(Applied) Cryptography

Tutorial #2

Manuel Barbosa (mbb@fc.up.pt) Rogério Reis (rvr@dcc.fc.up.pt)

MSI/MCC/MERSI – 2021/2022

1 - Use Python to encrypt a file in CBC mode (follow the example in Tutorial #0 available in Moodle)

2 - Decrypt the file with OpenSSL and check for success

3 - Edit the file to change the value of (but not delete!) one byte and decrypt again.

- What happened?
- Could you recover a file encrypted with CBC if the IV and the first ciphertext block were corrupted or lost?
- Could you recover it if during a satellite transmission one bit of the ciphertext is not delivered?
- Could you modify a byte in the middle of a CBC encrypted file without fully re-encrypting it?

4 - Repeat the exercise with CTR mode. What are the differences?

5 - Download the ciphertext corresponding to your group number.

- The ciphertext was created using the python file `aes_encrypt_weak.py`. Can you find the plaintext?
- Hint: One could use frequency analysis, but that is too much effort.