**Department of Computer Engineering**

**Name of the Student: Parth Das Roll Number: C-111**

**SAP ID: 60004220185 Class: Comps Division: C-2 Batch: 2**

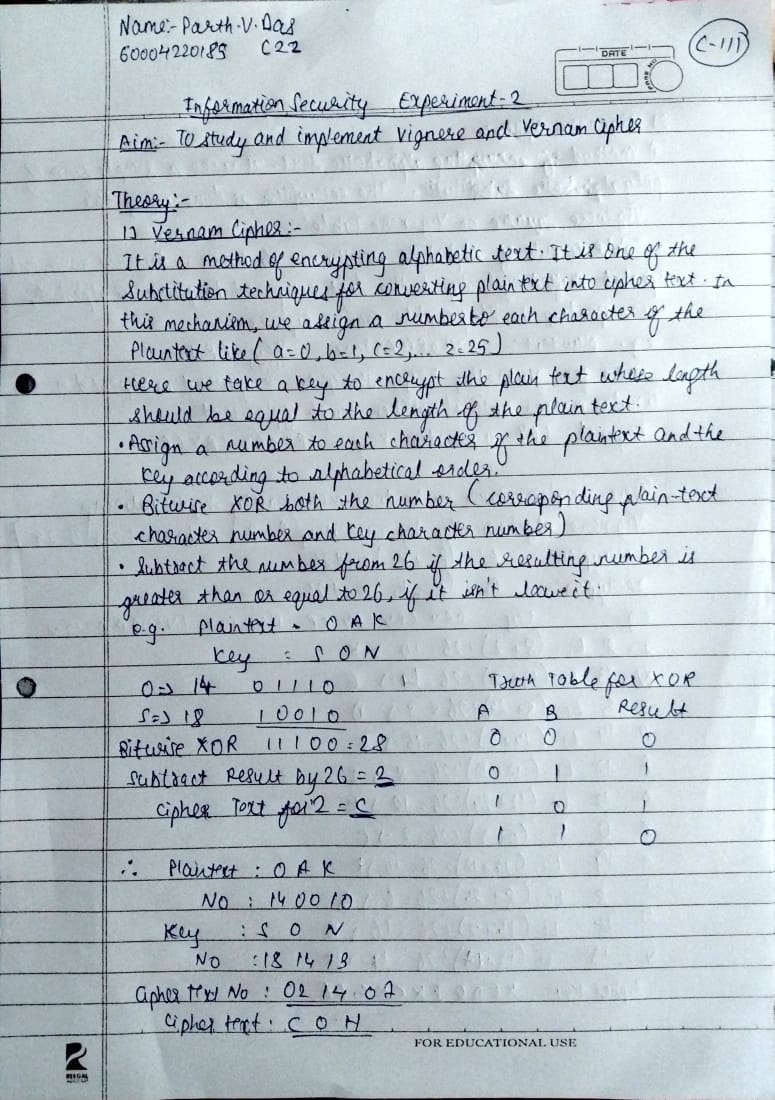
**Subject: Information Security**

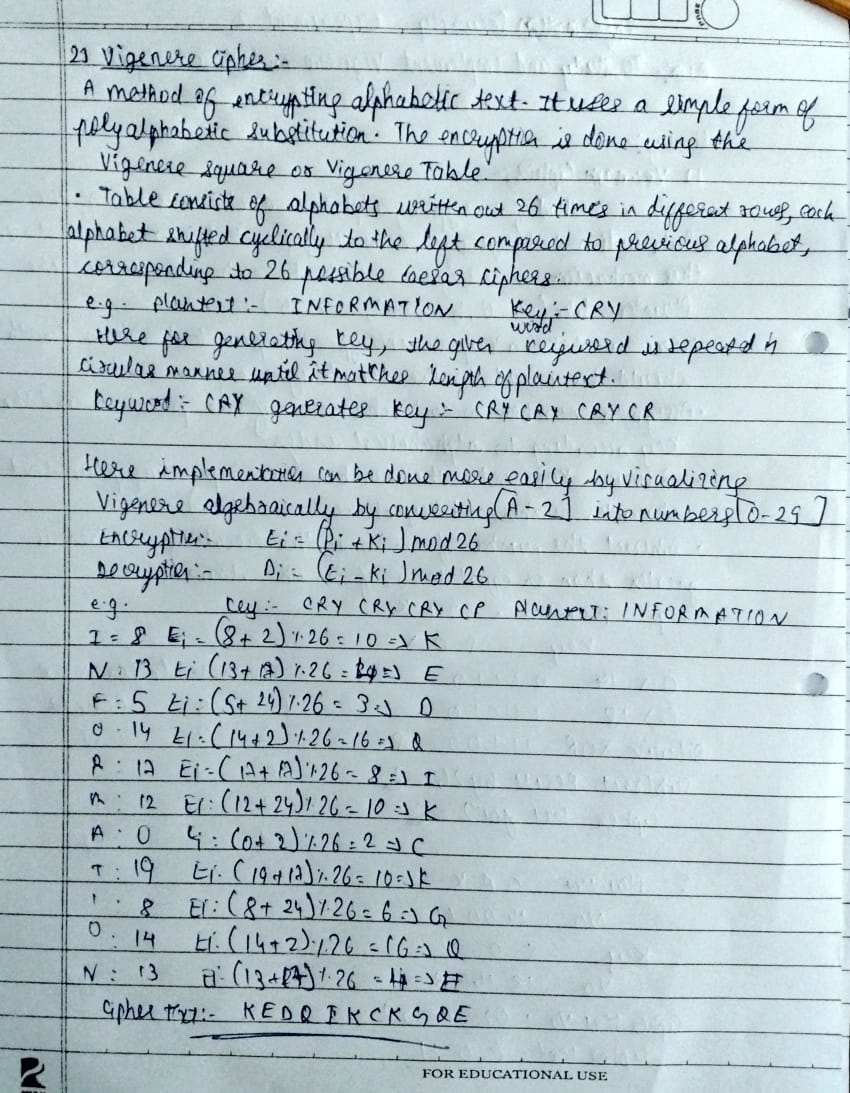
**DATE OF PERFORMANCE: 08/02/2025 DATE OF SUBMISION: 08/02/2025**

**EXPERIMENT NO: 2**

**AIM: To study and Implement Vignere and Vernam Cipher**

**Theory:**

****

****

**SOURCE CODE WITH OUTPUTS:**

def extend\_key(text, key):

extended\_key = []

key\_length = len(key)

for i in range(len(text)):

if text[i] == ' ':

extended\_key.append(' ')

else:

extended\_key.append(key[i % key\_length])

return ''.join(extended\_key)

def vigenere\_encrypt(text, key):

cipher\_text = []

extended\_key = extend\_key(text, key)

for i in range(len(text)):

if text[i] == ' ':

cipher\_text.append(' ')

else:

encrypted\_char = chr(((ord(text[i]) - ord('A') + ord(extended\_key[i]) - ord('A')) % 26) + ord('A'))

cipher\_text.append(encrypted\_char)

return ''.join(cipher\_text)

def vigenere\_decrypt(cipher\_text, key):

plain\_text = []

extended\_key = extend\_key(cipher\_text, key)

for i in range(len(cipher\_text)):

if cipher\_text[i] == ' ':

plain\_text.append(' ')

else:

decrypted\_char = chr(((ord(cipher\_text[i]) - ord(extended\_key[i]) + 26) % 26) + ord('A'))

