Advanced Cryptography Exercises I

Mihai Prunescu

1 Permutations

Exercise 1 *According to the Theorem of Cayley there is an embedding of the group S_3 in the group S_6. Find the image of the transposition* (1 2) *by this embedding.*

As the group S_3 has 6 elements, we denote them by 1 = the identity, 2 = (1 2), 3 = (1 3), 4 = (2 3), 5 = (1 2 3) and 6 = (1 3 2). The action of (1 2) by multiplication $x \rightsquigarrow (1\ 2)x$ can be expressed as follows:

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & (1\ 2) & (1\ 3) & (2\ 3) & (1\ 2\ 3) & (1\ 3\ 2) \\ (1\ 2) & 1 & (1\ 3\ 2) & (1\ 2\ 3) & (2\ 3) & (1\ 3) \\ 2 & 1 & 6 & 5 & 4 & 3 \end{array}$$

$$(1\ 2)(1\ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2)$$

$$(1\ 2)(2\ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3)$$

$$(1\ 2)(1\ 2\ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\ 3)$$

$$(1\ 2)(1\ 3\ 2) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3)$$

$$(1\ 2) \rightsquigarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 5 & 4 & 3 \end{pmatrix} = (1\ 2)(3\ 6)(4\ 5).$$

Exercise 2 *Prove the identity:*

$$(k\ k+1) = (1\ 2\ \ldots\ n)^{k-1}(1\ 2)(1\ 2\ \ldots\ n)^{1-k}.$$

The proof works by induction. For $k = 1$ we see that the identity yields (1 2) = (1 2), which is trivially true. The step $k \rightsquigarrow k+1$ would be done, if we know that:

$$(1\ 2\ \ldots\ n)(k\ k+1)(n\ n-1\ \ldots\ 1) = (k+1\ k+2).$$

In order to prove this last identity, consider an object $\alpha \neq k+1, k+2$. Then:

$$(n\ n-1\ \ldots\ 1)(\alpha) = \alpha - 1 \neq k, k+1$$

$$(1\ 2\ \ldots\ n)(\alpha - 1) = \alpha.$$

For $\alpha = k+1$ one has:

$$k+1 \to k \to k+1 \to k+2.$$

For $\alpha = k+2$ one has:

$$k+2 \to k+1 \to k \to k+1.$$

Exercise 3 *For $1 \leq i < j \leq n$ prove the identity:*

$$(i\ j) = (j-1\ j)(j-2\ j-1)\dots(i+1\ i+2)(i\ i+1)(i+1\ i+2)\dots(j-2\ j-1)(j-1\ j).$$

Every $\alpha < i$ is not moved either by the left hand side, nor by the right hand side.
For $\alpha = i$, the right hand side works as follows:

$$i \to i+1 \to i+2 \to \dots \to j-1 \to j.$$

For $i < \alpha < j$, the right hand side does:

$$\alpha \to \alpha+1 \to \alpha.$$

For $\alpha = j$, the right hand side works as follows:

$$j \to j-1 \to j-2 \to \dots \to i+1 \to i.$$

Finally, $\alpha > j$ is not moved by any transposition.

Exercise 4 *Show that every permutation can be decomposed in a product of disjoint cycles by working out the following example:*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 6 & 1 & 2 & 4 \end{pmatrix}.$$

Indeed:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 6 & 1 & 2 & 4 \end{pmatrix} = (1\ 3\ 6\ 4)(2\ 5).$$

Exercise 5 *Show that every permutation can be decomposed in a product of transpositions by working out the following example:*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 6 & 1 & 2 & 4 \end{pmatrix}.$$

$$(1\ 3)\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 6 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 6 & 3 & 2 & 4 \end{pmatrix}.$$

$$(2\ 5)\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 6 & 3 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 6 & 3 & 5 & 4 \end{pmatrix}.$$

$$(3\ 6)\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 6 & 3 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 6 & 5 & 4 \end{pmatrix}.$$

$$(4\ 6)\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 6 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = id.$$

In conclusion,

$$(4\ 6)(3\ 6)(2\ 5)(1\ 3)\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 6 & 1 & 2 & 4 \end{pmatrix} = id,$$

and it follows that:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 6 & 1 & 2 & 4 \end{pmatrix} = (1\ 3)(2\ 5)(3\ 6)(4\ 6).$$

Exercise 6 *Conclude that every finite permutation group is generated by two elements, more exactly that:*

$$S_n = \langle (1\ 2), (1\ 2\ \ldots\ n) \rangle.$$

We have seen that every permutation is a product of transpositions $(i\ j)$. Every transposition $(i\ j)$ is a product of transpositions of the form $(k\ k+1)$. Finally, every transposition of the form $(k\ k+1)$ is a product of the transposition $(1\ 2)$ and powerds of the cycle $(1\ 2\ \ldots\ n)$.

