**Encryption**

The process of converting information or data into a code, especially to prevent unauthorized access.

Encryption is a process by which a message (called plaintext) is transformed into another message (called ciphertext) using a mathematical function and a special encryption password , called the key.

**Decryption**

It is the reverse process, from ciphertext to plaintext.

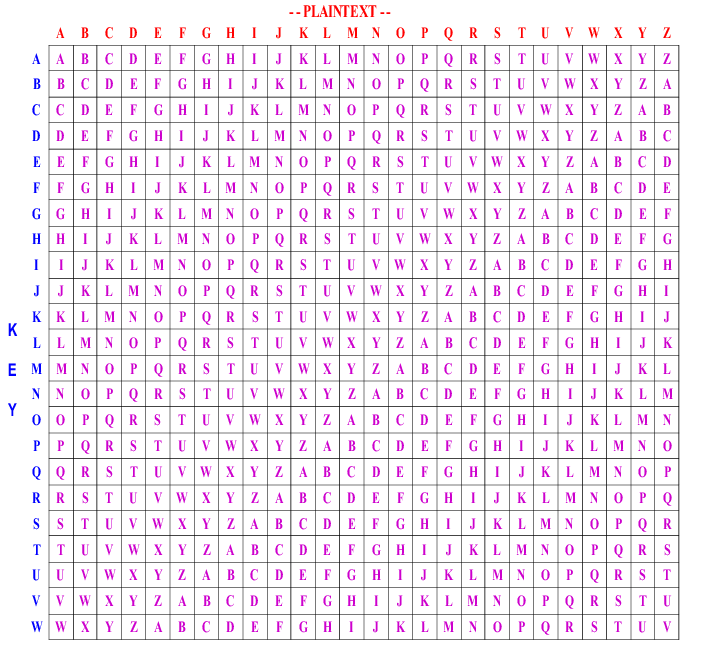
**Ceasar Cipher**

Is one of the earliest known and simplest cipher

works on letters from 1 – 26

Shifts left 1 letter.

**Vigenère cipher**



|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Encrypted message | I | L | E | E | W | K | C | G | S |
| key | p | e | a | r | s | o | n | p | e |
| Plain text | **T** | **H** | **E** | **N** | **E** | **W** | **P** | **R** | **O** |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Encrypted message | C | V | K | G | V | H | Z | E | I |
| key | a | r | s | o | n | p | e | a | r |
| Plain text | **C** | **E** | **S** | **S** | **I** | **S** | **V** | **E** | **R** |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Encrypted message | Q | S | S | U | M | C | Z | W | B |
| key | s | o | n | p | e | a | r | s | o |
| Plain text | **Y** | **E** | **F** | **F** | **I** | **C** | **I** | **E** | **N** |

|  |  |
| --- | --- |
| Encrypted message | G |
| key | N |
| Plain text | **T** |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Encrypted message | I | L | E | E | W | K | C | G | S |
| key | p | e | a | r | s | o | n | p | e |
| Plain text | **T** | **H** | **E** | **N** | **E** | **W** | **P** | **R** | **O** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Encrypted message | C | V | K | G | V | H |
| key | a | r | s | o | n | p |
| Plain text | **C** | **E** | **S** | **S** | **I** | **S** |

**Reasons why a Vigenère cipher is more secure than a Caesar cipher?**

1. Multi alphabetical
2. Each letter of the message shifts by a different amount
3. Generates a greater number of permutations for each letter
4. More resistant to frequency analysis
5. Repeated letters are disguised
6. More resistant to Bruce force attack