabetic cipher wherein each letter of the plaintext is substituted by another letter to form the ciphertext. It is a simplest form of substitution cipher scheme and this cryptosystem is generally referred to as the Shift Cipher especially when ‘shift of three’ is used.

For this type of scheme, both sender and receiver agree on a ‘secret shift number’ for shifting the alphabet. The process of Shift cipher involoves the following steps;

1. In order to encrypt a plaintext letter, the sender positions the sliding ruler underneath the first set of plaintext letters and slides it to LEFT by the number of positions of the secret shift.
2. The plaintext letter is then encrypted to the ciphertext letter on the sliding ruler underneath. The result of this process is depicted in the following illustration for an agreed shift of three positions. In this case, the plaintext ‘laura’ is encrypted to the ciphertext ‘ODXUD’. Here is the ciphertext alphabet for a shift of 3 –

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Plaintext Alphabet | 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 |
| Ciphertext Alphabet | 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 |

1. On receiving the ciphertext, the receiver who also knows the secret shift, positions his sliding ruler underneath the ciphertext alphabet and slides it to RIGHT by the agreed shift number, 3 in this case.
2. He then replaces the ciphertext letter by the plaintext letter on the sliding ruler underneath. Hence the ciphertext ‘ODXUD’ is decrypted to ‘tutorial’. To decrypt a message encoded with a Shift of 3, generate the plaintext alphabet using a shift of ‘-3’ as shown below –

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ciphertext Alphabet | 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 |
| Plaintext Alphabet | 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 |

Security Value

Caesar Cipher is not a secure cryptosystem because there are only 26 possible keys to try out. An attacker can carry out an exhaustive key search with available limited computing resources.

Examples:

1. Using the table above:

Text: abuad we come

Ciphertext: DEXDG ZH FRPH

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Plaintext Alphabet | 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 |
| Ciphertext Alphabet | 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 |

Shift: 5

Plaintext: CRYPTOGRAPHY

Ciphertext: HWDUYTLWFUMD

1. **Monoalphabetic cipher or Simple cipher:**

Monoalphabetic cipher, also known as a simple substitution cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process. It relies on a fixed replacement structure. That is, the substitution is fixed for each letter of the alphabet. Thus, if ‘A’ is encrypted as ‘D’, for any number of occurrence in that plaintext, ‘A’ will always get encrypted to ‘D’.

A simple example is where each letter is encrypted as the next letter in the alphabet: "AFE BABALOLA UNIVERSITY" becomes "DIH EDEDOROD XQLYHUVLWB". In general, when performing a simple substitution manually, it is easiest to generate the ciphertext alphabet first, and encrypt by comparing this to the plaintext alphabet. The table below shows how one might choose to, and we will, lay them out for this example.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |

The ciphertext alphabet for the cipher where you replace each letter by the next letter in the alphabet.

There are many different monoalphabetic substitution ciphers, in fact infinitely many, as each letter can be encrypted to any symbol, not just another letter. With so many substitutions, monoalphabetic substitution might appear as a very strong cipher technique but, in reality, it is a very weak cipher. Cryptanalysis of a message enciphered using a monoalphabetic substitution takes into consideration that each plain letter is always transformed into the same encipher equivalent, and that in any language there are some letters that occur more often than others.

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. The technique encrypts pairs of letters (digraphs), instead of single letters as in the case of simple substitution cipher. The Playfair is significantly harder to break since the frequency analysis used for simple substitution ciphers does not work with it.

The Playfair cipher encryption algorithm consists of two (2) following steps –

1. Generate the key Square:

In playfair cipher, initially a key table is created. The key table is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table as we need only 25 alphabets instead of 26. If the plaintext contains J, then it is replaced by I.

For example;

The sender and the receiver deicide on a particular key, say ‘tutorials’. In a key table, the first characters (going left to right) in the table is the phrase, excluding the duplicate letters. The rest of the table will be filled with the remaining letters of the alphabet, in natural order. The key table works out to be −

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

1. Algorithm to encrypt the plain text: First, a plaintext message is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter. Let us say we want to encrypt the message “hide money”. It will be written as −

Plaintext: "hide money"

After split: HI DE MO NE YZ

The rules of encryption are –

1. If both the letters are in the same column, take the letter below each one (going back to the top if at the bottom).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| T | U | O | R | I | ‘H’ and ‘I’ are in same column, hence take letter below them to replace. HI → QC |
| A | L | S | B | C |
| D | E | F | G | H |
| K | M | N | P | Q |
| V | W | X | Y | Z |

