## **Vigenère Ciphering**:

This cipher was invented in 1586 by Blaise de Vigenère with a reciprocal table of ten alphabets. Vigenère's version used an agreed-upon letter of the alphabet as a primer, making the key by writing down that letter and then the rest of the message. The Vigenère Cipher was adapted as a twist on the standard Caesar cipher to reduce the effectiveness of performing frequency analysis on the ciphertext. The cipher accomplishes this using **a text string (for example, a word) as a key, which is then used for doing a number of alphabet shifts on the plaintext**.

Vigenere cipher algorithm: E = M+K mod 26 

Expressed mathematically, the encryption of the message at letter \*i\*, is equal to the alphabetic value of \*i\* in the plaintext plus the alphabetic value of the corresponding \*i\* in the key.

Decryption is the same process reversed, subtracting the key instead of adding to arrive back at the original, plaintext value.

Vigenere decipher algorithm: D = C - K mod 26

More popular autokeys use a tabula recta, a square with 26 copies of the alphabet, the first line starting with 'A', the next line starting with 'B' etc. Instead of a single letter, a short agreed-on keyword is used, and the key is generated by writing down the primer and then the rest of the message, as in Vigenère's version. To encrypt a plaintext, the row with the first letter of the message and the column with the first letter of the key are located. The letter in which the row and the column cross is the ciphertext letter.

An **autokey cipher (also known as the autoclave cipher**) is a cipher that **incorporates the message (the plaintext) into the key**. The key is generated from the message in some automated fashion, sometimes by selecting certain letters from the text or, more commonly, by adding a short primer key to the front of the message.

There are two forms of autokey cipher: key-autokey and text-autokey ciphers. A key-autokey cipher uses previous members of the keystream to determine the next element in the keystream. A text-autokey uses the previous message text to determine the next element in the keystream.

In modern cryptography, self-synchronizing stream ciphers are autokey ciphers.

**To encrypt a letter, we write the key underneath the plaintext. We take the plaintext letter at the top and the key letter on the left. The cross section of those two letters is the ciphertext. In the first letter of our example below, the crossing between the plaintext T and key X is ciphertext Q.**

**Example:**

**Plaintext: T H I S I S S E C R E T**

**OTP-Key : X V H E U W N O P G D Z**

**Ciphertext: Q C P W C O F S R X H S**

