PRAKTIKUM KRIPTOGRAFI

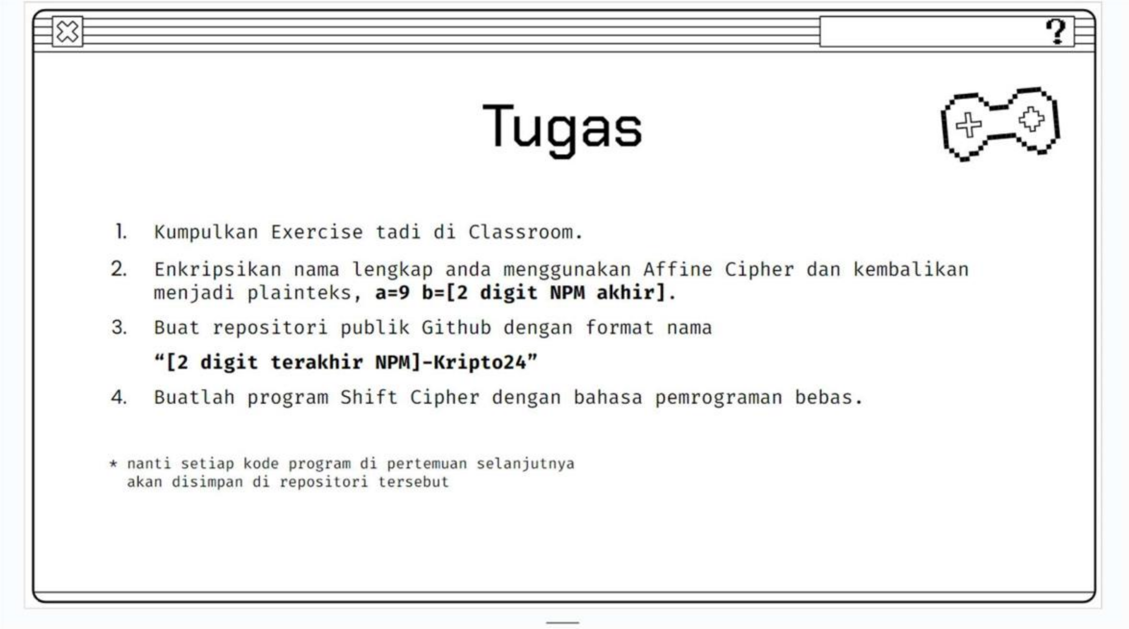
TUGAS 2

DISUSUN OLEH :

Muhammad Danendra Syah H – 140810220064

PROGRAM STUDI S1 TEKNIK INFORMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS PADJADJARAN

2024



Tugas

1. Kumpulkan Exercise tadi di Classroom.
2. Enkripsikan nama lengkap anda menggunakan Affine Cipher dan kembalikan menjadi plainteks, **a=9 b=[2 digit NPM akhir].**
3. Buat repositori publik Github dengan format nama
   “[2 digit terakhir NPM]-Kripto24”
4. Buatlah program Shift Cipher dengan bahasa pemrograman bebas.

* nanti setiap kode program di pertemuan selanjutnya
  akan disimpan di repositori tersebut

2. Nama lengkap menggunaka Affine Chiper dan kembalikan menjadi plainteks, a = 9, b = 64

Enkripsi :

MUHAMMAD = 12, 20, 7, 0, 12, 12, 0, 3

E(12)=(9(12) + 64) mod 26 = 172 mod 26 = 16 ➔ Q

E (20) = (9(20) + 64) mod 26 = 244 mod 26 = 10 ➔ K

E (7) = (9(7) + 64) mod 26 = 127 mod 26 = 23 ➔ X

E (0) = (9(0) + 64) mod 26 = 64 mod 26 = 12 ➔ M

E (12) = 16 ➔ Q

E (12) = 16 ➔ Q

E (0) = 12 ➔ M

E (3) = (9(3) + 64) mod 26 = 91 mod 26 = 13 ➔ N

MUHAMMAD ➔ E(x) ➔ QKXMQQMN

Dekripsi :

QKXMQQMN = 16, 10, 23, 12, 16, 16, 12, 13

D(16) = 3(16−64) mod 26 = −144 mod 26 = 12 ➔ M

D(10) = 3(10−64) mod 26 = −162 mod 26 = 20 ➔ U

D(23) = 3(23−64) mod 26 = −123 mod 26 = 7 ➔ H

D(12) = 3(12−64) mod 26 = −156 mod 26 = 0 ➔ A

D(16) = 12 ➔ M

D(16) = 12 ➔ M

D(12) = 0 ➔ A

D(13) = 3(13−64) mod 26 = −153 mod 26 = 3 ➔ D

QKXMQQMN ➔ D(y) ➔ MUHAMMAD

Enkripsi :