Exercise 7 *Show the following identity:*

$$(1\ 2\ \ldots\ n) = (1\ 2)(2\ 3)\ldots(n-2\ n-1)(n-1\ n).$$

Just figure out how every object 1, 2, ..., n does transform in any of the sides of this equality.

Observation: A better idea to decompose permutations in transpositions: first decompose them in disjoint cycles, and then decompose every cycle in transpositions.

Exercise 8 *Compute the elements generated by the cyclic permutation* $(1\ 2\ 3\ 4\ 5\ 6)$.

$$(1\ 2\ 3\ 4\ 5\ 6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}.$$

$$(1\ 2\ 3\ 4\ 5\ 6)(1\ 2\ 3\ 4\ 5\ 6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix} = (1\ 3\ 5)(2\ 4\ 6).$$

$$(1\ 2\ 3\ 4\ 5\ 6)(1\ 3\ 5)(2\ 4\ 6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix} = (1\ 4)(2\ 5)(3\ 6).$$

$$(1\ 2\ 3\ 4\ 5\ 6)(1\ 4)(2\ 5)(3\ 6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 3 & 4 \end{pmatrix} = (1\ 5\ 3)(2\ 6\ 4).$$

$$(1\ 2\ 3\ 4\ 5\ 6)(1\ 5\ 3)(2\ 6\ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix} = (1\ 6\ 5\ 4\ 3\ 2) = (6\ 5\ 4\ 3\ 2\ 1).$$

$$(1\ 2\ 3\ 4\ 5\ 6)(6\ 5\ 4\ 3\ 2\ 1) = id.$$

Exercise 9 *All cycles generated by the cycle* $(1\ 2\ 3\ 4\ 5)$ *are cycles of length* 5.

$$(1\ 2\ 3\ 4\ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}.$$

$$(1\ 2\ 3\ 4\ 5)(1\ 2\ 3\ 4\ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix} = (1\ 3\ 5\ 2\ 4).$$

$$(1\ 2\ 3\ 4\ 5)(1\ 3\ 5\ 2\ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix} = (1\ 4\ 2\ 5\ 3).$$

$$(1\ 2\ 3\ 4\ 5)(1\ 4\ 2\ 5\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix} = (1\ 5\ 4\ 3\ 2) = (5\ 4\ 3\ 2\ 1).$$

$$(1\ 2\ 3\ 4\ 5)(5\ 4\ 3\ 2\ 1) = id.$$

This happens for all cyclic permutation over a prime number p of objects. This is an immediate consequence of the fact that all elements of a cyclic group of order p, which are different from 1, have order p as well.

Exercise 10 *Let $\sigma \in S_n$ be some permutation and $(a_1, \ldots, a_k)$ be a cycle. Show that:*

$$\sigma(a_1, \ldots, a_k)\sigma^{-1} = (\sigma a_1, \ldots, \sigma a_k).$$

In the following lines, x is different from $a_1, \ldots, a_k$. Indeed,

$$\sigma(a_1, \ldots, a_k)\sigma^{-1} = \sigma(a_1, \ldots, a_k)\begin{pmatrix} \sigma a_1 & \ldots & \sigma a_k & \sigma x \\ a_1 & \ldots & a_k & x \end{pmatrix} =$$

$$= \sigma\begin{pmatrix} \sigma a_1 & \ldots & \sigma a_k & \sigma x \\ a_2 & \ldots & a_1 & x \end{pmatrix} = \begin{pmatrix} \sigma a_1 & \ldots & \sigma a_k & \sigma x \\ \sigma a_2 & \ldots & \sigma a_1 & \sigma x \end{pmatrix} = (\sigma a_1, \ldots, \sigma a_k).$$

Exercise 11 *Let G be a finite group with n elements and $c : G \to S_n$ the embedding given by Cayley's Theorem. Find all finite groups G such that $c(G) \trianglelefteq S_n$.*

This is a sketch of proof, based on some knowledge from outside this course. According to the previous exercise, two permutations are conjugated if and only if they have similar decompositions in disjoint cycles. It is not hard to prove that all permutations with similar cycle decomposition built a conjugation class in S_n. Normal subgroups in S_n are unions of such conjugation classes.

If $n = 1$, the group $G = \{1\}$ is the only one group with one element. But $|S_1| = 1$ so the Cayley embedding is surjective, $c(\{1\}) = S_1 \trianglelefteq S_1$.

Also, if $n = 2$, the group $G = \mathbb{Z}_2$ is the only one group with one element. Again $|S_2| = 2$ so the Cayley embedding is surjective, $c(\mathbb{Z}_2) = S_2 \trianglelefteq S_2$.

