In [26]:

```python
import random

# Diffie-Hellman parameters
p = 23  # A prime number
g = 5   # A primitive root modulo p

# Generate private key (a) and public key (A) using Diffie-Hellman
a = random.randint(2, p - 2)
A = (g ** a) % p

# Receiver's private key (b) and public key (B)
b = random.randint(2, p - 2)
B = (g ** b) % p

# Your roll number and first name
#roll_number = "12345"
#first_name = "John"
roll_no = int(input("Enter the Rollno:- "))
first_name = input("Enter the first_name- ")

# ElGamal Encryption
def encrypt(message, recipient_public_key):
    k = random.randint(2, p - 2)
    shared_secret = (recipient_public_key ** a) % p
    c1 = (g ** k) % p
    c2 = (message * (shared_secret ** k)) % p
    return c1, c2

# ElGamal Decryption
def decrypt(c1, c2):
    shared_secret = (c1 ** b) % p
    inverted_shared_secret = pow(shared_secret, -1, p)
    decrypted_message = (c2 * inverted_shared_secret) % p
    return decrypted_message

# Encrypt and Decrypt your roll number and first name
encrypted_roll_number = encrypt(int(roll_number), B)
encrypted_first_name = encrypt(int.from_bytes(first_name.encode(), 'big'),

decrypted_roll_number = decrypt(*encrypted_roll_number)
decrypted_first_name_bytes = decrypt(*encrypted_first_name)
decrypted_first_name = decrypted_first_name_bytes.to_bytes((decrypted_firs

print("Original Roll Number:", roll_number)
print("Encrypted Roll Number:", encrypted_roll_number)
print("Decrypted Roll Number:", decrypted_roll_number)
print("Original First Name:", first_name)
print("Encrypted First Name:", encrypted_first_name)
print("Decrypted First Name:", decrypted_first_name)

```

```
Enter the Rollno:- 125563
Enter the first_name- Amardeep
Original Roll Number: 12345
Encrypted Roll Number: (17, 1)
Decrypted Roll Number: 11
Original First Name: Amardeep
Encrypted First Name: (11, 12)
Decrypted First Name: 
```

In [ ]:

```
1
```