Topics in Algebra: Cryptography - Blatt 6

http://www.mat.univie.ac.at/~gagt/crypto2019

Goulnara Arzhantseva
goulnara.arzhantseva@univie.ac.at

Martin Finn-Sell
martin.finn-sell@univie.ac.at

1 Exercises

Question 1. Which of the following binary codes are linear codes?

- $C_1 = \{00, 01, 10, 11\}$,
- $C_2 = \{000, 011, 101, 110\}$,
- $C_3 = \{00000, 01101, 10110, 11011\}$,
- $C_4 = \{101, 111, 011\}$,
- $C_5 = \{000, 001, 010, 011\}$,
- $C_6 = \{0000, 1001, 0110, 1110\}$.

Question 2. Let C be a ternary code (i.e a code over the field of three elements) generated by the matrix

$$A = \begin{pmatrix} 0 & 1 & 2 & 1 \\ 2 & 0 & 1 & 1 \end{pmatrix}$$

.

a) List all the codevectors of C and find the minimal Hamming length $h(C)$ by inspection. Deduce that C is a perfect code.

b) Find a generator matrix of C in standard form.

Question 3. Let C and D be linear codes over $\mathbb{F}_q$, the field with q elements where q is prime. Define:

$$C + D = \{c + d \mid c \in C, d \in D\}.$$

Show that $C + D$ is a linear code.

Question 4. A code C is called **systematic** on k-positions (and the symbols on these positions are called information symbols) if $\|C\| = q^k$ and there is exactly one codeword for ever possible choice of coordinates in these k positions. Show that C has minimum distance $d = n - k + 1$.

Question 5. Prove that it is not possible to find 32 binary words, each of length 8 bits, such that each word differs from every other word in at least 3 places.

Question 6. Suppose that Alice is using the ElGamal signature scheme. In order to save time in generating random numbers k such that are used to sign messages, Alice choses an initial random value k_0 and then signs the i^{th} message using the value $k_i = k_0 + 2i \mod p - 1$ (note that this means $k_i = k_{i-1} + 2 \mod p - 1$).

i) Suppose that Bob observes two consecutive signed messages

$$(x_i, sig(x_i, k_i))$$

and

$$(x_{i+1}, sig(x_{i+1}, k_{i+1})).$$

Describe how Bob can easily compute Alice's secret key a given this information without solving an instance of the discrete logarithm problem. Is this method independent of i?

ii) What if random values follow another recusive relation - would this still allow us to do as above?

iii) (Practical) Suppose that the parameters of the scheme are $p = 28703$ and $\alpha = 5, \beta = 11339$, and the two messages observed by Bob are:

$$x_i = 12000, sig(x_i, k_i) = (26530, 19862)$$
$$x_{i+1} = 24567, sig(x_{i+1}, k_{i+1}) = (3081, 7604).$$

Find the value of a using the attack from part i).