Crypto-refresh. Exercise sheet # 2.

Extension fields and discrete probabilities

Exercice 1. The field with 4 elements

a. Write down the addition and multiplication tables of $\mathbb{Z}/4\mathbb{Z}$

b. Write down the addition and multiplication tables of $\mathbb{F}_4$.

c. Is there a isomorphism between both sets ?

Exercice 2. The AES field $\mathbb{F}_{256}$

a. Explain how to define the finite field $\mathbb{F}_{256}$ with 256 elements.

b. Among the following polynomials, only one can be used for this construction, which one is it ?

1. $X - 256$
2. $X^2 + X + 1$
3. $X^{256} + X + 1$
4. $X^4 + X + 1$
5. $X^8 + X^4 + X^3 + X^2 + 1$
6. $X^8 + X^4 + X + 1$

c. Explain how you would prove that the selected polynomial is irreducible (but don't do it).

d. You have to provide a `C` implementation of $\mathbb{F}_{256}$. How would you represent an element ?

e. Write the addition and multiplication functions

Exercice 3. $\mathbb{F}_8$

a. Prove that $Q = x^3 + x + 1$ is a primitive polynomial over $\mathbb{F}_2[x]$.

b. Provide a `C` implementation of $\mathbb{F}_8$ using a Zech log representation

Exercice 4. (Multi)-collisions

In this exercise we let $\mathcal{S}$ be an arbitrary finite set of size N and we denote by $X \twoheadleftarrow S$ the process of drawing from $\mathcal{S}$ uniformly and independently of any other process.

Let $X \twoheadleftarrow \mathcal{S}$, $Y \twoheadleftarrow \mathcal{S}$ and $Z \twoheadleftarrow \mathcal{S}$.

a. Compute $\Pr[(X = x) \wedge (Y = y)]$ for all $(x, y) \in \mathcal{S}^2$

b. Compute $\Pr[X = Y]$.

c. Compute $\Pr[X = Y = Z]$.

Exercice 5. (Non-)uniform Masks

Let X and Y be two independent random variables drawn from $\mathbb{F}_2$ with a uniform law for X and an unknown law for Y.

a. What is the distribution of $X + Y$? (That is compute $\Pr[X + Y = 0]$).

We now draw X and Y independently from a finite group $(\mathbb{G}, +)$ of size N.

b. What is the distribution of $X + Y$.

Remark : the result shown in those two questions is essential in cryptography and is used to justify the security of many constructions.

Exercice 6. Pigeon's birthday

Let $\mathcal{S}$ be again a finite set of size N, which we sample repeatedly by drawing $X_1, X_2, \ldots, X_k$.

a. (Pigeon hole principle) How many samples are necessary to ensure that $\exists i, j \neq i$ s.t. $X_i = X_j$ with probability 1 ?

b. (Birthday paradox) How many samples are approximately needed to ensure that $\exists i, j \neq i$ s.t. $X_i = X_j$ with "high" probability ? (e.g. constant in function of N).