T.C.
ONDOKUZ MAYIS ÜNİVERSİTESİ
MÜHENDİSLİK FAKÜLTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

Bilgisayar Mühendisliği Özel Konular- 2
Şifreleme Sistemi Tasarımı Ve Uygulaması

ALEYNA KAHRAMAN

20060355

KOD

```python
ALFABE = 'abcçdefgğhıijklmnoöprsştuüvyz'

def sifrele(metin, a, b):
    sifreli_metin = ''
    for harf in metin:
        if harf.lower() in ALFABE:
            harf_sira = ALFABE.index(harf.lower())
            sifreli_harf_sira = (a * harf_sira + b) % len(ALFABE)
            sifreli_metin += ALFABE[sifreli_harf_sira].upper() if harf.isupper() else ALFABE[sifreli_harf_sira]
        else:
            sifreli_metin += harf
    return sifreli_metin

def desifre(sifreli_metin, a, b):
    orijinal_metin = ''
    for harf in sifreli_metin:
        if harf.lower() in ALFABE:
            sifreli_harf_sira = ALFABE.index(harf.lower())
            orijinal_harf_sira = ((sifreli_harf_sira - b) * mod_inverse(a, len(ALFABE))) % len(ALFABE)
            orijinal_metin += ALFABE[orijinal_harf_sira].upper() if harf.isupper() else ALFABE[orijinal_harf_sira]
        else:
            orijinal_metin += harf
    return orijinal_metin

def mod_inverse(a, m):
    for i in range(1, m):
        if (a * i) % m == 1:
            return i
    return None

def ayarla_dogum_tarihi(tarih):
    try:
        gun, ay, yil = map(int, tarih.split('.'))
    except ValueError:
        print("Hatalı format! Lütfen doğru formatta (GG.AA.YYYY) girin.")
        return None, None
    # Basit bir örnek doğum tarihine dayalı ayarlama
    a = (gun + ay) % len(ALFABE) + 1  # 1-29 arası bir çarpma faktörü
    b = (ay + yil) % len(ALFABE) + 1  # 1-29 arası bir kaydırma miktarı
    return a, b
```

```python

while True:
    islem_turu = input("Şifrelemek için 'şifrele', deşifrelemek için 'deşifrele' yazın, çıkmak için 'q' yazın: ").lower()

    if islem_turu == 'şifrele':
        metin = input("Şifrelemek istediğiniz metni girin: ")

        while True:
            dogum_tarihi = input("Doğum tarihinizi (GG.AA.YYYY formatında) girin: ")
            a, b = ayarla_dogum_tarihi(dogum_tarihi)
            if a is not None and b is not None:
                break

        # Şifreleme işlemi
        sifreli_metin = sifrele(metin, a, b)
        print("Şifrelenmiş Metin:", sifreli_metin)
    elif islem_turu == 'deşifrele':
        sifreli_metin = input("Deşifrelemek istediğiniz metni girin: ")

        while True:
            dogum_tarihi = input("Doğum tarihinizi (GG.AA.YYYY formatında) girin: ")
            a, b = ayarla_dogum_tarihi(dogum_tarihi)
            if a is not None and b is not None:
                break

        # Şifre çözme işlemi
        orijinal_metin = desifre(sifreli_metin, a, b)
        print("Orijinal Metin:", orijinal_metin)
    elif islem_turu == 'q':
        break
    else:
        print("Geçersiz işlem türü. Lütfen 'şifrele', 'deşifrele' veya 'q' (çıkış) olarak yazın.")

```

1. ALFABE Tanımı:

- **`ALFABE`**, Türk alfabesindeki karakterleri içeren bir dizedir. Türk alfabesindeki tüm harfler ve ek olarak bazı özel karakterler bulunmaktadır.

2. Şifreleme Fonksiyonu (`sifrele`):

- Bu fonksiyon, verilen bir metni şifreler.
- Metindeki her bir harfi alır ve eğer bu harf Türk alfabesinde bulunuyorsa şifreleme işlemine tabi tutar.
- Şifreleme işlemi için verilen iki anahtar (**`a`** ve **`b`**) kullanılır.
- Harfin sırasını (**`harf_sira`**) hesaplar ve bu sırayı **`a`** ile çarparak **`b`** ile kaydırma yapar.
- Sonuç olarak şifrelenmiş metni döndürür.

