Crypto 2022. Final exam preparation.

Shannon's entropy

Exercise 1. Prove that for every triple of jointly distributed random variables (X, Y, Z) we have
(a) $H(X, Y|Z) \le H(X|Z) + H(Y|Z)$,
(b) $2H(X, Y, Z) \le H(X, Y) + H(X, Z) + H(Y, Z|X)$,
(c) $H(X) \le H(X|Y) + H(X|Z) + I(Y : Z)$,
(d) $H(X|Z) \le H(X|Y) + H(Y|Z)$.

Exercise 2. There is a pair of random variables X and Y that are distributed on the set $\{1, 2, \dots, n\}$. It is known that $\mathrm{Prob}[X \ne y] = \epsilon$. Prove that

$$H(X|Y) \le 1 + \epsilon \log(n - 1).$$

Hint: It is useful to introduce a new variables

$$Z := \begin{cases} 1, & \text{if } X = Y, \\ 0, & \text{otherwise} \end{cases}$$

and compare $H(X|Y)$ with $H(X|Y, Z) + H(Z)$.

Secret sharing

Exercise 3. We need to share a secret k (which is a bit string of length n) among four participants Alice, Bob, Charlie, Dan in such a way that the minimal groups that known the secret are $\{\text{Alice}, \text{Bob}\}$, $\{\text{Alice}, \text{Charlie}\}$, $\{\text{Alice}, \text{Dan}\}$ (Alice alone as well as Bob, Charlie and Dan together should have no information on the secret).
(a) Construct a secret sharing scheme with the required property.
(b) Construct a secret sharing scheme with the required property so that each share of the secret S_A, S_B , S_C , S_D is a represented by a string of n bits.
(c) Show that in every secret sharing scheme for Alice, Bob, Charlie, Dan the space of shares for Alice consists of at least 2^n different values (i.e., we cannot give to Alice less than n bits of information.

Exercise 4. We need to share a secret k (which is a bit string of length n) among four participants Alice, Bob, Charlie, Dan in such a way that the minimal groups that known the secret are

$$\{\text{Alice}, \text{Bob}\},\ \{\text{Alice}, \text{Charlie}\},\ \{\text{Alice}, \text{Dan}\},\ \{\text{Bob}, \text{Charlie}, \text{Dan}\}.$$

(a) Construct a secret sharing scheme with the required property.
(b)* Show that in this case in every secret sharing scheme one of the participants must receive a share with strictly more than 2^n possible values (i.e., we cannot give to each participant only n bits of information),

Shamir's secret sharing and polynomials the modular arithmetic.

Exercise 5. Let a_0, a_1, a_2, a_3 be integer numbers, and

$$f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3.$$

It is know that

$$f(1) = 0 \mod 31,\ f(2) = 0 \mod 31,\ f(3) = 0 \mod 31,\ f(4) = 30 \mod 31.$$

Find $a_0 \mod 31$.

Exercise 6. Find a triple of numbers a_0, a_1, a_2 (not all congruent to zero modulo 10) such that the polynomial $f(x) = a_0 + a_1 x + a_2 x^2$ has at least three different roots in $\mathbb{Z}/10\mathbb{Z}$.

Exercise 7. For the following n find without a computer a number k such that $100 \cdot k = 1 \mod n$.
(a) $n = 61$; (b) $n = 599$; (c) $n = 1009$.

Exercise 8. It is known that the number $p = 5\,104\,051$ is prime.
(a) Show without using a computer that the number $g_1 = 3$ the numbers

$$g,\ (g^2 \mod p),\ (g^3 \mod p), \ldots$$

cover the whole set $\{1, 2, \ldots, p-1\}$. *Hint:* compute $g_1^{(p-1)/2} \mod p$.
(b) Show without using a computer that the same property is not true for the number $g_2 = 9$.
(c) Let $g_3 = 522904$. Count the number of different elements in the list

$$\{1, 2, \ldots, p-1\}.$$

(d) Using (c), find without a computer a number x such that

$$g_3^x = 4581146 \mod p.$$

Moralité de la fable : if the subgroup generated by g is small, then the problem of discrete logarithm with the base g is simple.