# Implementation of Vernam Cipher or One Time Pad Algorithm

One Time Pad algorithm is the improvement of the [Vernam Cipher](https://www.geeksforgeeks.org/vernam-cipher-in-cryptography/), proposed by An Army Signal Corp officer, Joseph Mauborgne. It is the only available algorithm that is unbreakable(completely secure). It is a method of encrypting alphabetic plain text. It is one of the Substitution techniques which converts plain text into ciphertext. In this mechanism, we assign a number to each character of the Plain-Text.

The two requirements for the One-Time pad are

* 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.

The ciphertext generated by the One-Time pad is random, so it does not have any statistical relation with the plain text.

The assignmentis as follows:

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

**The relation between the key and plain text:** In this algorithm, the length of the key should be equal to that of plain text.

**Examples:**

***Input:*** *Message = HELLO, Key = MONEY* ***Output:*** *Cipher - TSYPM, Message - HELLO* ***Explanation:*** *Part 1: Plain text to Ciphertext         Plain text — H E L L O ? 7 4 11 11 14         Key — M O N E Y ? 12 14 13 4 24         Plain text + key ? 19 18 24 15 38 ? 19 18 24 15 12 (= 38 – 26)* ***Cipher Text ? T S Y P M*** *Part 2: Ciphertext to Message         Cipher Text — T S Y P M ? 19 18 24 15 12         Key — M O N E Y? 12 14 13 4 24         Cipher text - key ? 7 4 11 11 -12 ? 7 4 11 11 14* ***Message ? H E L L O******Input:*** *Message = SAVE, Key = LIFE* ***Output:*** *Cipher - DIAI Message - SAVE*

**Security of One-Time Pad**

* If any way cryptanalyst finds these two keys using which two plaintext are produced but if the key was produced randomly, then the cryptanalyst cannot find which key is more likely than the other. In fact, for any plaintext as the size of ciphertext, a key exists that produces that plaintext.
* So if a cryptanalyst tries the brute force attack(try using all possible keys), he would end up with many legitimate plaintexts, with no way of knowing which plaintext is legitimate. Therefore, the code is unbreakable.
* The security of the one-time pad entirely depends on the randomness of the key. If the characters of the key are truly random, then the characters of the ciphertext will be truly random. Thus, there are no patterns or regularities that a cryptanalyst can use to attack the ciphertext.

**Advantages**

* 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).

**Disadvantages**

* There is the practical problem of making large quantities of random keys. Any heavily used system might require millions of random characters on a regular basis.
* For every message to be sent, a key of equal length is needed by both sender and receiver. Thus, a mammoth key distribution problem exists.