# SEBUCSERT CRYPTOSYSTEM

## Overview

The SEBUCSERT CRYPTOSYSTEM provides security for messages through the power of cubes. It does not require any complex computations or mathematics, making it ideal for use by field operatives. Thanks to the size of the key space (just over 93 bits of security), it is considered suitable for protecting flags which must be kept secret for the duration of the CTF.

## The Key:

To exchange messages, parties must have pre-shared a 3x3x3 cube comprised of the letters of the alphabet, and underscore ('_'). Make sure the orientation of the cube is well-established with both parties.

## Preparation:

To prepare a message for encryption, convert it to uppercase, and replace all spaces (' ') with underscores ('_').

## Encryption:

Encryption is performed line by line. First, convert each character ($P_i$) that appears in the cube into its cube-coordinates ($X_i$,$Y_i$,$Z_i$).

| $P_0$ | $P_1$ | $P_2$ | $P_3$ | $P_4$ | $P_5$ | ... | $P_n$ |
|---|---|---|---|---|---|---|---|
| $X_0$ | $X_1$ | $X_2$ | $X_3$ | $X_4$ | $X_5$ | ... | $X_n$ |
| $Y_0$ | $Y_1$ | $Y_2$ | $Y_3$ | $Y_4$ | $Y_5$ | ... | $Y_n$ |
| $Z_0$ | $Z_1$ | $Z_2$ | $Z_3$ | $Z_4$ | $Z_5$ | ... | $Z_n$ |

Then, each such character passes its Y-coordinate one character forward, and Z-coordinate two characters forward. Coordinates passed off the end wrap to the beginning.

| $C_0$ | $C_1$ | $C_2$ | $C_3$ | $C_4$ | $C_5$ | ... | $C_n$ |
|---|---|---|---|---|---|---|---|
| $X_0$ | $X_1$ | $X_2$ | $X_3$ | $X_4$ | $X_5$ | ... | $X_n$ |
| $Y_n$ | $Y_0$ | $Y_1$ | $Y_2$ | $Y_3$ | $Y_4$ | ... | $Y_{n-1}$ |
| $Z_{n-1}$ | $Z_n$ | $Z_0$ | $Z_1$ | $Z_2$ | $Z_3$ | ... | $Z_{n-2}$ |

After passing coordinates, use the new coordinates to find the encrypted character from the cube.

Note: Non-cube characters are removed from the plaintext before enciphering, with the exception of '{' and '}' from the flag.

## Decryption:

To decrypt a message, follow the same process for encryption, except negate the shifts for Y and Z. **Note the flag should be converted to all lowercase for submission.**

# Test Vectors

## Vector 1

| | Z=0 | | | Z=1 | | | Z=2 | | |
|---|---|---|---|---|---|---|---|---|---|
| | X=0 | X=1 | X=2 | X=0 | X=1 | X=2 | X=0 | X=1 | X=2 |
| Y=0 | A | J | R | B | K | S | C | L | T |
| Y=1 | D | M | U | E | _ | V | F | N | W |
| Y=2 | G | O | X | H | P | Y | I | Q | Z |

Plain: “Please help. I am trapped in a crypto factory and the only way I can communicate is by test vectors.”

Cipher:“JPBFSA_EH_KQEPFKMUSCJOHE_DPNFKDSTOYKQDECRLZROEKDNUBI__PMTQVETOEPFBLMFKQMUMDICTANEYLESPVBWSKWEESLZR”

## Vector 2

| | Z=0 | | | Z=1 | | | Z=2 | | |
|---|---|---|---|---|---|---|---|---|---|
| | X=0 | X=1 | X=2 | X=0 | X=1 | X=2 | X=0 | X=1 | X=2 |
| Y=0 | T | H | C | P | A | W | I | V | K |
| Y=1 | U | Z | Q | J | M | B | R | E | D |
| Y=2 | S | G | X | Y | _ | N | L | F | O |

Plain: “Believe in yourself and you can achieve anything!”

Cipher:“NZJLVEVELWFYNYRUFUFFFWNMLNYEXAC__WATHEVEFWYYATCF”

## Vector 3

| | Z=0 | | | Z=1 | | | Z=2 | | |
|---|---|---|---|---|---|---|---|---|---|
| | X=0 | X=1 | X=2 | X=0 | X=1 | X=2 | X=0 | X=1 | X=2 |
| Y=0 | T | D | B | O | J | Q | G | U | M |
| Y=1 | P | F | E | A | X | S | C | Y | R |
| Y=2 | _ | K | H | N | V | W | L | Z | I |

Plain: “I figure three test vectors is enough. You'll probably want to test your decryption function too, so run these through backwards :)”

Cipher:“W_ZE_UMRC_BHERP_BEPOKHAPGBSCWHCWP_JOMLKPUOLLLEPMOEOKCI_ANO_TTNBEPOKPUQCZBPEYCCB_GNVFTLAM_GNNTTOWPOWFGLNBHEEA_BHPUOMLHTPXI_SXMP”