Things are different at $n = 3$. On one hand, there is only one group with 3 elements, and this is $\mathbb{Z}_3 = \{0, 1, 2\}$. Its Cayley embedding is given by:

$$\begin{aligned} c(0) &= id \\ c(1) &= (0, 1, 2) \\ c(2) &= (0, 2, 1) \end{aligned}$$

The group S_3 has 6 elements partitioned in three classes of permutations as follows: $C_1 = \{id\}$, $C_2 = \{(0, 1), (1, 2), (0, 2)\}$ and $C_3 = \{(0, 1, 2), (0, 2, 1)\}$. As $c(\mathbb{Z}_3) = C_1 \cup C_3$, we have $c(\mathbb{Z}_3) \trianglelefteq S_3$.

For $n = 4$, there are two groups with 4 elements, $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$. On the other hand the group S_4 has 24 elements, partitioned in classes of conjugation as follows: $C_1 = \{id\}$, C_2 consists of the 6 transposions (a, b), C_3 consists of the 3 products of disjoint transpositions $(a, b)(c, d)$, C_4 consists of the 8 cycles of length 3 of the form (a, b, c) and C_5 consists of the 6 cycles of length 4 of the form (a, b, c, d).

The group $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ has the following Cayley embedding:

$$\begin{aligned} c(0) &= id \\ c(1) &= (0, 1, 2, 3) \\ c(2) &= (0, 2)(1, 3) \\ c(3) &= (0, 3, 2, 1) \end{aligned}$$

As $c(\mathbb{Z}_4)$ is not a union of conjugation classes of S_4, $c(\mathbb{Z}_4)$ is not a normal subgroup of S_4.

The group $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0) = 0, (1,0) = \alpha, (0,1) = \beta, (1,1) = \gamma\}$ has the following Cayley embedding:

$$\begin{aligned} c(0) &= id \\ c(\alpha) &= (0,\alpha)(\beta,\gamma) \\ c(\beta) &= (0,\beta)(\alpha,\gamma) \\ c(\gamma) &= (0,\gamma)(\alpha,\beta) \end{aligned}$$

We see that $c(\mathbb{Z}_2 \times \mathbb{Z}_2) = C_1 \cup C_3$ so $c(\mathbb{Z}_2 \times \mathbb{Z}_2) \trianglelefteq S_4$.

For $n \geq 5$ it is known that S_n has only one proper normal subgroup, which is the alternative group $A_n = Ker\ \varepsilon$ and has $n!/2$ elements. But for $n \geq 5$, $n!/2 > n$ so there is no finite group with n elements that embeds in S_n as a normal subgroup. To sum up, we have proved the following:

Theorem: *The only four finite groups G which embed in $S(G)$ as normal subgroups over the Cayley embedding are: $\{1\}$, $\mathbb{Z}_2$, $\mathbb{Z}_3$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$.*

Exercise 12 *An encryption machine C works over the 26-letter alphabet. It has the property that for all $n \in \mathbb{N}$ there is a permutation $\sigma \in S_n$ such that if the clear text has n characters, the machine applies σ and produces the encrypted message. The corresponding decryption machine D finds out n an applies σ^{-1} to decrypt. An agent finds an encrypted message but can use only the machine C. How can he manage to decrypt the message?*

Solution 1: Let m be the clear text and $\sigma(m)$ the encrypted message. He keeps re-encryprting and produces the sequence $\sigma^2(m)$, $\sigma^3(m)$, $\sigma^4(m)$ and so on. As every permutation has a finite order, in this sequence appears the clear message m that can be recognized because it makes sense.

Solution 2: What can we do if the clear text does not make sense to be recognized as such, as it is for example a very long licence key or password? In this case we can produce a text to find out the positions $\sigma(1)$, $\sigma(2)$, ..., $\sigma(25)$, for example by encrypting:

$$ABC \ldots XYZZZ \ldots Z$$

In a second try we find out the values $\sigma(26)$, $\sigma(27)$, ..., $\sigma(50)$ by encrypting:

$$ZZZ \ldots ZABC \ldots XYZZZ \ldots Z$$

where ther first Z-block has length 25. In a finite number of tries the agent finds out the permutation σ, compute σ^{-1} and computes m.

Exercise 13 *Let $(G, \cdot, 1)$ be a commutative group with 900 elements. G contains elements a, b and c such that $a^{450} \neq 1$, $b^{300} \neq 1$ and $c^{180} \neq 1$. Show that the group G is cyclic.*

Hint: show that the element $g = a^{225}b^{100}c^{36}$ generates G.

We observe that $900 = 4 \times 9 \times 25$, and further that $450 = 900/2$, $300 = 900/3$ and $180 = 900/5$. Also, $(a^{225})^4 = a^{900} = 1$, so $\text{ord}(a^{225}) = 4$ because $a^{450} \neq 1$. Similarly, $(b^{100})^9 = b^{900} = 1$, so $\text{ord}(b^{100}) = 9$ because $b^{300} \neq 1$ and $(c^{36})^{25} = c^{900} = 1$, so $\text{ord}(c^{36}) = 25$ because $c^{180} \neq 1$. As the orders 4, 9 and 25 are relatively prime, $\text{ord}(g) = 4 \times 9 \times 25 = 900$, so g generates G and G is cyclic.