1. If both letters are in the same row, take the letter to the right of each one (going back to the left if at the farthest right)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| T | U | O | R | I | ‘D’ and ‘E’ are in same row, hence take letter to the right of them to replace. DE → EF |
| A | L | S | B | C |
| D | E | F | G | H |
| K | M | N | P | Q |
| V | W | X | Y | Z |

1. If neither of the preceding two rules are true, form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| T | U | O | R | I | ‘M’ and ‘O’ nor on same column or same row, hence form rectangle as shown, and replace letter by picking up opposite corner letter on same row MO → NU |
| A | L | S | B | C |
| D | E | F | G | H |
| K | M | N | P | Q |
| V | W | X | Y | Z |

Using these rules, the result of the encryption of ‘hide money’ with the key of ‘tutorials’ would be –

Plaintext: "hide money"

After split: HI DE MO NE YZ

Ciphertext: QC EF NU MF ZV

Note: Decrypting the Playfair cipher is as simple as doing the same process in reverse. Receiver has the same key and can create the same key table, and then decrypt any messages made using that key.

Another example, consider the following

Key: ‘abuad’

Plaintext: "dabo"

After split: DA BO

Table:

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| A | B | U | D | C | ‘D’ and ‘A’ are in same column, hence take letter below them to replace. DA → CB |
| E | F | G | H | I |
| K | L | M | N | O |
| P | Q | R | S | T |
| V | W | X | Y | Z |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| A | B | U | D | C | ‘B’ and ‘O’ are in same row, hence take letter to the right of them to replace. BO → CL |
| E | F | G | H | I |
| K | L | M | N | O |
| P | Q | R | S | T |
| V | W | X | Y | Z |

Ciphertext: CB CL

Security Value

It is also a substitution cipher and is difficult to break compared to the simple substitution cipher. As in case of substitution cipher, cryptanalysis is possible on the Playfair cipher as well, however it would be against 625 possible pairs of letters (25x25 alphabets) instead of 26 different possible alphabets.

The Playfair cipher was used mainly to protect important, yet non-critical secrets, as it is quick to use and requires no special equipment.

1. **Vigenere cipher:**

The Vigenere cipher is a method of encryption alphabetic text invented by Giovan Batista Belaso and described in his 1553 book, “La cifra del. Sig. Giovan Batista Belaso”. It was misattributed to Blaise de Vigenere in the 19th century, and given his name. The cipher is a keyword-based system that includes a twist with Caesar cipher algorithm used for encryption and decryption. Vignere cipher works similar to Caesar Cipher algorithm with only one major distinction: Caesar cipher includes algorithm for one-character shift, whereas Vignere Cipher includes key with multiple alphabets shift.

Vigenere cipher which is a simple form of polyalphabetic substitution that uses a text string (say, a word) as a key, which is then used for doing a number of shifts on the plaintext. 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 |

For example,

Plaintext: GEEKSFORGEEKS

Key: AYUSH

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"

The plain text is then encrypted using the process explained below.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 |

Ciphertext: GCYCZFMLYLEIM

Another example, let’s assume the key is ‘point’. Each alphabet of the key is converted to its respective numeric value: In this case,

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| p | o | i | n | t |
| 16 | 15 | 9 | 14 | 20 |

Thus, the key is: 16 15 9 14 20.

The process of Vigenere cipher involves;

1. The sender and the receiver decide on a key. Say ‘point’ is the key. Numeric representation of this key is ‘16 15 9 14 20’.
2. The sender wants to encrypt the message, say ‘attack from south east’. He will arrange plaintext and numeric key as follows –

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| a | t | t | a | c | k | f | r | o | m | s | o | u | t | h | e | a | s | t |
| 16 | 15 | 9 | 14 | 20 | 16 | 15 | 9 | 14 | 20 | 16 | 15 | 9 | 14 | 20 | 16 | 15 | 9 | 14 |

1. He now shifts each plaintext alphabet by the number written below it to create ciphertext as shown below –

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| a | t | t | a | c | k | f | r | o | m | s | o | u | t | h | e | a | s | t |
| 16 | 15 | 9 | 14 | 20 | 16 | 15 | 9 | 14 | 20 | 16 | 15 | 9 | 14 | 20 | 16 | 15 | 9 | 14 |
| Q | I | C | O | W | A | U | A | C | G | I | D | D | H | B | U | P | B | H |

1. Here, each plaintext character has been shifted by a different amount – and that amount is determined by the key. The key must be less than or equal to the size of the message.
2. For decryption, the receiver uses the same key and shifts received ciphertext in reverse order to obtain the plaintext.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Q | I | C | O | W | A | U | A | C | G | I | D | D | H | B | U | P | B | H |
| 16 | 15 | 9 | 14 | 20 | 16 | 15 | 9 | 14 | 20 | 16 | 15 | 9 | 14 | 20 | 16 | 15 | 9 | 14 |
| a | t | t | a | c | k | F | r | o | m | s | o | u | t | h | e | a | s | t |

Security Value

Vigenere cipher was designed by tweaking the standard Caesar cipher to reduce the effectiveness of cryptanalysis on the ciphertext and make a cryptosystem more robust. It is significantly more secure than a regular Caesar Cipher.

