Encryption

**Encryption** is the process of scrambling a message so that it cannot be understood without *decrypting* it, which requires knowing the method and the key used.

**Decryption** is the reverse – it takes the cipher text and key, and produces the original message.

# The Caesar Cipher

Named after Julius Caesar, this encryption method shifts all letters a certain number of places.

*Caesar shift of 14:*

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

*“HELLO WORLD” 🡪 “QYAAR FRMAC”*

A keyword can be used with a Caesar Cipher – all the keyword’s letters are used to start the alphabet (ignoring duplicates), and the remaining letters are filled in.

*Caesar cipher with “BEESWAX” as a keyword:*

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

*“HELLO WORLD” 🡪 “DAIIL ULOIW”*

# Frequency Analysis

The Caesar Cipher is very easy to crack, as certain letters (such as “e”) and certain combinations (like “ll”) are used more frequently than others

# Transposition Cipher

The letters of the message are re-arranged to form an anagram – a common method is the **railfence method**, which splits the method across multiple lines. The number of lines used is the *key*.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| B |  | O |  | D |  | W |  | R |  | C |  | L |  | I |  | G |
|  | R |  | A |  | S |  | O |  | D |  | A |  | L |  | N |  |

*“BROADSWORDCALLING” 🡪 “BODWRCLIGRASODALN”*

# Vernam Cipher

A key of equal length of the message is chosen, both the key and message are converted to binary. The cipher text is given by the XOR of the key and message.

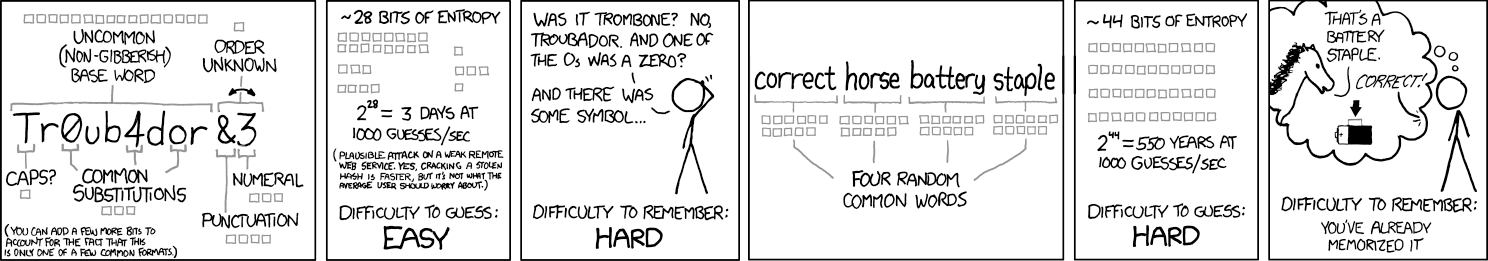
*Message: “HELLOWORLD”, Key: “APPLESUCKS”*

|  |  |
| --- | --- |
| Message2: | 01000 00101 01100 01100 01111 10111 01111 10010 01100 00100 |
| Key2: | 00001 10000 10000 01100 00101 10011 10101 00011 01011 10011 |
| XOR: | 01001 10101 11100 00000 01010 00100 11010 10001 00111 10111 |

# Computational Security

The Vernam Cipher is the only cipher considered to be 100% mathematically secure.

A cipher is **computationally secure** if it is *theoretically* breakable, but not in a practical timeframe – therefore being able to withstand most threats.



“Through 20 years of effort, we’ve successfully trained everyone to use passwords that are hard for humans to remember, but easy for computers to guess”