M1-AM Cryptology Complementary : Homework

This homework should be prepared individually. Your answers should be written in the form of a pdf file, together with one or several source code for the program requested. You should send all these files in a tar.gz archive attached to an email to `clement.pernet@univ-grenoble-alpes.fr` with subject `[M1 AM] HW <YOUR LAST NAME>` by **Monday May 6th, 2024**. All answers must be justified.

Exercice 1. Implementation of $\mathbb{F}_{256}$

a. Recall how is the field $\mathbb{F}_{256}$ defined. In particular, explain

1. the representation of its elements;
2. the principle of the field addition;
3. the principle of the field multiplication;
4. the principle of the field inversion.

b. Among the following polynomials, which one can you use to construct this field:

1. $P_1 = X^4 + X^3 + X^2 + X + 1$
2. $P_2 = X^4 + X^2 + X + 1$
3. $P_3 = X^4 + X^2 + 1$
4. $P_4 = X^8 + X^4 + 1$
5. $P_5 = X^8 + X^4 + X^3 + X + 1$
6. $P_6 = X^8 + X^4 + X^3 + X^2 + 1$

c. Implement all the field operations in `C`: addition, negation, subtraction, multiplication, inversion, division.

d. We now focus on a Zech-log representation. Explain the principle of this representation.

e. What additional condition should satisfy the polynomial used for the construction of the field? Which one can you use in the list of Question `b`.

f. Implement it.

Exercice 2. A Reed-Solomon code over $\mathbb{F}_{256}$

We want to design and implement a Reed-Solomon code over the field $\mathbb{F}_{256}$

a. The correctoin rate of a code is the ratio t/n between the maximum number of errors t which can be corrected and the length n of the code. The information rate is the ratio k/n between the dimension and the length of the code. For a Reed-Solomon code with correction rate τ, what is the maximum information rate?

b. We want to design a Reed-Solomon code over $\mathbb{F}_{256}$ which code-words can be stored on 16 bytes and correction rate $\tau \geq 0.1$. What is the dimension k maximizing the information rate?

c. Explain how is defined the Reed-Solomon code with the above parameters. Choose the points up to your convenience.

d. Implement in `C` an encoder, computing a code word from a vector of k coefficients of $\mathbb{F}_{256}$.

e. Recall how the extended Euclidean Algorithm applies for the decoding of a Reed-Solomon code.

f. Implement a decoder based on the Euclidean Algorithm for your code.

g. Experiment with these two functions, by e.g. encoding some data, introduce random errors with a probability τ, and then decode and correct these data. Illustrate your experiments as you prefer: compare the input and output data (text, image, etc), draw statistics of the percentage of correctly corrected errors, etc.