In the history, it was regularly used for protecting sensitive political and military information. It was referred to as the unbreakable cipher due to the difficulty it posed to the cryptanalysis.

Variants of Vigenere Cipher

There are two special cases of Vigenere cipher −

* The keyword length is same as plaintect message. This case is called Vernam Cipher. It is more secure than typical Vigenere cipher.
* Vigenere cipher becomes a cryptosystem with perfect secrecy, which is called One-time pad.

1. **Polyalphbetic cipher:**

Polyalphabetic cipher is a substitution cipher in which the cipher alphabet for the plain alphabet may be different at different places during the encryption process. It is any cipher based on substitution, using multiple substitution alphabets.

To facilitate encryption, all the alphabets are usually written out in a large table, traditionally called a tableau. Usually the tableau is , so that 26 full ciphertext alphabets are available. The method of filling the tableau, and of choosing which alphabet to use next, defines the particular polyalphabetic cipher. All such ciphers are easier to break than were believed since the substitution alphabets are repeated for sufficiently large plaintexts. One of the most popular was that of Vigenere cipher.

A simple substitution cipher involves a single mapping of the plaintext alphabet onto ciphertext characters. A more complex alternative is to use different substitution mappings (called multiple alphabets) on various portions of the plaintext. This results in so-called polyalphabetic substitution. In the simplest case, the different alphabets are used sequentially and then repeated, so the position of each plaintext character in the source string determines which mapping is applied to it. Under different alphabets, the same plaintext character is thus encrypted to different ciphertext characters, precluding simple frequency analysis as per monoalphabetic substitution. The simple Vigenere cipher is a polyalphabetic substitution cipher. The definition is repeated here for convenience. The advantage of Polyalphabetic ciphers is that they make frequency analysis more difficult. Frequency analysis is the practice of decrypting a message by counting the frequency of ciphertext letters, and equating it to the letter frequency of normal text. For instance if P occurred most in a ciphertext whose plaintext is in English, one could suspect that P corresponded to E, because E is the most frequently used letter in English. Using the Vigenere cipher, E can be enciphered as any of several letters in the alphabet in the Vigenere cipher, thus defeating simple frequency analysis.

Examples of polyalphabetic substitution ciphers are Playfair cipher, Autokey cipher, Engima cipher, Porta cipher, Vigenere and Gronsfeld cipher.

1. **One Time cipher:**

One-time pad cipher is a type of Vignere cipher which includes the following features

1. It is an unbreakable cipher.
2. The key is exactly same as the length of message which is encrypted.
3. The key is made up of random symbols.
4. 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.

The key is unbreakable owing to the following features −

The key is as long as the given message.

The key is truly random and specially auto-generated.

Key and plain text calculated as modulo 10/26/2.

Each key should be used once and destroyed by both sender and receiver.

Encryption

To encrypt a letter, a user needs to write a key underneath the plaintext. The plaintext letter is placed on the top and the key letter on the left. The cross section achieved between two letters is the plain text. It is described in the example below –

Plaintext: THIS IS SECRET

OTP-Key: XVHE UW NOPGDZ

Ciphertext: QCPW CO FSRXHS

In groups: QCPWC OFSRX HS

Decryption

To decrypt a letter, user takes the key letter on the left and finds cipher text letter in that row. The plain text letter is placed at the top of the column where the user can find the cipher text letter.

The difference between one-time pad cipher and shift cipher is that it is impossible to break. Let us say, we encrypt the name “point” with a one-time pad. It is a 5 letter text. To break the ciphertext by brute force, you need to try all possibilities of keys and conduct computation for (26 x 26 x 26 x 26 x 26) = 265 = 11881376 times. That’s for a message with 5 alphabets. Thus, for a longer message, the computation grows exponentially with every additional alphabet. This makes it computationally impossible to break the ciphertext by brute force.

In case of Shift cipher, the entire message could have had a shift between 1 and 25. This is a very small size, and very easy to brute force. However, with each character now having its own individual shift between 1 and 26, the possible keys grow exponentially for the message.