Week 3 - 7/10/2022

Exercício 1:

Executando o código abaixo obtemos o ficheiro encriptado *ciphertext.bin*:

```
import os as os
from os import urandom
from binascii import hexlify
from cryptography . hazmat . primitives . ciphers import Cipher , algori

key = os.urandom(32)
print('KEY: ' + key)
iv = os.urandom(16)
print('IV: ' + iv)
cipher = Cipher(algorithms.AES(key),modes.CBC(iv))
encryptor = cipher.encryptor()
ct = encryptor.update(b"A secret message") + encryptor.finalize()
cphFile = open("ciphertext.bin", "wb")
cphFile.write(ct)
```

Exercício 2:

Com a chave e iv impressas pelo código anterior, foi possível desencriptar o ficheiro recorrendo ao seguinte comando:

```
$ openssl aes-256-cbc -d -a -pbkdf2 -in ciphertext.bin -out plain.txt.ne
```

Exercício 3:

3.1) O byte alterado vai afetar (na íntegra) o plaintext resultante da desencriptação do bloco correspondente e, vai afetar em 1 byte o plaintext resultante da desencriptação do 2º bloco, a partir daí, o output mantém-se correto.

3.2) Dada a estrutura do CBC em que após a inicialização com o IV cada bloco serve de IV na desencriptação do seguinte, logo caso o IV e 1º bloco sejam perdidos, o resto do ficheiro pode ser recuperado. Pelo que, o ficheiro não pode ser recuperado na íntegra mas sim truncado (perdem-se os 2 primeiros blocos).

3.3) Caso um dos bits não seja transmitido (ou seja, seja perdido), vai levar ao desalinhamento dos blocos, pelo que, toda a desencriptação vai ser comprometida pois o alinhamento dos blocos é fulcral no processo de desencriptação (dado este esquema ser centrado no processo de XOR).

3.4) Sim, apesar de ser mais simples reencriptar o ficheiro todo, basta reencriptar o ficheiro a partir do bloco alterado (por exemplo, se o ficheiro for alterado a meio no 3º bloco, terá que ser reencriptado do 3º bloco para a frente).

Exercício 4:

A principal diferença de CBC para CTR, é que o CTR tem encriptação e desencriptação independente por blocos, isto é, afetar o ciphertext de um bloco, afeta-o exclusivamente a ele e não aos restantes.

Exercício 5:

Código para resolver o exercício:

```
import itertools as itt
from ciphersuite_aes_weak import *
from string import printable

with open("./group_4.txt", "r") as f:
    data = f.read()

data = bytes.fromhex(data)

with open("possibilities.txt", "wb") as f:
    i = 0
    # Bruteforce das chaves
    for k in itt.product("\x00\x01", repeat=16):
        i += 1
        #debug info
        if i % 100 == 0:
            print(i)
        #teste do decode
        d = dec(''.join(k)).encode('ascii'), data)
        #imprimir apenas quando o output for plausível
        if all(map( lambda x: chr(x) in printable, d)):
            print(d)
            input()
```

Plain Text resultante:

de ha quinze anos alguem de influencia sugerisse que se adoptasse como uma das prioridades no ambito do fomento da economia a producao de desenhos animados isso mesmo desenhos animados da multidao destas criancas e destes adolescentes iria sucessivamente subindo para mais altos voos um vasto numero que se dedicaria a criar com as maos o coracao a inteligencia obras visualmente belas em regime profissional isto e de actividade normal devida boxe mark mcccreath britteknkalantekefr no royal albert hall de londres para o titulo europeu de super ligeiros boxe antonio renzoit steveboyle brit para decidir campeao europeu de ligeiros em rossano italia albertino braga ministro da defesa e ordem interna de sao tome anunciou ontem a participacao de portugal no programa de reestruturacao da direccao nacional de seguranca daquele pais um servico ate agora orientado por tecnicos sovieticos e cubanos uma delegacao dos servicos de informacao portugueses chega a sao tome na proxima terca feira onde vai proferir uma palestra sobre os servicos de informacao nos novos estados democraticos o anuncio da participacao portuguesa na reestruturacao dos servicos de informacao coincide com a divulgacao por miguel trovo