2 Rings and fields

Exercise 14 *Describe the group of units of the ring $\mathbb{Z}_{12}$.*

$$\mathbb{Z}_{12} \simeq \mathbb{Z}_4 \times \mathbb{Z}_3.$$

$$\mathbb{Z}_{12}^{\times} \simeq \mathbb{Z}_4^{\times} \times \mathbb{Z}_3^{\times} = \{1 \bmod 4, 3 \bmod 4\} \times \{1 \bmod 3, 2 \bmod 3\} =$$

$$= \{(1,1),(1,2),(3,1),(3,2) \mid \in \mathbb{Z}_4 \times \mathbb{Z}_3\} = \{1,5,7,11 \mid \in \mathbb{Z}_{12}\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2.$$

This is Klein's Vierergruppe. We observe that indeed $5^2 = 7^2 = 11^2 = 1 \bmod 12$.

Exercise 15 *Find a generator of the group $\mathbb{Z}_{11}^{\times}$. How many generators are there, and who are they?*

The group of units is cyclic because $\mathbb{Z}_{11}$ is a field. We compute successive powers of 2 mod 11 and we get:

$$2, 4, 8, 5, 10, 9, 7, 3, 6, 1.$$

It follows that $(\mathbb{Z}_{11}^{\times}, \cdot, 1) = \langle 2 \bmod 11 \rangle$. We know that $(\mathbb{Z}_{11}^{\times}, \cdot) \simeq (\mathbb{Z}_{10}, +)$ as cyclic groups. We already found an isomorphism $f : \mathbb{Z}_{11}^{\times} \to \mathbb{Z}_{10}$, putting $f(2) = 1$ and $f(2^k) = k \bmod 10$. This isomorphism is the discrete logarithm for this field. Now the elements which generate $(\mathbb{Z}_{10}, +)$ are exactly $\mathbb{Z}_{10}^{\times} = \{1, 3, 7, 9\}$, so the generators of $\mathbb{Z}_{11}^{\times}$ are $2^1 = 2$, $2^3 = 8$, $2^7 = 7$ and $2^9 = 6$. The powers of 8 are indeed:

$$8, 64 = 9, 72 = 6, 48 = 4, 32 = 10, 80 = 3, 24 = 2, 16 = 5, 40 = 7, 56 = 1 \bmod 11$$

Exercise 16 *Find a representation of the field $\mathbb{F}_9$.*

The first step towards such a representation is to find an irreducible polynomial over the field $\mathbb{F}_3 = \mathbb{Z}_3$. The polynomial $X^2 + 1$ has no root modulo 3. If reducible, it would split in two factors of degree 1, which cannot be the case. So $\mathbb{F}_9 = \mathbb{Z}_3[\omega]$ with $\omega^2 = 2$.

$$\mathbb{F}_9 = \{0, 1, 2, \omega, \omega + 1, \omega + 2, 2\omega, 2\omega + 1, 2\omega + 2\}.$$

The powers of ω are: $\omega^2 = 2$, $\omega^3 = 2\omega$, $\omega^4 = 2\omega^2 = 1$. So ω does not generate the cyclic multiplicative group. Let us try with $\omega + 1$. Its powers are: $\omega^2 + 2\omega + 1 = 2\omega$, $2\omega^2 + 2\omega = 2\omega + 1$, $2\omega^2 + 1 = 2$, $2\omega + 2$, $2(\omega + 1)^2 = 4\omega = \omega$, $\omega^2 + \omega = \omega + 2$, $\omega^2 + 2 = 1$. So $\mathbb{F}_9^{\times} = \langle \omega + 1 \rangle$ is cyclic.

Exercise 17 *Find a representation of the field $\mathbb{F}_8$.*

The polynomial $X^3 + X + 1$ has no root modulo 2. If reducible, a degree 3 polynomial should have a linear factor, which is not the case. So the polynomial is irreducible. It follows that $\mathbb{F}_8 = \mathbb{F}_2[\omega]$ with $\omega^3 = \omega + 1$.

$$\mathbb{F}_8 = \{0, 1, \omega, \omega + 1, \omega^2, \omega^2 + 1, \omega^2 + \omega, \omega^2 + \omega + 1\}$$

The element ω proves to be a generator of the multiplicative group, as the sequence o powers is: ω, ω^2, $\omega + 1$, $\omega^2 + \omega$, $\omega^2 + \omega + 1$, $\omega^2 + 1$, 1.

Exercise 18 *The chinese captain of a ship is very old but wants to keep secret his age. Curious crewmen inspect his personal letters and find out different hints about his age.*

- One year ago the age of the captain was divisible by 3*.*

- In two years, his age will be a multiple of 5*.*

- In four years, his age will be a multiple of 7*.*

How old is the captain?

