(Applied) Cryptography

Tutorial #4

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

MSI/MCC/MERSI – 2025/2026

1 - Consider the following polynomials modulo 2:

- $x^3 + x + 1$
- $x^4 + x + 1$
- $x^4 + x^3 + x^2 + 1$

1.1 - Start with different initial (non-zero) states and test the periods. What can you conclude about the LFSRs?

1.2 - Can you ascertain which is the *best* polynomial for an LFSR?

1.3 - Check if any of these is an *irreducible polynomial* in sage. What does this say about the polynomial, when used in LFSRs?

2 - Obtain a Python implementation of RC4 and use it to encrypt a file.

3 - Check if this algorithm is compatible with OpenSSL. use OpenSSL to decrypt the file encrypted with your Python implementation, and check if your Python implementation can decrypt a file encrypted with OpenSSL.

4 - Demonstrate with OpenSSL that ChaCha20 produces a repeated ciphertext if you encrypt the same file with the same key and nonce. Why is this the case?

5 - In questions 2 and 4, compare the size of the plaintext with the size of the ciphertext. What can you conclude with respect, for example, to AES-CTR and AES-CBC modes studied last week.