plain\_text.append(decrypted\_char)

return ''.join(plain\_text)

def vernam\_cipher(text, key):

cipher\_text = []

for i in range(len(text)):

encrypted\_char = chr(ord(text[i]) ^ ord(key[i % len(key)]))

cipher\_text.append(encrypted\_char)

return ''.join(cipher\_text)

if \_\_name\_\_ == "\_\_main\_\_":

plaintext = "INTELLIGENCE IS PRICELESS"

key = "CRYPTO"

vigenere\_encrypted = vigenere\_encrypt(plaintext, key)

print("Vigenere Encrypted:", vigenere\_encrypted)

vigenere\_decrypted = vigenere\_decrypt(vigenere\_encrypted, key)

print("Vigenere Decrypted:", vigenere\_decrypted)

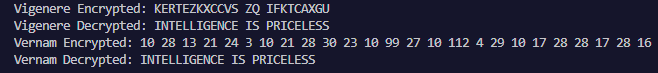
vernam\_encrypted = vernam\_cipher(plaintext, key)

print("Vernam Encrypted:", ' '.join(str(ord(c)) for c in vernam\_encrypted))

vernam\_decrypted = vernam\_cipher(vernam\_encrypted, key)

print("Vernam Decrypted:", vernam\_decrypted)

**Output:-**



**CONCLUSION:**

The experiment showed that the Vigenère Cipher is better than simple substitution but can be broken if the key repeats. It keeps spaces unchanged, making it easier to analyze. The Vernam Cipher (One-Time Pad), using XOR, completely scrambles the text, including spaces, making it impossible to break if the key is truly random and used only once. While Vigenère is mostly for learning, Vernam’s method is still used in highly secure communication.