We first write down the conditions,

$$\begin{aligned} x-1 &= 0 \bmod 3, \\ x+2 &= 0 \bmod 5, \\ x+4 &= 0 \bmod 7, \end{aligned}$$

meaning:

$$\begin{aligned} x &= 1 \bmod 3, \\ x &= 3 \bmod 5, \\ x &= 3 \bmod 7. \end{aligned}$$

As 3, 5 and 7 are pairwise relatively prime, this is a case for the Chinese Remainder Theorem.

$$x = (1 \cdot 5 \cdot 7 \cdot (35^{-1} \bmod 3) + 3 \cdot 3 \cdot 7 \cdot (21^{-1} \bmod 5) + 3 \cdot 3 \cdot 5 \cdot (15^{-1} \bmod 7)) \bmod 105.$$

We easily compute that:

$$\begin{aligned} 35^{-1} \bmod 3 &= 2^{-1} \bmod 3 = 2, &(1)\\ 21^{-1} \bmod 5 &= 1^{-1} \bmod 5 = 1, &(2)\\ 15^{-1} \bmod 7 &= 1^{-1} \bmod 7 = 1. &(3) \end{aligned}$$

It follows that:

$$x = (70 + 63 + 45) \bmod 105 = 178 \bmod 105 = 73.$$

Exercise 19 *Find all irreducible polynomials of degree* 5 *over* $\mathbb{F}_2$.

We observe that the irreducible polynomials of degree 1 are X and $X+1$ and that X^2+X+1 is the only one irreducible polynomial of degree 2. We observe that $f_1(X) = X^5 + X^2 + 1$ is not divisible by any of those three polynomials, so it is irreducible. Further we observe that:

$$f(X) \text{ irreducible} \to f(X+1) \text{ irreducible}$$
$$f(X) \text{ irreducible} \to X^5 f(\tfrac{1}{X}) \text{ irreducible}$$

$$f_2(X) = f_1(X+1) = (X+1)^5+(X+1)^2+1 = X^5+X^4+X+1+X^2+1+1 = X^5+X^4+X^2+X+1,$$
$$f_3(X) = X^5 f_1(\frac{1}{X}) = X^5 + X^3 + 1,$$

are both irreducible. Moreover,

$$f_4(X) = f_3(X+1) = X^5 + X^4 + X + 1 + X^3 + X^2 + X + 1 + 1 = X^5 + X^4 + X^3 + X^2 + 1,$$
$$f_5(X) = X^5 f_2(\frac{1}{X}) = X^5 + X^4 + X^3 + X + 1,$$
$$f_6(X) = X^5 f_4(\frac{1}{X}) = X^5 + X^3 + X^2 + X + 1,$$

are all irreducible. But as $\mathbb{F}_{32} \setminus \mathbb{F}_2$ has exactly $30 = 6 \times 5$ elements, those 6 polynomials are all irreducible polynomials of degree 5.

Exercise 20 *Let* $|\mathcal{A}| = 26$ *and blocks of length* 2*, so that the encryption reads* $x_1x_2 \rightsquigarrow y_1y_2$*. We identify* $\mathcal{A}$ *with* $\mathbb{Z}_{26}$*. The operation:*

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 6 & 2 \\ 5 & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \bmod 26$$

is not good to perform a linear encryption because $\gcd(26, \det(M)) = 2$*, so* M *is not invertible. Find different blocks* x_1x_2 *and* $x_1'x_2'$ *with the same encryption* y_1y_2*.*

Indeed, the pairs $(x, 0)$ and $(x, 13)$ have the same encryption $(6x, 5x)$ mod 26.

Exercise 21 *For the operation:*

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 6 & 1 \\ 5 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \bmod 26$$

find the rule of decryption.

As the matrix has the determinant 1, it is invertible. The inverse is:

$$\begin{pmatrix} 1 & -1 \\ -5 & 6 \end{pmatrix}$$

Modulo 26 this means:

$$\begin{pmatrix} 1 & 25 \\ 21 & 6 \end{pmatrix}$$

Exercise 22 *Show that the group $\mathbb{Z}_{2^k}^\times$ is cyclic if and only if $k \in \{1, 2\}$.*

Indeed $\mathbb{Z}_2^\times = \{1\} = \langle 1 \rangle$ and $\mathbb{Z}_4^\times = \{1, 3\} = \langle 3 \rangle$.
$\mathbb{Z}_8^\times = \{1, 3, 5, 7\}$ is not cyclic, because all elements have order 1 or 2. $3^2 = 5^2 = 7^2 = 1$.
For $k \geq 3$, $\mathbb{Z}_{2^k}^\times$ is not cyclic, because there is a surjective homomorphism of rings $f : \mathbb{Z}_{2^k} \to \mathbb{Z}_8$ given by $f(x) = x \bmod 8$. If $k \geq 3$, $\mathbb{Z}_{2^k}^\times$ was cyclic, so was also $\mathbb{Z}_8^\times$, which is not the case.

