(Applied) Cryptography

Tutorial #5

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

MSI/MCC/MERSI – 2023/2024

1 - Consider the following polynomials of degree 8:

- $x^8 + x^7 + x^6 + x^2 + 1$
- $x^8 + x^6 + x^4 + 1$
- $x^8 + x^5 + x^3 + x^2 + 1$

1.1 - Implement an LFSR in Python generating values, modulo 31721. Start with intial element 1. How long does it take to find a period (finding the same number again) for each one?

1.2 - Now try it out with different initial elements. 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 from the web and use it to encrypt a file.

3 - Check that this algorithm is compatible with OpenSSL

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

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.