Cryptography and Network Security Lab

Assignment 5

Student Details

Name : Krunal Rank
Adm No. : U18CO081

1

```
# sample text : once upon a time there was a little girl named goldilocks she went
for a walk in the forest pretty soon she came upon a house she knocked and when no
one answered she walked right in at the table in the kitchen there were three bowls
of porridge goldilocks was hungry she tasted the porridge from the first bowl
import math


class ERRORS:
    """
    Error Messages
    """
    INVALID_CHOICE = "Please enter a valid Integer choice."
    INVALID_LINEAR_COEFFICIENT = "Please enter a valid value of Linear Coefficient. It
should be coprime with 26."
    INVALID_TEXT = "Please enter a valid Text. Text must only contain Lowercase
Alphabets."


MOD = 26


class UtilityHelper:
    """
    Contains Utility Methods
    """
    @staticmethod
    def mod_inverse(a):
        """
        Returns Modular Inverse of a
        """
        for i in range(MOD):
            if (a*i) % MOD == 1:
                return i
```

```
        return -1

    @staticmethod
    def mod_add(a, b):
        """
        Returns Modular Addition of a and b
        """
        return (a+b) % MOD

    @staticmethod
    def mod_sub(a, b):
        """
        Returns Modular Subtraction of a and b
        """
        return (a-b+MOD) % MOD

    @staticmethod
    def mod_mul(a, b):
        """
        Returns Modular Multiplication of a and b
        """
        return (a % MOD*b % MOD) % MOD


def affine_cipher_encrypt(text: str, linear_coefficient: int, shift: int):
    """
    Affine Cipher Encryption using given linear_coefficient and shift.
    Returns:
        Encrypted Text
    """
    linear_coefficient %= MOD
    if math.gcd(linear_coefficient, MOD) != 1:
        raise Exception(ERRORS.INVALID_LINEAR_COEFFICIENT)

    text = text.lower()

    for c in text:
        if not (c.isalpha() or c.isspace()):
            raise Exception(ERRORS.INVALID_TEXT)

    encrypted_chars = []
    for i in range(len(text)):
        if text[i].isspace():
            encrypted_chars.append(" ")
            continue
        encrypted_chars.append(chr(UtilityHelper.mod_add(UtilityHelper.mod_mul(
```

```
            linear_coefficient, ord(text[i])-ord('a')), shift) + ord('a')))

    return "".join(encrypted_chars)


def affine_cipher_decrypt(text: str, linear_coefficient: int, shift: int):
    """
    Affine Cipher Decryption using given linear_coefficient and shift.
    Returns:
        Decrypted Text
    """
    linear_coefficient %= MOD
    if math.gcd(linear_coefficient, MOD) != 1:
        raise Exception(ERRORS.INVALID_LINEAR_COEFFICIENT)

    decrypted_chars = []
    for i in range(len(text)):
        if text[i].isspace():
            decrypted_chars.append(" ")
            continue
        decrypted_chars.append(chr(ord(
            'a') +
UtilityHelper.mod_mul(UtilityHelper.mod_inverse(linear_coefficient),
UtilityHelper.mod_sub(ord(text[i])-ord('a'), shift))))

    return "".join(decrypted_chars)


def affine_cipher_encrypt_dialog():
    """
    Runs Affine Cipher Encryption Dialog
    """
    text = input("Enter text to be encrypted: ")
    linear_coefficient = int(input("Enter a Linear Coefficient(Must be coprime with
26): "))
    shift = int(input("Enter a Shift value: "))
    encrypted_text = affine_cipher_encrypt(text,linear_coefficient,shift)


    print(f"Encrypted Text: {encrypted_text}")


def affine_cipher_decrypt_dialog():
    """
    Runs Affine Cipher Decryption Dialog
    """
```

```
    text = input("Enter text to be decrypted: ")
    linear_coefficient = int(input("Enter a Linear Coefficient(Must be coprime with
26): "))
    shift = int(input("Enter a Shift value: "))
    decrypted_text = affine_cipher_decrypt(text, linear_coefficient,shift)

    print(f"Decrypted Text: {decrypted_text}")

def main_dialog():
    """
    Runs main dialog sequence
    """
    try:
        choice = int(input(
            "Affine Cipher Program\n1. Encrypt\n2. Decrypt\nPlease enter your choice:
"))
    except Exception as e:
        raise Exception(ERRORS.INVALID_CHOICE)

    if choice == 1:
        affine_cipher_encrypt_dialog()
    elif choice == 2:
        affine_cipher_decrypt_dialog()
    else:
        raise Exception(ERRORS.INVALID_CHOICE)

if __name__ == "__main__":
    try:
        main_dialog()
    except Exception as e:
        print(e)
```

```
kr@arc-warden:/mnt/6AD574E142A88B4D/BTech/Assignments/4th_Year/CNS/Assignment_5$ python3 1.py
Affine Cipher Program
1. Encrypt
2. Decrypt
Please enter your choice: 1
Enter text to be encrypted: once upon a time there was a little girl named goldilocks she went for a walk in the forest pretty
soon she came upon a house she knocked and when no one answered she walked right in at the table in the kitchen there were thre
e bowls of porridge goldilocks was hungry she tasted the porridge from the first bowl
Enter a Linear Coefficient(Must be coprime with 26): 5
Enter a Shift value: 8
Encrypted Text: avsc efav i zwqc zrcpc oiu i lwzzlc mwpl viqcx malxwlasgu urc ocvz hap i oilg wv zrc hapcuz fpczzy uaav urc siq
c efav i raeuc urc gvasgcx ivx orcv va avc ivuocpcx urc oilgcx pwmrz wv iz zrc zinlc wv zrc gwzsrcv zrcpc ocpc zrpcc naolu ah f
appwxmc malxwlasgu oiu revmpy urc ziuzcx zrc fappwxmc hpaq zrc hwpuz naol
kr@arc-warden:/mnt/6AD574E142A88B4D/BTech/Assignments/4th_Year/CNS/Assignment_5$ python3 1.py
Affine Cipher Program
1. Encrypt
2. Decrypt
Please enter your choice: 2
Enter text to be decrypted: avsc efav i zwqc zrcpc oiu i lwzzlc mwpl viqcx malxwlasgu urc ocvz hap i oilg wv zrc hapcuz fpczzy
uaav urc siqc efav i raeuc urc gvasgcx ivx orcv va avc ivuocpcx urc oilgcx pwmrz wv iz zrc zinlc wv zrc gwzsrcv zrcpc ocpc zrpc
c naolu ah fappwxmc malxwlasgu oiu revmpy urc ziuzcx zrc fappwxmc hpaq zrc hwpuz naol
Enter a Linear Coefficient(Must be coprime with 26): 5
Enter a Shift value: 8
Decrypted Text: once upon a time there was a little girl named goldilocks she went for a walk in the forest pretty soon she cam
e upon a house she knocked and when no one answered she walked right in at the table in the kitchen there were three bowls of p
orridge goldilocks was hungry she tasted the porridge from the first bowl
```