INF143A 2022: Mock exam

Nikolay Kaleyski

May 3, 2022

Problem 1. *Briefly describe how the Playfair cipher operates. Encrypt the plaintext "This is an example" using the Playfair cipher with the key "MOCK-EXAM".*

Problem 2. *Consider the linear recurrence*

$$s_5 = s_3 \oplus s_2 \oplus s_0.$$

1. *Draw the LFSR implementing this recurrence.*
2. *Find the polynomial representation of this LFSR.*
3. *Clock the LFSR starting from* $(1, 0, 1, 0, 0)$ *until it loops.*
4. *Is the polynomial representation primitive?*

Problem 3.

1. *Describe a single round of a Feistel network.*
2. *Explain what changes need to be made to the cipher to perform decryption.*
3. *Give an example of a cipher based on a Feistel network.*

Problem 4. *Consider the finite field* $\mathbb{F}_{2^4}$ *given by the irreducible polynomial*

$$g(x) = x^4 + x^3 + 1.$$

Compute:

1. $(0, 1, 1, 0) + (1, 1, 0, 1)$*;*
2. $(1, 1, 1, 0) \times (0, 1, 1, 0)$*;*
3. $(1, 1, 0, 0)^3$.

Problem 5. *Define the differential uniformity of an* (n, m)*-function* F*. Give a pseudocode procedure for computing the differential uniformity.*

Problem 6. *Compute* $5^{20} \pmod{17}$.

Problem 7. *Let* $(p, q) = (5, 17)$*,* $e = 19$*,* $d = 27$.

1. *Verify that* e *and* d *is valid RSA public key-private key pair.*
2. *Encrypt the message* $x = 32$.
3. *Explain how the message would be decrypted.*

Problem 8. *1. Explain what is a "mode of operation".*

2. Decipher (dis-abbreviate) the following modes of operation: ECB, CBC, OFB.

3. Describe how ECB works.

4. What are some of the major disadvantages of ECB?