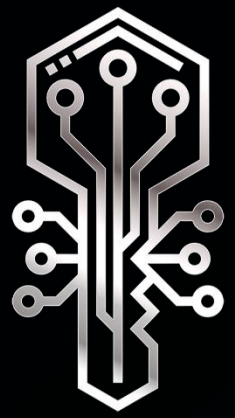
ST. VINCENT PALLOTTI COLLEGE OF ENGINEERING & TECHNOLOGY

ARISE & SHINE

TECHNEX-22

PRESENTS



ENCIPHERX

WHAT IS ENCIPHERX JR.?

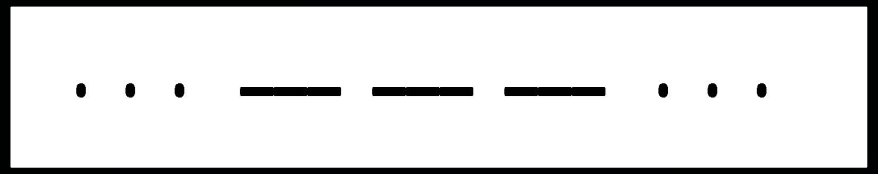
- Team EncipherX is working on making the youth of India skilled in the area of cybersecurity.
- Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks and knowledge in this area can reduce the chances of your data being stolen and misused.
- EnchipherX Jr. aims to help the participants in improving their skills and expanding their knowledge in cryptography and steganography

CRYPTOGRAPHY

- Cryptography is technique for secure communication in the presence of adversarial behaviour. More generally, cryptography is about constructing and analysing protocols that prevent third parties or the public from reading private messages or information.
- Cryptography can be used to secure communications by encrypting them. Websites use encryption via HTTPS.
- Operating systems use encryption to keep passwords secret, conceal parts of the system, and ensure the authenticity of software updates.

MORSE CODE

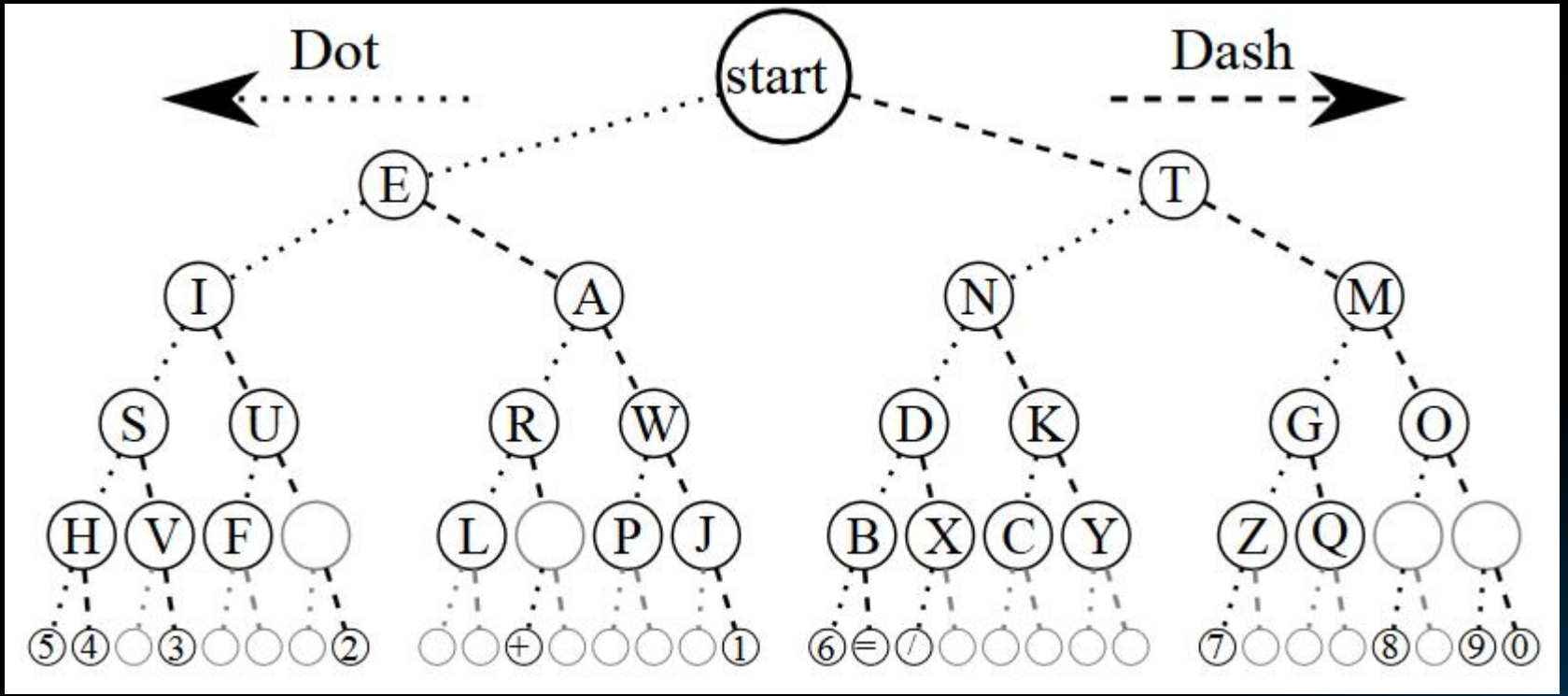
- Morse code is a method used in telecommunication to encode text characters as standardized sequences of two different signal durations, called dots and dashes.
- Named after the inventor of telegraph.
- Morse code can be sent in a form sound waves or visible light, such that it can be directly interpreted by persons.