DANENDRA = 3, 0, 13, 4, 13, 3, 17, 0

$E(3) = (9(3) + 64) \bmod 26 = 91 \bmod 26 = 13$ ➔ N

$E (0) = (9(0) + 64) \bmod 26 = 64 \bmod 26 = 12$ ➔ M

$E (13) = (9(13) + 64) \bmod 26 = 181 \bmod 26 = 25$ ➔ Z

$E (4) = (9(4) + 64) \bmod 26 = 100 \bmod 26 = 22$ ➔ W

$E (13) = 25$ ➔ Z

$E (3) = 13$ ➔ N

$E (17) = (9(17) + 64) \bmod 26 = 217 \bmod 26 = 9$ ➔ J

$E (0) = 12$ ➔ M

DANENDRA ➔ E(x) ➔ NMZWZNJM

Dekripsi :

NMZWZNJM = 13, 12, 25, 22, 25, 13, 9, 12

$D(13) = 3(13-64) \bmod 26 = -153 \bmod 26 = 3$ ➔ D

$D(12) = 3(12-64) \bmod 26 = -156 \bmod 26 = 0$ ➔ A

$D(25) = 3(25-64) \bmod 26 = -117 \bmod 26 = 13$ ➔ N

$D(22) = 3(22-64) \bmod 26 = -126 \bmod 26 = 4$ ➔ E

$D(25) = 13$ ➔ N

$D(13) = 3$ ➔ D

$D(9) = 3(9-64) \bmod 26 = -165 \bmod 26 = 17$ ➔ R

$D(12) = 0$ ➔ A

NMZWZNJM ➔ D(y) ➔ DANENDRA

Enkripsi :

SYAH = 18, 24, 0, 7

$E(18) = (9(18) + 64) \bmod 26 = 226 \bmod 26 = 18$ ➔ S

$E (24) = (9(24) + 64) \bmod 26 = 280 \bmod 26 = 20$ ➔ U

$E (0) = (9(0) + 64) \bmod 26 = 64 \bmod 26 = 12$ ➔ M

$E (7) = (9(7) + 64) \bmod 26 = 127 \bmod 26 = 23$ ➔ X

SYAH ➔ E(x) ➔ SUMX

Dekripsi:

SUMX = 18, 20, 12, 23

$D(18) = 3(18-64) \bmod 26 = -138 \bmod 26 = 18$ ➔ S

$D(20) = 3(20-64) \bmod 26 = -132 \bmod 26 = 24$ ➔ Y

$D(12) = 3(12-64) \bmod 26 = -156 \bmod 26 = 0$ ➔ A

$D(23) = 3(23-64) \bmod 26 = -123 \bmod 26 = 7$ ➔ H

SUMX ➔ D(y) ➔ SYAH

Enkripsi :

HIDAYATULLAH = 7, 8, 3, 0, 24, 0, 19, 20, 11, 11, 0, 7

$E (7) = (9(7) + 64) \bmod 26 = 127 \bmod 26 = 23$ ➔ X

$E (8) = (9(8) + 64) \bmod 26 = 136 \bmod 26 = 6$ ➔ G

$E(3) = (9(3) + 64) \bmod 26 = 91 \bmod 26 = 13$ ➔ N

E (0) = (9(0) + 64) mod 26 = 64 mod 26 = 12 → M

E (24) = (9(24) + 64) mod 26 = 280 mod 26 = 20 → U

E (0) = 12 → M

E (19) = (9(19) + 64) mod 26 = 235 mod 26 = 1 → B

E (20) = (9(20) + 64) mod 26 = 244 mod 26 = 10 → K

E (11) = (9(11) + 64) mod 26 = 163 mod 26 = 7 → H

E (11) = 7 → H

E (0) = 12 → M

E (7) = 23 → X

HIDAYATULLAH → E(x) → XGNMUMBKHHMX

Dekripsi:

