

# UPB – Zadanie 2

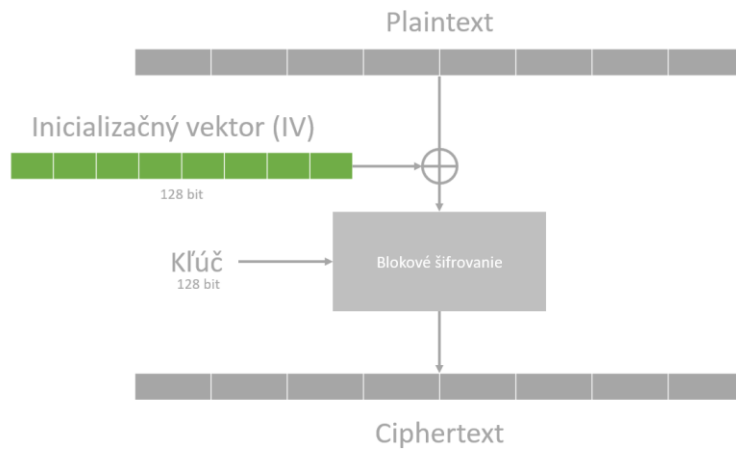
## Symetrická kryptografia

Jazyk : **Python**

Knižnica : **Pycryptodome**

Šifrovanie : **AES** (Advanced encryption standard)

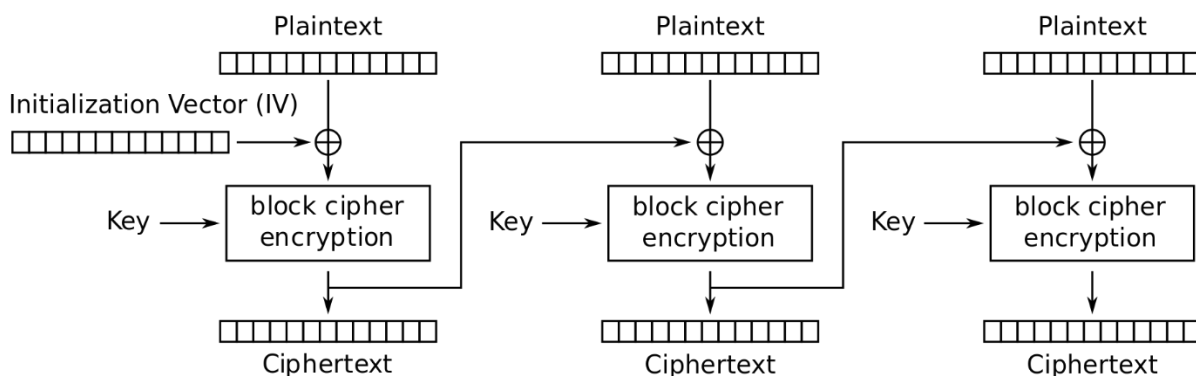
- Veľmi rýchle a bezpečné pre symetrické šifrovanie (Využíva ho americká vláda)
- 128 bitová bloková šifra, je **autogenerovaná**
- 128 bitová dĺžka kľúča (dá sa aj 192 alebo 256 bitová)
- **Vstup sa nazýva „Plaintext“ a výstup „Ciphertext“**



Inicializačný vektor je využití kvôli opakovanému textu. V prípade že sa opakovaný text zašifruje týmto spôsobom bez využitia vektora, zašifrovanie by bolo pre opakovaný text rovnaké v každom prípade a skúsenejší človek by to dokázal odhaliť.

## Mód : CBC (Cipher Block Chaining)

- Potrebný je len jeden inicializačný vektor. Pre nasledujúce bloky sa využíva „Ciphertext“ na náhodné vytvorenie „Plaintext“, zabezpečí sa tým že aj opakujúci text alebo frázy majú rozdielny „Ciphertext“
- Je bežný a jednoduchý na vysvetlenie
- Využíva blokovú šifru na poskytnutie informačnej bezpečnosti. Mód operácie využíva opakovane jedno-blokové operácie na zašifrovanie väčšieho množstva dát ako má samotný blok



Cipher Block Chaining (CBC) mode encryption

*CBC – schéma (zdroj: [https://en.wikipedia.org/wiki/Block\\_cipher\\_mode\\_of\\_operation](https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation))*

**Originálny text :** „Robert Fico“





**Zašifrovaný text:** „xe2\x9e\xe8\x7fY\x0“

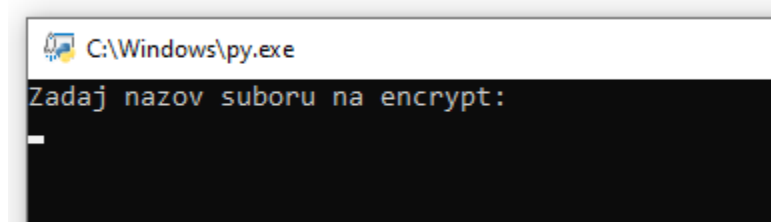
(Ide len o príklad)