Exercise 23 *Consider a random $m \times m$ matrix over $\mathbb{F}_2$.*
- Compute the probability that the matrix is invertible.
- Show that this probability has a limit bigger than $1/4$ as $m \to \infty$.

$$\frac{1}{2^{m^2}} \prod_{k=0}^{m-1} (2^m - 2^k) = \prod_{k=1}^{m} \left(1 - \frac{1}{2^k}\right)$$

It is interesting, that this sequence has a limit bigger than $1/4$:

$$\frac{1}{p} = \prod_{i=0}^{m-1} \frac{2^m}{2^m - 2^i} = \prod_{i=0}^{m-1} \frac{2^{m-i}}{2^{m-i} - 1} \leq \prod_{i=1}^{m} \frac{2^i}{2^i - 1} = 2 \prod_{i=2}^{m} (1 + \frac{1}{2^i - 1}).$$

This implies:

$$\ln \frac{1}{2p} \leq \sum_{i=2}^{m} (1 + \frac{1}{2^i - 1}) \leq \sum_{i=2}^{m} \frac{1}{2^i - 1} \leq \sum_{i=2}^{m} \frac{1}{\frac{3}{4} \cdot 2^i} < \frac{4}{3} \sum_{i=2}^{\infty} \frac{1}{2^i} = \frac{4}{3} \cdot \frac{1}{2} = \frac{2}{3}.$$

In conclusion $\frac{1}{2p} < \mathrm{e}^{\frac{2}{3}} < 2$ so $p > \frac{1}{4}$.

3 Symmetric cryptography

Exercise 24 *Consider the 32-letters alphabet $\mathcal{A}$, starting with A, B, C, ..., Z and ending with $\breve{A}$, $\hat{A}$, $\hat{I}$, Ş, Ţ, □. The alphabet is encoded using the binary strings* 00000, 00001, 00010, ..., 11111. *Let $k \in \{0, 1\}^{25}$ be a key for One Time Pad modulo 2 such that:*

$$Enc_k(ELENA) = MARIA.$$

- *Find out* $Enc_k(MARIA)$.

- *Compute* $Enc_k(k)$.

- *Compute the key* k.

Letter-wise, $ELENA \oplus k = MARIA$, so $MARIA \oplus k = ELENA$, so $Enc_k(MARIA) = ELENA$. Trivially $Enc_k(k) = AAAAA$. Also,

$$k = MARIA \oplus ELENA = 01100|00000|10001|01000|00000 \oplus 00100|01011|00100|01101|00000 =$$

$$= 01000|01011|10101|00101|00000 = ILVFA.$$

Exercise 25 *Consider the* 32*-letters alphabet* $\mathcal{A}$*, starting with A, B, C, . . . , Z and ending with* Ă*,* Â*,* Î*,* Ş*,* Ţ*,* □*. Let* $k \in \mathcal{A}^5$ *be a key for One Time Pad modulo* 32 *such that:*

$$Enc_k(ELENA) = MARIA.$$

- *Find out* $Enc_k(MARIA)$.

- *Compute* $Enc_k(k)$.

- *Compute the key* k.

In this case we must first compute the key.

$$k = MARIA - ELENA = (12, 0, 17, 8, 0) - (4, 11, 4, 13, 0) =$$

$$= (8, -11, 13, -5, 0) = (8, 21, 13, 27, 0) \bmod 32.$$

Translated in letters, this is IVNÂA.

$$Enc_k(MARIA) = (12, 0, 17, 8, 0) + (8, 21, 13, 27, 0) =$$

$$= (20, 21, 30, 3, 0) \bmod 32.$$

Translated in letters, this is UVŞCA.

$$Enc_k(k) = 2 \cdot (8, 21, 13, 27, 0) = (16, 10, 26, 22, 0) \bmod 32.$$

Exercise 26 *Relatively to the event that one attacker finds out* $Enc_k(k)$*, which of the following systems is more secure and which is less secure?*

- *OTP modulo* 2.

- *OTP modulo* 31.

- *OTP modulo* 32.

OTP modulo 31 is the least secure, because 2 is invertible modulo 31, and $2^{-1} \bmod 31 = 16$. So:

$$k = 2^{-1} Enc_k(k) \bmod 31 = 16 Enc_k(k) \bmod 31,$$

is very easy to find out.

OTP modulo 2 and OTP modulo 32 are at the first sight equally secure. For key of length n, in OTP modulo 2 the only one information provided by $Enc_k(k) = 0^n$ is the length of the key. So there are 2^n possible keys. In OTP modulo 32, every solvable equation $2x = a$ has two solutions x_1 and $x_2 = x_1 + 16 \bmod 32$. So for keys of length n we get also 2^n possible keys for the same $Enc_k(k)$.

