বরেন্দ্র বিশ্ববিদ্যালয়
VARENDRA UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Lab Report-3

Course Title: Cryptography and Network Security Lab

Course Code: CSE-432

Submitted By	Submitted To
Name: Md. Nahid Hasan **ID:** 221311131 **Section:** D **Semester:** 9th **Batch:** 29th **Dept. Of CSE** **Varendra University,** **Rajshahi**	**Mohammad Faisal Al-Naser** Lecturer **Md. Fayzul Islam** Lecturer **Dept. Of CSE** **Varendra University,** **Rajshahi**

Submission Date: 14.08.2025

❒ Experiment No: 03

❒ Experiment Name: Affine Cipher for Extended ASCII (0–255)

❖ Code

```
#include <iostream>
#include <string>
using namespace std;

const int M = 256;

int modInverse(int a, int m) {
    a = a % m;
    for (int x = 1; x < m; x++) {
        if ((a * x) % m == 1) return x;
    }
    return -1;
}

string encrypt(string text, int a, int b) {
    string result = "";
    for (unsigned char ch : text) {
        int x = ch;
        int enc = (a * x + b) % M;
        result += (unsigned char)enc;
    }
    return result;
}

string decrypt(string text, int a, int b) {
    string result = "";
    int a_inv = modInverse(a, M);
    if (a_inv == -1) return "Invalid 'a'!";

    for (unsigned char ch : text) {
        int y = ch;
        int dec = (a_inv * (y - b + M)) % M;
        result += (unsigned char)dec;
    }
    return result;
}

int main() {
    string text;
    int a, b;

    cout << "Enter plain text: ";
    getline(cin, text);

    cout << "Enter key a (coprime with 256): ";
    cin >> a;
```

```
    cout << "Enter key b: ";
    cin >> b;

    if (modInverse(a, M) == -1) {
        cout << "a must be coprime with 256" << endl;
        return 1;
    }

    string cipher = encrypt(text, a, b);
    cout << "Encrypted: " << cipher << endl;
    cout << "Decrypted: " << decrypt(cipher, a, b) << endl;

    return 0;
}
```

❖ **Output:**