HAI709I : Fondements cryptographiques de la sécurité, Université de Montpellier, 2023

25/09/2023. Lecture 3.

1 A few algebraic facts

Lemma 1. *Let n be an integer number and*

$$f(x) = c_0 + c_1 x + \ldots + c_d x^d$$

be a polynomial with integer coefficient. Assume that $f(a) = 0 \mod n$ for some $a \in \mathbb{Z}/\mathbb{Z}$. Then there exists another polynomial $g(x)$ with integer coefficients such that

$$f(x) = (x - a)g(x) \mod n.$$

Theorem 1. *Let p be a prime number and*

$$f(x) = c_0 + c_1 x + \ldots + c_d x^d$$

be a polynomial with integer coefficient. Then there is at most d different $a_i \in \{0, 1, \ldots p - 1\}$ such that

$$f(a_i) = 0 \mod p.$$

In other words, polynomial of degree $\leq d$ has at most d different roots modulo p.

This theorem can be reformulated as follows: *if $f(x) = c_0 + c_1 x + \ldots + c_d x^d$ has $(d + 1)$ different roots modulo p, then $c_0 = c_1 = \ldots = c_d = 0$.*

Corollary 1. *Let p be a prime number, and*

$$f(x) = c_0 + c_1 x + \ldots + c_d x^d$$

and

$$g(x) = \hat{c}_0 + \hat{c}_1 x + \ldots + \hat{c}_d x^d$$

be two polynomials with integer coefficients, and degrees of these polynomials are not greater than d. Assume that there exists $(d + 1)$ numbers $a_i \in \{0, 1, \ldots, p - 1\}$ such that

$$f(a_i) = g(a_i) \mod p.$$

Then $c_0 = \hat{c}_0 \mod p, \ldots, c_d = \hat{c}_d \mod p$ (i.e., these polynomials are identical modulo p).

In other words, graph of two different *polynomials of degree d cannot have more than d points of intersection (in the arithmetic modulo of $\mathbb{Z}/p\mathbb{Z}$ for a prime p).*

Corollary 2. *Let p be a prime number and $a_1, \ldots, a_d$ be pairwise different numbers from $\{0, \ldots, p - 1\}$ and $b_1, \ldots, b_d$ be arbitrary numbers from the same set. Then there exists a unique array of coefficients $c_0, \ldots c_{d-1} \in \{0, \ldots, p - 1\}$ such that for the polynomial*

$$f(x) = c_0 + c_1 x + \ldots c_{d-1} x^{d-1}$$

we have $f(a_i) = b_i \mod p$. In other words, a polynomial of degree $< d$ is uniquely defined by its values in d points.

(Uniqueness follows from the previous corollary; existence was proved using the Lagrange interpolation formula.)

2 Secret sharing revisited: Shamir's scheme

Let p be a prime number, n ($n < p$) and t ($1 \le t \le n$) be integer numbers. We construct a secret sharing scheme with participants so that every t (or more) participants can reconstruct the secret, but any $t-1$ (or less) participants have no information on the secret.

We assume that a secret is integer number $k \in \{0, 1, \ldots, p-1\}$. To describe the scheme, we fix in advance n pairwise different numbers $a_i \in \{1, \ldots, p-1\}$ (these numbers and p are known to everyone, including the potential attacker). To share the key k *Dealer* chooses at random $c_i \in \{0, 1, \ldots, p-1\}$ for $i = 1, \ldots, t-1$, defines

$$f(x) = k + c_1 x + c_2 x^2 + \ldots + c_{t-1} x^{t-1}.$$

The i-th participant receives the *share* $S_i = f(a_i) \mod p$

In the class we proved that

- given any t values S_i, we can reconstruct the polynomial $f(x)$ (Lagrange interpolation) and find the secret k, which is the lowest term of this polynomial;
- if we know less than t values S_i, then we have no information on the value of k.

This secret sharing scheme is called *Shamir's scheme*.

Exercise 1. We want to share a secret between four participants, A, B, C, D so that the groups

$$\{A, B\},\ \{B, C\},\ \{C, D\}$$

(and all extensions of these sets) know the secret, and every group of participants that does not contain these *minimal authorised sets* get no information on the secret.

(a) Construct some secret sharing scheme for the given classes of authorised and non-authorised groups.

(b)* Construct some secret sharing scheme for the given classes of authorised and non-authorised groups so that the size of each share S_i (measured in bits) is at most $3/2$ of the size of the secret (also measure in bits).

(c)** Prove that the factor $3/2$ is optimal: in this setting we cannot share the secret so that the size of each share is is strictly less than $(3/2) \cdot$ size of the secret.