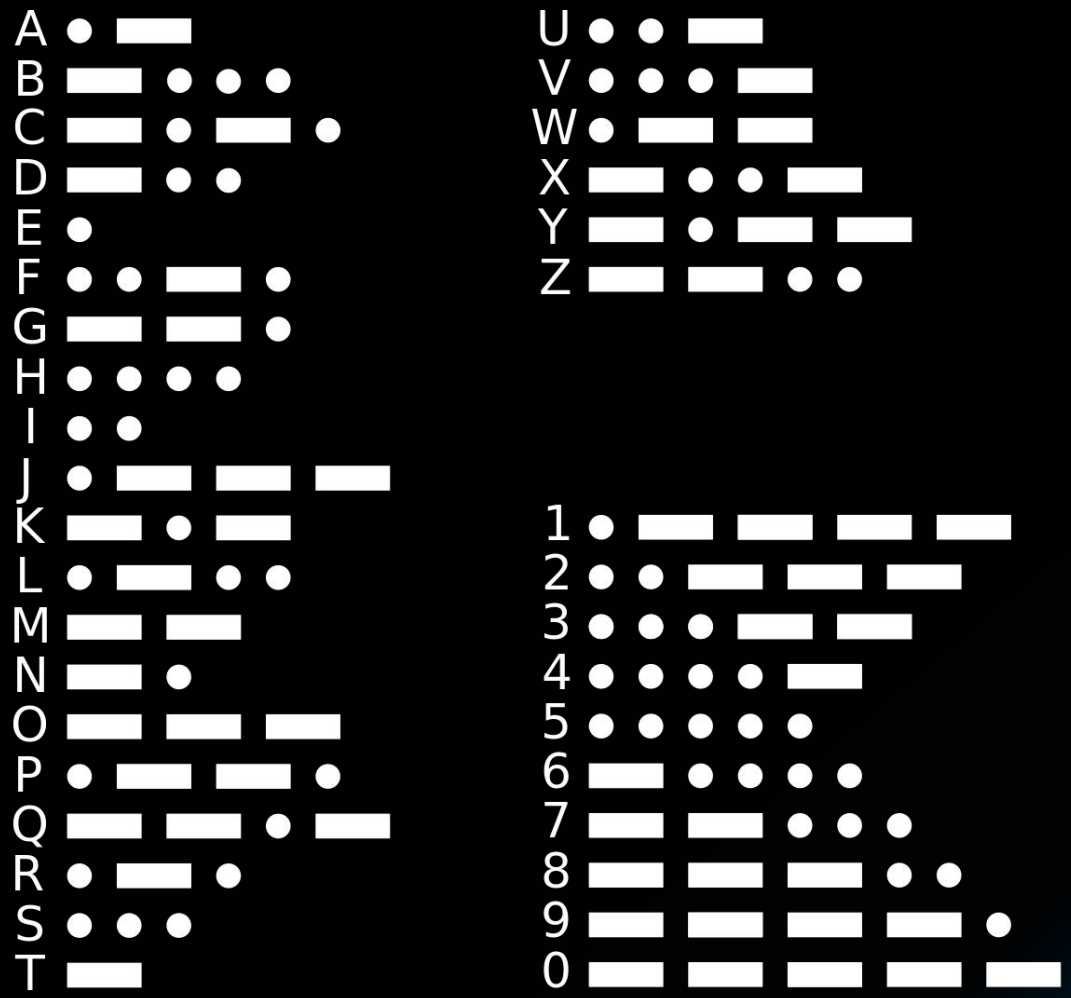
- $\overline{\text{SOS}}$ is an example of Morse code.

International Morse Code

1. The length of a dot is one unit.
2. A dash is three units.
3. The space between parts of the same letter is one unit.
4. The space between letters is three units.
5. The space between words is seven units.



International Morse Code:



CAESAR CIPHER

- Caesar’s cipher/shift, is one of the simplest and most widely known substitution cipher.
- The method is named after Julius Caesar, who used it in his private correspondence.
- Letters are shifted according to the shift/key, and then substituted to create the ciphertext.
- It can be stacked by shifting the ciphertext again using another key.