But recall the last exercise. In order to encode the word $ELENA$ in OTP modulo 2 we need keys of length 25 while in OTP modulo 32 we need keys of length 5. So by accidental deconspiration of $Enc_k(k)$, in OTP modulo 2 we need 2^{25} many tries to find the right key, while in OTP modulo 32 we need only 2^5 tries. So OTP modulo 32 is more secure relatively to this test then OTP modulo 31 but less secure then OTP modulo 2.

Exercise 27 *Let S be a finite set and $f : S \to S$ an arbitrary function.*

- Show that there is a maximal subset $S_0 \subseteq S$ such that $f(S_0) = S_0$.

- Deduce that $f|S_0$ is a permutation of S_0.

- Conclude that the edges $(x, f(x))$ with $x \in S_0$ build a finite union of closed cycles and the edges $(x, f(x))$ with $x \in S \setminus S_0$ build a finite union of descdendent trees with roots in S_0.

Indeed, for every $x \in S$, the sequence x, $f(x)$, $f^2(x)$, $f^3(x)$, ..., is ultimately periodic. The periodic part builds a cycle. If one starts with an element, which is not in the previous sequence, one finds eventually another cycle. The initial part of the sequences, before they become periodic, build the trees.

Exercise 28 *Show that the polynomial $X^4 + X + 1$ is irreducible over $\mathbb{F}_2$ and primitive by constructing the associated linear feed-back register.*

We show irreducibility directly. The polynomial has no solutions in $\mathbb{F}_2$, so it has no degree 1 factors. The unique irreducible polynomial of degree 2 is $X^2 + X + 1$. One has $X^4 + X + 1 = X(X + 1)(X^2 + X + 1) + 1$. So $X^4 + X + 1$ is irreducible over $\mathbb{F}_2$. The associated matrix is:

$$M = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

The transition is:

$$M \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} b \\ c \\ d \\ a + d \end{pmatrix}.$$

Its action yields the following cycle of length 15:

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = 1 \rightsquigarrow \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = 8 \rightsquigarrow \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} = 12 \rightsquigarrow \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = 14 \rightsquigarrow \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = 15 \rightsquigarrow \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} = 7 \rightsquigarrow$$

$$\begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} = 11 \rightsquigarrow \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = 5 \rightsquigarrow \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = 10 \rightsquigarrow \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = 13 \rightsquigarrow \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = 6 \rightsquigarrow \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = 3 \rightsquigarrow$$

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = 9 \rightsquigarrow \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = 4 \rightsquigarrow \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = 2 \rightsquigarrow \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = 1 \rightsquigarrow$$

As the cycle is maximal, the irreducible polynomial is primitive.

The state 0 builds its own cycle.

Exercise 29 *The polynomial $X^4 + X^2 + 1$ is reducible over $\mathbb{F}_2$. Construct the associated linear feed-back register.*

Indeed, $X^4+X^2+1=(X^2+X+1)^2$. The associated matrix is:

$$M=\begin{pmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&1&0\end{pmatrix}.$$

The transition is:

$$M\begin{pmatrix}a\\b\\c\\d\end{pmatrix}=\begin{pmatrix}b\\c\\d\\a+c\end{pmatrix}.$$

We compute the following cycles:

$$\begin{pmatrix}1\\0\\0\\0\end{pmatrix}=1\rightsquigarrow\begin{pmatrix}0\\0\\0\\1\end{pmatrix}=8\rightsquigarrow\begin{pmatrix}0\\0\\1\\0\end{pmatrix}=4\rightsquigarrow\begin{pmatrix}0\\1\\0\\1\end{pmatrix}=10\rightsquigarrow\begin{pmatrix}1\\0\\1\\0\end{pmatrix}=5\rightsquigarrow\begin{pmatrix}0\\1\\0\\0\end{pmatrix}=2\rightsquigarrow\begin{pmatrix}1\\0\\0\\0\end{pmatrix}=1\rightsquigarrow$$

$$\begin{pmatrix}1\\1\\0\\0\end{pmatrix}=3\rightsquigarrow\begin{pmatrix}1\\0\\0\\1\end{pmatrix}=9\rightsquigarrow\begin{pmatrix}0\\0\\1\\1\end{pmatrix}=12\rightsquigarrow\begin{pmatrix}0\\1\\1\\1\end{pmatrix}=14\rightsquigarrow\begin{pmatrix}1\\1\\1\\1\end{pmatrix}=15\rightsquigarrow\begin{pmatrix}1\\1\\1\\0\end{pmatrix}=7\rightsquigarrow\begin{pmatrix}1\\1\\0\\0\end{pmatrix}=3\rightsquigarrow$$

$$\begin{pmatrix}0\\1\\1\\0\end{pmatrix}=6\rightsquigarrow\begin{pmatrix}1\\1\\0\\1\end{pmatrix}=11\rightsquigarrow\begin{pmatrix}1\\0\\1\\1\end{pmatrix}=13\rightsquigarrow\begin{pmatrix}0\\1\\0\\1\end{pmatrix}=10\rightsquigarrow\begin{pmatrix}0\\1\\1\\0\end{pmatrix}=6\rightsquigarrow$$

So there are two cycles of length 6, $(1,8,4,10,5,2)$ and $(3,9,12,14,15,7)$ and a cycle of length 4, $(6,11,13,10)$. The state 0 builds its own cycle.

