INS Practical 1

Date: **02-02-2023**

Roll no.: **20BCE119**

Name: **Kartavya Patel**

Course Code and Name: 2CSDE54 **Information and Network Security**

Task

- Implementation and crypt-analysis of shift-based ciphers- Caesar Cipher, ROT-13 cipher)

```
const caesar_cipher = {
  validate_character: (input) => {
    if (input.length == 1) {
      let charCodeAt = input.charCodeAt(0);
      if (
        (64 < charCodeAt && charCodeAt < 91) ||
        (96 < charCodeAt && charCodeAt < 123)
      ) {
        return charCodeAt;
      }
    }
    return false;
  },
  encrypt: (input, key) => {
    let encrypted = "";
    key %= 26;
    [...input].forEach((element, index) => {
      let validate_character_result =
        caesar_cipher.validate_character(element);
      if (typeof validate_character_result === "number") {
```

```
            let subtract_value = 97;
            if (validate_character_result < 96) {
              subtract_value = 65;
            }
            encrypted += String.fromCharCode(
              subtract_value +
                ((validate_character_result + key - subtract_value) %
                  26)
            );
          } else {
            encrypted += input[index];
          }
        });
        return encrypted;
    },
    decrypt: (input, key) => {
        let decrypted = "";
        key %= 26;
        decrypted = caesar_cipher.encrypt(input, (26 - key) % 26);
        return decrypted;
    },
    ROT13: {
        encrypt: (input) => {
            return caesar_cipher.encrypt(input, 13);
        },
        decrypt: (input) => {
            return caesar_cipher.decrypt(input, 13);
        },
    },
};
let input = "Lorem Ipsum",
    key = 10;
console.log(`\nOriginal text: ${input}`);
console.log(
    `\nCipher text when key is ${key}: ${caesar_cipher.encrypt(input, key)}`
);
console.log(
```

```
  `\nCipher text of ROT-13 cipher: ${caesar_cipher.ROT13.encrypt(input)}`
);
console.log(
  `\nDecrypted back to original text: ${caesar_cipher.decrypt(
    caesar_cipher.encrypt(input, key),
    key
  )}`
);
```

Output