3. Deşifreleme Fonksiyonu (`desifre`):

- Bu fonksiyon, şifrelenmiş bir metni çözer.
- Şifrelenmiş metindeki her bir harfi alır ve eğer bu harf Türk alfabesinde bulunuyorsa çözme işlemine tabi tutar.
- Şifre çözme işlemi için verilen iki anahtar (**`a`** ve **`b`**) kullanılır.
- Şifrelenmiş harfin sırasını (**`sifreli_harf_sira`**) hesaplar ve bu sırayı orijinal metne dönüştürür.
- Sonuç olarak orijinal metni döndürür.

4. Ters Mod Fonksiyonu (`mod_inverse`):

- Bu fonksiyon, verilen bir sayının modüler tersini bulur.
- Şifreleme ve çözme işlemlerinde kullanılan anahtarları hesaplamak için kullanılır.

5. Doğum Tarihine Göre Anahtar Ayarlama Fonksiyonu (`ayarla_dogum_tarihi`):

- Bu fonksiyon, kullanıcının doğum tarihine dayalı olarak şifreleme ve çözme için anahtarları ayarlar.
- Kullanıcının girdiği doğum tarihine göre, iki anahtar (**`a`** ve **`b`**) hesaplanır.
- **`a`** parametresi, gün ve ayın toplamının alfabenin uzunluğuna göre mod alınmasıyla elde edilir.
- **`b`** parametresi ise ay ve yılın toplamının alfabenin uzunluğuna göre mod alınmasıyla elde edilir.

6. Ana Döngü:

- Kullanıcıya, metni şifrelemek için 'şifrele', deşifrelemek için 'deşifrele' veya çıkmak için 'q' yazması istenir.
- Kullanıcının seçimine göre, ilgili işlem yapılır.
- İşlem yapılmadan önce, kullanıcıdan doğum tarihini girmesi istenir ve bu tarih doğrultusunda anahtarlar ayarlanır.
- Sonuçlar kullanıcıya gösterilir ve döngü devam eder veya çıkış yapılır.

Bu kod, kullanıcıya basit bir metni şifreleme ve çözme aracı sunar. Kullanıcıların kendi doğum tarihlerine dayalı olarak şifreleme anahtarlarını ayarlaması, güvenlik açısından her kullanıcının farklı bir şifreleme algoritması kullanmasını sağlar.

Uygulama

```
PS C:\Users\aleyy\Desktop\20060355_AleynaKahraman> python sifre.py
Şifrelemek için 'şifrele', deşifrelemek için 'deşifrele' yazın, çıkmak için 'q' yazın: şifrele
Şifrelemek istediğiniz metni girin: Merhaba, ben Aleyna...
Doğum tarihinizi (GG.AA.YYYY formatında) girin: 28.09.2002
Şifrelenmiş Metin: Byoeiri, ryı Isyşıi...
Şifrelemek için 'şifrele', deşifrelemek için 'deşifrele' yazın, çıkmak için 'q' yazın: deşifrele
Deşifrelemek istediğiniz metni girin: Byoeiri, ryı Isyşıi...
Doğum tarihinizi (GG.AA.YYYY formatında) girin: 28.09.2002
Orijinal Metin: Merhaba, ben Aleyna...
Şifrelemek için 'şifrele', deşifrelemek için 'deşifrele' yazın, çıkmak için 'q' yazın: şifre
Geçersiz işlem türü. Lütfen 'şifrele', 'deşifrele' veya 'q' (çıkış) olarak yazın.
Şifrelemek için 'şifrele', deşifrelemek için 'deşifrele' yazın, çıkmak için 'q' yazın: şifrele
Şifrelemek istediğiniz metni girin: Ondokuz Mayıs Üniversitesi
Doğum tarihinizi (GG.AA.YYYY formatında) girin: 55555
Hatalı format! Lütfen doğru formatta (GG.AA.YYYY) girin.
Doğum tarihinizi (GG.AA.YYYY formatında) girin: 01.04.1975
Şifrelenmiş Metin: Toçtzgc Iğüıö Konphjönbhön
Şifrelemek için 'şifrele', deşifrelemek için 'deşifrele' yazın, çıkmak için 'q' yazın: q
PS C:\Users\aleyy\Desktop\20060355_AleynaKahraman>
```