Key = 3
i.e. Shift of 3 to the right

For Decryption:
Shift normal letters by 3 to the right
OR
By 26-3 to the left

Ciphertext: ZOVMQLDOXMEVFPCRK

Plaintext: CRYPTOGRAPHYISFUN

In case of Multiple shifts:

Ciphertext: UJQHLGYJSHZQAKXMF

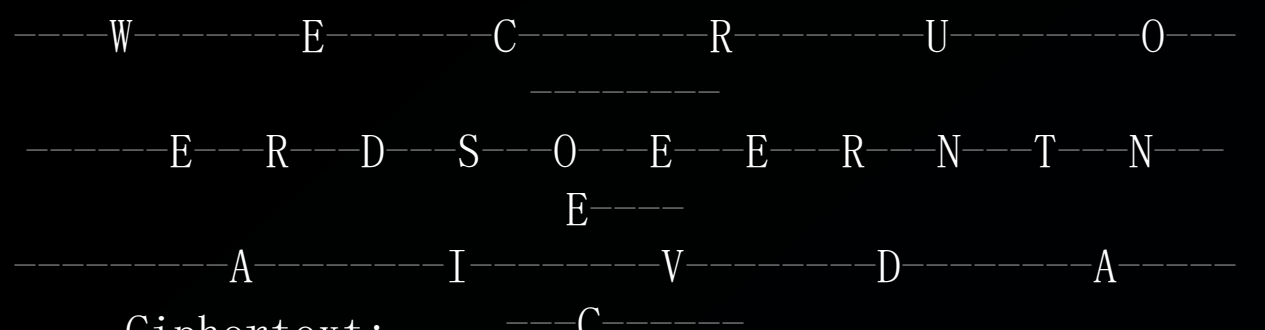
Ciphertext: ZOVMQLDOXMEVFPCRK

Plaintext: CRYPTOGRAPHYISFUN

RAIL FENCE CIPHER

- Rail fence/zigzag cipher is a form of classical transposition cipher.
- It derives its name from the manner in which encryption is performed.
- In the rail fence cipher, the plaintext is written downwards diagonally on successive "rails" of an imaginary fence, then moving up when the bottom rail is reached, down again when the top rail is reached, and so on until the whole plaintext is written out.
- The ciphertext is then read off in rows.

WE ARE DISCOVERED RUN AT ONCE



Ciphertext:

WECRUO ERDSOEERNTNE AIVDAC

Ciphertext:

WVUTRO EAEAGTHTATR HCHEI

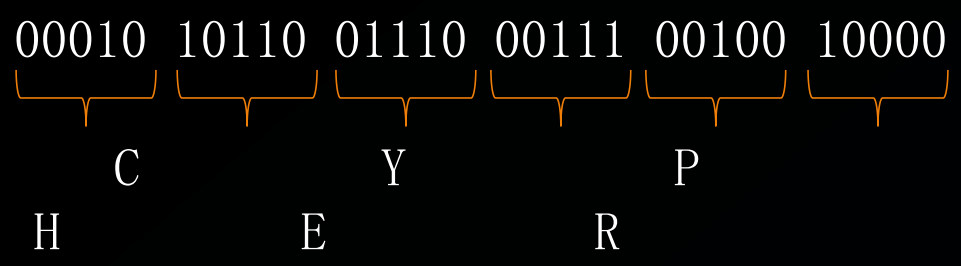
WE HAVE CAUGHT THE TRAITOR

BACON CIPHER

- Bacon's cipher or the Baconian cipher is a method of message encoding devised by Francis Bacon in 1605.
- The plaintext is replaced by a 5-bit binary equivalent of each letter according to the cipher.
- The ciphertext is either in the form of 0's and1's or a's and b's. These 5-bit binary sequences can also be inverted.

Letter	Code	Binary
A	aaaaa	00000
B	aaaab	00001
C	aaaba	00010
D	aaabb	00011
E	aabaa	00100
F	aabab	00101
G	aabba	00110
H	aabbb	00111
I, J	abaaa	01000
K	abaab	01001
L	ababa	01010
M	ababb	01011

Letter	Code	Binary
N	abbaa	01100
O	abbab	01101
P	abbba	01110
Q	abbbb	01111
R	baaaa	10000
S	baaab	10001
T	baaba	10010
U, V	baabb	10011
W	babaa	10100
X	babab	10101
Y	babba	10110
Z	babbb	10111



Ciphertext:

00001 00000 00010 01101 01100

BACON

STEGANOGRAPHY

- Steganography is the practice of concealing a message within another message or a physical object.
- Here, a computer file, message, image, or video is concealed within another file, message, image, or video.

STEGANOGRAPHY

- You will encounter different scenarios where you have to manage different media to completely solve the given situation.
- You can use the internet and any other open-source software to find the flags.
- You will be provided with an encrypted password for the required media and you will have to decrypt it to open the document.

THANK YOU