XGNMUMBKHHMX = 23, 6, 13, 12, 20, 12, 1, 10, 7, 7, 12, 23

D(23) = 3(23−64) mod 26 = −123 mod 26 = 7 → H

D(6) = 3(6−64) mod 26 = −174 mod 26 = 8 → I

D(13) = 3(13−64) mod 26 = −153 mod 26 = 3 → D

D(12) = 3(12−64) mod 26 = −156 mod 26 = 0 → A

D(20) = 3(20−64) mod 26 = −132 mod 26 = 24 → Y

D(12) = 0 → A

D(1) = 3(1−64) mod 26 = −189 mod 26 = 19 → T

D(10) = 3(10−64) mod 26 = −162 mod 26 = 20 → U

D(7) = 3(7−64) mod 26 = −171 mod 26 = 11 → L

D(7) = 11 → L

D(12) = 0 → A

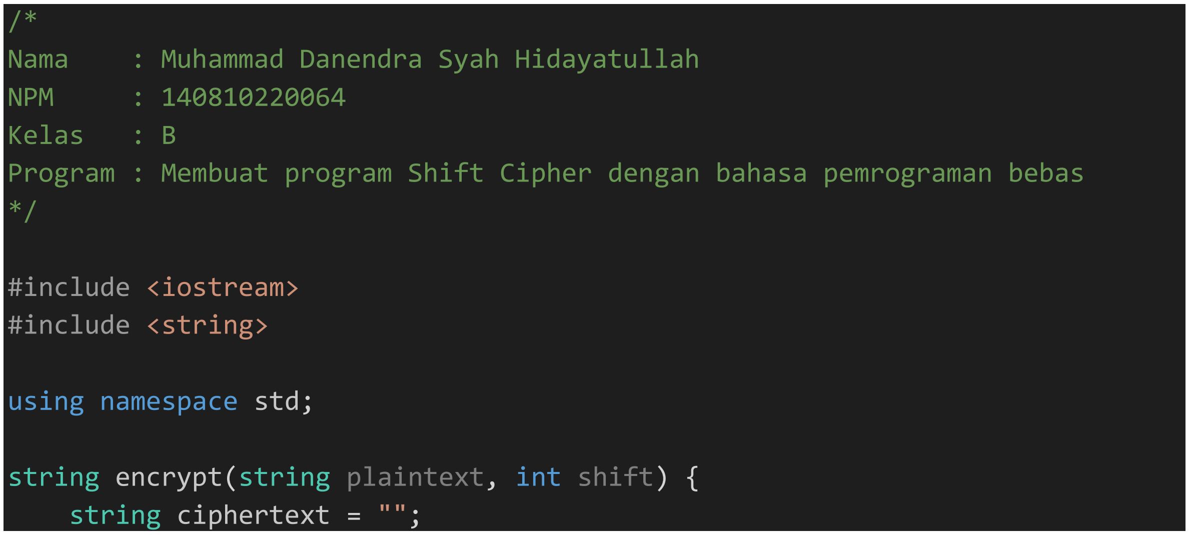
D(23) = 7 → H

XGNMUMBKHHMX → D(y) → HIDAYATULLAH

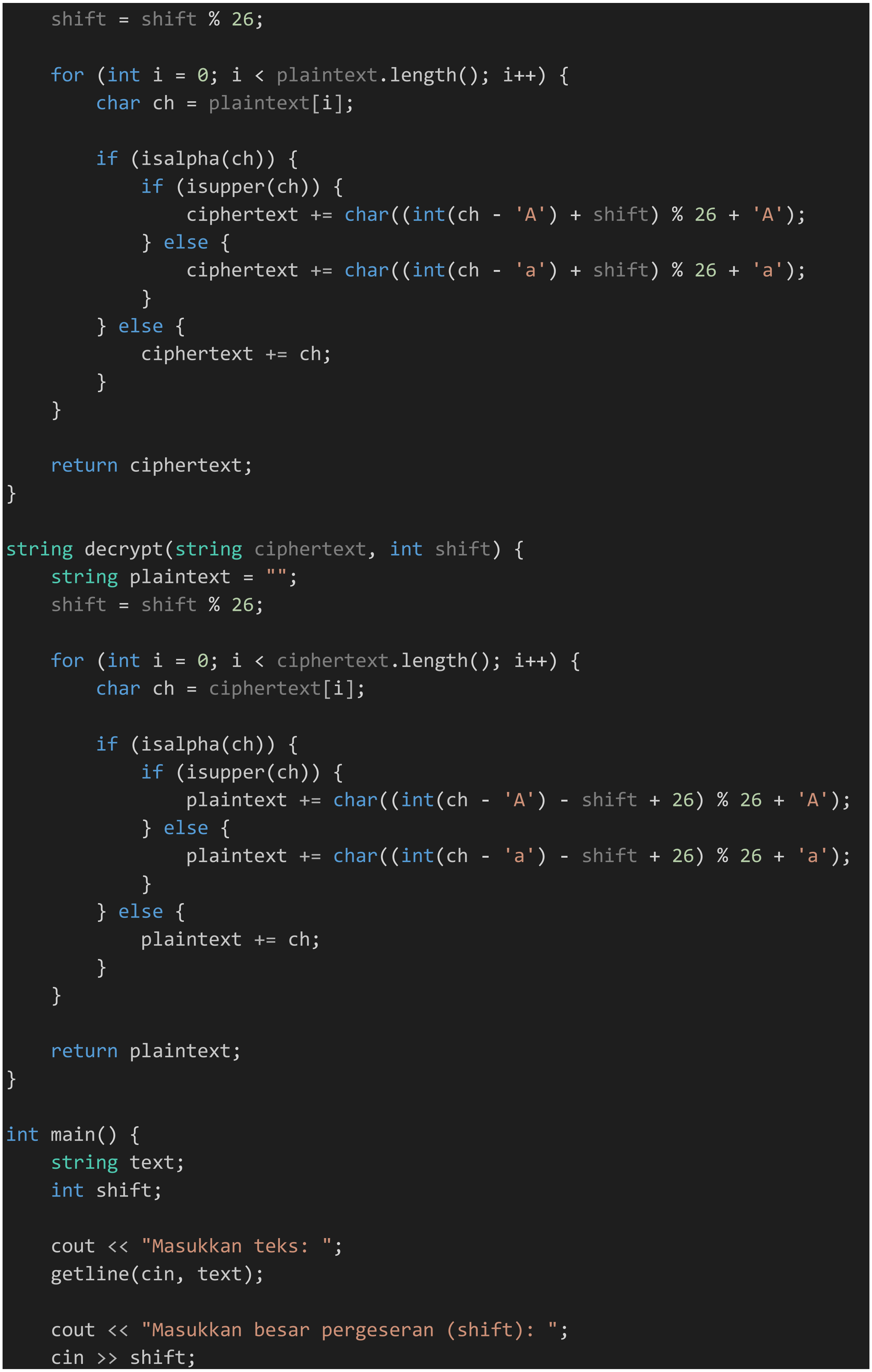
3. Buat repositori public github

   https://github.com/Danendra1-ux/64-kripto24

4. Buat Bahasa pemrograman Shift Cipher dengan Bahasa pemrograman bebas

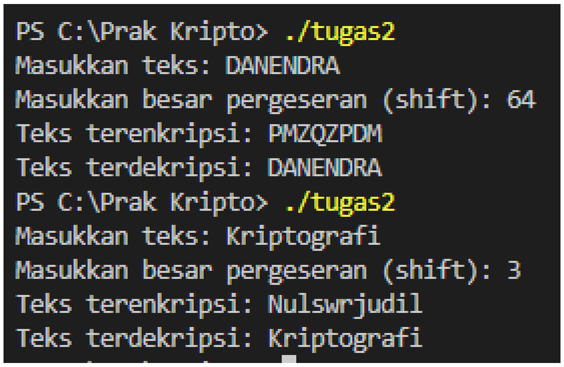


```
/*
Nama    : Muhammad Danendra Syah Hidayatullah
NPM     : 140810220064
Kelas   : B
Program : Membuat program Shift Cipher dengan bahasa pemrograman bebas
*/

#include <iostream>
#include <string>

using namespace std;

string encrypt(string plaintext, int shift) {
    string ciphertext = "";
```



```
    shift = shift % 26;

    for (int i = 0; i < plaintext.length(); i++) {
        char ch = plaintext[i];

        if (isalpha(ch)) {
            if (isupper(ch)) {
                ciphertext += char((int(ch - 'A') + shift) % 26 + 'A');
            } else {
