تمرین عملی دوم درس مبانی امنیت

نام دانشجو: رهام زنده دل نوبری **شماره دانشجویی:** ۹۷۳۱۰۸۸

لود کردن کلید

در ابتدا کلید را از فایل لود می کنیم.

In [1]:
```
import os
from dotenv import load_dotenv
import binascii,pbkdf2,secrets,pyaes

load_dotenv()
key = os.getenv('KEY')
key = key.encode('utf-8')
print(f"Key is {key}")
```

```
Key is b'AUT*ICTSec*2022'
```

ساختن کلید رمزنگاری

در ابتدا یک سالت رندوم درست می کنیم.

In [2]:
```
salt = os.urandom(16)
print(f"Salt is {binascii.hexlify(salt)}")
```

```
Salt is b'8fd92185a09e889ee06080047b88e6f5'
```

سپس کلید فایل را با سالت بدست آمده تبدیل به هش ۲۵۶ بیتی می کنیم که کلید الگوریتم ماست.

In [3]:
```
enc_key = pbkdf2.PBKDF2(salt, key).read(32)
print(f"Algorithm Key is: {binascii.hexlify(enc_key)}")
```

```
Algorithm Key is: b'a257b323f9849883e51a7f0f4022129961467a04d404f8928bcf020160776505'
```

رمزنگاری متن واضح

در ابتدا یک بردار ابتدایی برای مد کاری درست می کنیم.

In [4]:
```
initialvector= secrets.randbits(256)
print(f"Initial Vector is: {initialvector}")
```

```
Initial Vector is: 83399119975984147159554147068933982571323124603614559499956305582821953
314010
```

سپس فایل متن واضح را لود می کنیم.

In [5]:
```
plaintext_file = open("plaintext.txt","r")
plaintext = plaintext_file.read()
print(f"Plain-text is: {plaintext}")
plaintext_file.close()
```

```
Plain-text is: 9731088
```

در مرحله بعدی الگوریتم رمزنگاری با مد کاری ذکر شده را لود می کنیم. سپس متن واضح را رمزنگاری می کنیم.

In [6]:
```
aes = pyaes.AESModeOfOperationCTR(enc_key, pyaes.Counter(initialvector))
ciphertext = aes.encrypt(plaintext)
print(f"Encrypted text is: {binascii.hexlify(ciphertext)}")
ciphertext_file = open("ciphertext.txt", "w")
ciphertext_file.write(str(binascii.hexlify(ciphertext)))
ciphertext_file.close()
```

```
Encrypted text is: b'6eb34f5990e261'
```

در مرحله بعدی متن رمزنگاری شده را دیکود می کنیم.

In [7]:
```
aes = pyaes.AESModeOfOperationCTR(enc_key, pyaes.Counter(initialvector))
decrypted_text = aes.decrypt(ciphertext)
print(f"Decrypted text is: {decrypted_text}")
```

```
Decrypted text is: b'9731088'
```

عملکرد تحت کنسول

در این مرحله کدهای نوشته شده برای رمزنگاری را در حلقه ای می گذاریم و در هر دور از کاربر دیکود کردن یا.
انکود کردن را درخواست می کنیم

In [8]:
```
while(True):
    inp = input("Enter E/D for Encryption/Decryption. Enter Stop for Stopping: ")
    if (inp == "E"):
        plaintext_file = open("plaintext.txt", "r")
        plaintext = plaintext_file.read()
        aes = pyaes.AESModeOfOperationCTR(enc_key, pyaes.Counter(initialvector))
        ciphertext = aes.encrypt(plaintext)
        print(f"Encrypted text is: {binascii.hexlify(ciphertext)}")
        ciphertext_file = open("ciphertext.txt", "w")
        ciphertext_file.write(str(binascii.hexlify(ciphertext)))
        ciphertext_file.close()
        plaintext_file.close()
    elif (inp == "D" and ciphertext != ""):
        #the last ciphertext is stored in ciphertext
        aes = pyaes.AESModeOfOperationCTR(enc_key, pyaes.Counter(initialvector))
        decrypted_text = aes.decrypt(ciphertext)
        print(f"Decrypted text is: {decrypted_text}")
    elif (inp == "Stop"):
        break
    else:
        print("Wrong Input! Please try again!\n")
```

```
Enter E/D for Encryption/Decryption. Enter Stop for Stopping: E
Encrypted text is: b'6eb34f5990e261'
Enter E/D for Encryption/Decryption. Enter Stop for Stopping: D
Decrypted text is: b'9731088'
```

```
Enter E/D for Encryption/Decryption. Enter Stop for Stopping: E
Encrypted text is: b'6eb34f5990e261'
Enter E/D for Encryption/Decryption. Enter Stop for Stopping: D
Decrypted text is: b'9731088'
Enter E/D for Encryption/Decryption. Enter Stop for Stopping: F
Wrong Input! Please try again!

Enter E/D for Encryption/Decryption. Enter Stop for Stopping: Stop
```