(Applied) Cryptography

Tutorial #3

Bernardo Portela (bernardo.portela@fc.up.pt) Rogério Reis (rvreis@fc.up.pt)

MSI/MCC/MERSI – 2023/2024

1 - Use Python to encrypt a file in CBC mode and decrypt it. Check for success
(ref: https://cryptography.io/en/latest/hazmat/primitives/symmetric-encryption/).

2 - Repeat this process with OpenSSL
(ref: https://www.openssl.org/docs/man1.1.1/man1/enc.html).

3 - Edit the file to change the value of (but not delete!) one byte and decrypt again.
3.1 - What happened?
3.2 - Could you recover a file encrypted with CBC if the IV and the first ciphertext block were corrupted or lost?
3.3 - Could you recover it if during a satellite transmission one bit of the ciphertext is not delivered?
3.4 - 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?