                ciphertext += char((int(ch - 'a') + shift) % 26 + 'a');
            }
        } else {
            ciphertext += ch;
        }
    }

    return ciphertext;
}

string decrypt(string ciphertext, int shift) {
    string plaintext = "";
    shift = shift % 26;

    for (int i = 0; i < ciphertext.length(); i++) {
        char ch = ciphertext[i];

        if (isalpha(ch)) {
            if (isupper(ch)) {
                plaintext += char((int(ch - 'A') - shift + 26) % 26 + 'A');
            } else {
                plaintext += char((int(ch - 'a') - shift + 26) % 26 + 'a');
            }
        } else {
            plaintext += ch;
        }
    }

    return plaintext;
}

int main() {
    string text;
    int shift;

    cout << "Masukkan teks: ";
    getline(cin, text);

    cout << "Masukkan besar pergeseran (shift): ";
    cin >> shift;
    string encryptedText = encrypt(text, shift);
    cout << "Teks terenkripsi: " << encryptedText << endl;

    string decryptedText = decrypt(encryptedText, shift);
    cout << "Teks terdekripsi: " << decryptedText << endl;

    return 0;
}
```

Hasil Running:



```
PS C:\Prak Kripto> ./tugas2
Masukkan teks: DANENDRA
Masukkan besar pergeseran (shift): 64
Teks terenkripsi: PMZQZPDM
Teks terdekripsi: DANENDRA
PS C:\Prak Kripto> ./tugas2
Masukkan teks: Kriptografi
Masukkan besar pergeseran (shift): 3
Teks terenkripsi: Nulswrjudil
Teks terdekripsi: Kriptografi
```