# Aplikácia

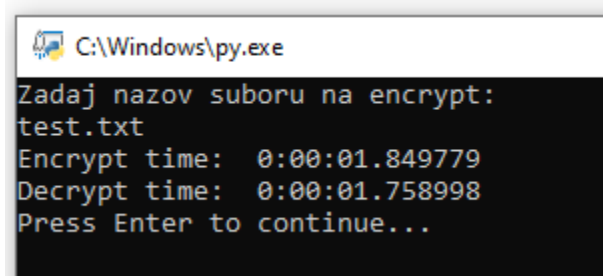
```
1  from Crypto.Cipher import AES
2  from Crypto.Util.Padding import pad
3  from Crypto.Util.Padding import unpad
4  import os
5  from datetime import datetime
6
7  key = os.urandom(16) #generuje 16 bytovy kluc
8  cipher = AES.new(key,AES.MODE_CBC)
9  #vytvara sifru, podľa klucu a algoritmu AES
10 # a mod CBC
11
12 print('Zadaj nazov suboru na encrypt: ')
13 fileName = input()
14
15
16 with open(fileName,mode='rb') as file: #otvori zadany subor a na cita ho ako bity
17     fileContent = file.read()
18
19 nowEncrypt = datetime.now() #zaznamenava cas
20 ciphertext = cipher.encrypt(pad(fileContent,AES.block_size)) #zasifrujem pomocou sifry
21 #pridavam padding aby to bolo urcite nasobok 128 bitov a pridam AES block size
22 thenEncrypt = datetime.now()
23
24 with open('cipher_file', 'wb') as c_file: #ulozim si sifru s inicializacnym vektorom
25     c_file.write(cipher.iv)
26
27 with open('encrypted_file', 'wb') as c_file: #ulozim si zasifrované data "ciphertext"
28     c_file.write(ciphertext)
29
30 with open('cipher_file', 'rb') as c_file: #otvaram si uložený kluc o veľkosti 16 bytov
31     iv = c_file.read(16)
32
33 nowDecrypt = datetime.now()
34 cipher = AES.new(key, AES.MODE_CBC,iv) #sifra na desifrovanie, kedze vieme co pouzivame
35 #vyuzivame nas nacistany IV (inicializacny vektor)
36 plaintext = unpad(cipher.decrypt(ciphertext), AES.block_size)
37 #odstranim padding a desifrujem
38 thenDecrypt = datetime.now()
39
40 text_file = open("output.txt",'w' ,newline='')
41 #zapiseme nas text do suboru
42 text_file.write(plaintext.decode())
43
44
45 deltaEncrypt = thenEncrypt - nowEncrypt
46 deltaDecrypt = thenDecrypt - nowDecrypt
47 print("Encrypt time: " , deltaEncrypt)
48 print("Decrypt time: " , deltaDecrypt)
49
50 input("Press Enter to continue...")
```

Name	Date modified	Type	Size
 app.py	10/7/2021 9:30 PM	Python File	2 KB
 test.txt	10/6/2021 9:01 PM	Text Document	1,048,576 KB

Vidíme ako vyzerá priečink s aplikáciou a testovacím súborom o veľkosti presne 1GB








Začneme spustením „app.py“. Do konzoly jednoducho zadáme názov súboru, ktorý chceme zašifrovať a stlačíme enter.



Konzola nám vypíše čo ako dlho trvalo.

(V tomto prípade je to celkom rýchle, keďže to bežalo na AMD Ryzen 5600, 16GB RAM, 3060ti, 512GB NVMe SSD)

Name	Date modified	Type	Size
 app.py	10/7/2021 9:30 PM	Python File	2 KB
 cipher_file	10/7/2021 9:35 PM	File	1 KB
 encrypted_file	10/7/2021 9:35 PM	File	1,048,577 KB
 output.txt	10/7/2021 9:35 PM	Text Document	1,048,576 KB
 test.txt	10/6/2021 9:01 PM	Text Document	1,048,576 KB

V priečinku nám vznikli tri nové súbory.

- cipher\_file : obsahuje kľúč
- encrypted\_file : náš zašifrovaný súbor
- output.txt : výsledný súbor

**Dôležité info:** Kód v tomto prípade bol napísaný aby sa jednoducho ukázal príklad na šifrovanie a dalo sa to jednoducho zmerať. Šifra je autogenerovaná ale jednoducho sa dá v kóde prepísať. Funkčnosť aplikácie bola ukázaná na šifrovaní a dešifrovaní 1GB súboru (.txt) a jeho následnom outpute to textového súboru pre porovnanie.