3 Shannon's entropy and text compression.

Definition 1. Let Code : $\{a_1, \ldots, a_m\} \to \{0, 1\}^*$ be a function mapping each letter a_i to a binary word. We extend this mapping to all words over the same alphabet: for each m-letter word $w_1 \ldots w_n \in \{a_1, \ldots, a_m\}^*$ we let

$$\text{Code}^+(w_1 \ldots w_n) = \text{Code}(w_1) \ldots \text{Code}(w_n)$$

(a concatenation of codes assigned to the letters of the word). We say that this code is *prefix-free* if for every two letters $a_i \neq a_i$ Code(a_i) is not a prefix of Code(a_j).

A prefix-free code is uniquely decodable: given a binary string s we can reconstruct uniquely the sequence of letters $w_{i_1} \ldots w_{i_s}$ such that

$$\text{Code}^+(w_{i_1} \ldots w_{i_s}) = s.$$

(if such a word $w_{i_1} \ldots w_{i_s}$ exists).

If we want to encode text in the most economical way, it is natural to choose short codewords for the most common letters and longer codewords for rarer letters. However, it is not clear exactly how to establish the trade-off between the frequency of a letter and the length of the corresponding codeword. The answer to this question helps to find the concept of entropy.

Definition 2. For a random variable α with n possible values $a_1, \ldots, a_n$ such that $\mathrm{Prob}[\alpha = a_i] = p_i$, we define its Shannon's entropy as

$$H(\alpha) := \sum_{i=1}^{n} p_i \log \frac{1}{p_i}$$

(with the usual convention $0 \cdot \log \frac{1}{0} = 0$).

The value $H(\alpha)$ can be understood as the "amount of information" in a random message α. The following two theorems show that $H(\alpha)$ represents the average number of bits needed to encode a random message $H(\alpha)$.

Theorem 2. *For every distribution of probabilities* $(p_1, \ldots, p_m)$*, if*

$$\text{Code} : \{a_1, \ldots, a_m\} \to \{0,1\}^*$$

is uniquely decodable then

$$\sum_{i=1}^{m} p_i |\text{Code}(a_i)| \geq \sum_{i=1}^{m} p_i \log_2 \frac{1}{p_i}$$

(*the average length of the codewords cannot be less than entropy*).

Theorem 3. *For every distribution of probabilities* $(p_1, \ldots, p_m)$ *there exists a uniquely decodable* Code : $\{a_1, \ldots, a_m\} \to \{0,1\}^*$ *such that*

$$\sum_{i=1}^{m} p_i |\text{Code}(a_i)| < \sum_{i=1}^{m} p_i \log_2 \frac{1}{p_i} + 1$$

(*the average length of the codewords can be made close to the value of entropy, with an overhead smaller than one bit*).

In the class we did not proved Theorem 2. The proof was based on *concavity* of logarithm, which implies the following lemma.

Lemma 2 (Jensen's inequality)**.** *Let* $p_1, \ldots, p_k$ *be positive numbers such that* $\sum p_i = 1$*, and* $x_1, \ldots, x_k$ *be any positive numbers. Then*

$$\sum_{i=1}^{k} p_i \log_2 x_i \leq \log_2 \left(\sum_{i=1}^{k} p_i \cdot x_i \right).$$

Moreover, this inequality terms into equality if and only if $x_1 = \ldots = x_k$*.*

Another tool in the proof of Theorem 2 was the following fact about prefix-free codes.

Lemma 3. *If* $c_1, \ldots, c_k$ *are codewords of a prefix-free code, then*

$$\sum_{i=1}^{k} 2^{-|c_i|} \leq 1.$$

The proof of Theorem 3 is postponed to the next lecture.

We proved the basic properties of Shannon's entropy that follow directly from the definition.

Proposition 1. *For every random variable α distributed on a set of n values*

$$0 \le H(\alpha) \le \log n.$$

Moreover, $H(\alpha) = 0$ if and only if the distribution is concentrated at one point (one probability p_i is equal to 1, and the other p_j for $j \neq i$ are equal to 0), and $H(\alpha) = \log n$ if and only if the distribution is uniform ($p_1 = \ldots = p_n = \frac{1}{n}$).

Idea of the proof: The first inequality is simple. To prove the second one, we used again Jensen's inequality. (In the class we discussed the proof in more detail.) □

References

[1] C. Walter. Arithmétique. Univ. de Nice, 2011. Chapitre 3.
`https://math.unice.fr/~walter/L1_Arith/`

[2] B. Martin. Codage, cryptologie et applications. PPUR presses polytechniques, 2004

[3] V. V. Yaschenko, Cryptography: An Introduction, AMS, 2002

[4] Thomas M. Cover and Joy A. Thomas. Elements of Information Theory. Cover, Thomas M. Elements of information theory. John Wiley & Sons. 1999. [chapter 2]