Exercise 30 *Construct the graph of the linear feed-back register given by the polynomial* X^3+X+1 *on words of length* 4 *over* $\mathbb{F}_2$.

$$M=\begin{pmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\0&1&0&1\end{pmatrix}.$$

The transition is:

$$M\begin{pmatrix}a\\b\\c\\d\end{pmatrix}=\begin{pmatrix}b\\c\\d\\b+d\end{pmatrix}.$$

One finds a cycle of length 7 with one-segment edges of length 1 landing on its vertexes. In a separated component, a state lands in the one-element cycle (0). Indeed:

$$\begin{pmatrix}1\\0\\0\\1\end{pmatrix}=9\rightsquigarrow\begin{pmatrix}0\\0\\1\\1\end{pmatrix}=12\rightsquigarrow\begin{pmatrix}0\\1\\1\\1\end{pmatrix}=14\rightsquigarrow\begin{pmatrix}1\\1\\1\\0\end{pmatrix}=7\rightsquigarrow$$

$$\begin{pmatrix}1\\1\\0\\1\end{pmatrix} = 11 \rightsquigarrow \begin{pmatrix}1\\0\\1\\0\end{pmatrix} = 5 \rightsquigarrow \begin{pmatrix}0\\1\\0\\0\end{pmatrix} = 2 \rightsquigarrow \begin{pmatrix}1\\0\\0\\1\end{pmatrix} = 9 \rightsquigarrow$$

build the cycle $(9, 12, 14, 7, 11, 5, 2)$. The one-edge arrows landing on this cycle are the following:

$$\begin{pmatrix}1\\1\\0\\0\end{pmatrix} = 3 \quad \rightsquigarrow \quad \begin{pmatrix}1\\0\\0\\1\end{pmatrix} = 9$$
$$\begin{pmatrix}0\\0\\0\\1\end{pmatrix} = 8 \quad \rightsquigarrow \quad \begin{pmatrix}0\\0\\1\\1\end{pmatrix} = 12$$
$$\begin{pmatrix}1\\0\\1\\1\end{pmatrix} = 13 \quad \rightsquigarrow \quad \begin{pmatrix}0\\1\\1\\1\end{pmatrix} = 14$$
$$\begin{pmatrix}0\\1\\1\\0\end{pmatrix} = 6 \quad \rightsquigarrow \quad \begin{pmatrix}1\\1\\0\\1\end{pmatrix} = 11$$
$$\begin{pmatrix}0\\1\\0\\1\end{pmatrix} = 10 \quad \rightsquigarrow \quad \begin{pmatrix}1\\0\\1\\0\end{pmatrix} = 5$$
$$\begin{pmatrix}0\\0\\1\\0\end{pmatrix} = 4 \quad \rightsquigarrow \quad \begin{pmatrix}0\\1\\0\\0\end{pmatrix} = 2$$
$$\begin{pmatrix}1\\1\\1\\1\end{pmatrix} = 15 \quad \rightsquigarrow \quad \begin{pmatrix}1\\1\\1\\0\end{pmatrix} = 7$$

The separated component of 0 contains:

$$\begin{pmatrix}1\\0\\0\\0\end{pmatrix} = 1 \rightsquigarrow \begin{pmatrix}0\\0\\0\\0\end{pmatrix} = 0 \rightsquigarrow \begin{pmatrix}0\\0\\0\\0\end{pmatrix} = 0 \rightsquigarrow$$

Exercise 31 *Construct the graph of the linear feed-back register given by the polynomial* $X^4 + X^3 + X^2 + X + 1$ *on words of length* 4 *over* $\mathbb{F}_2$. *Observe that this polynomial is irreducible, but not primitive.*

Because $f(0) = f(1) = 1$, the polynomial has no linear factors. Also, $f(X) = X^2(X^2 + X + 1) + X + 1$, so is not divisible with the only one irreducible polynomial of degree 2. It follows that f is irreducible. The fact that f is not primitive will follow from the fact that the linear feed-back system of f does not operate in a big cycle consisting of all states different of 0.

$$M = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

The transition is:

$$M \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} b \\ c \\ d \\ a+b+c+d \end{pmatrix}.$$

In the situation of an irreducible polynomial which is not primitive, the states build cycles of equal length. In our case there will be three cycles of length 5.

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = 1 \rightsquigarrow \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = 8 \rightsquigarrow \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} = 12 \rightsquigarrow \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = 6 \rightsquigarrow \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = 3 \rightsquigarrow \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = 1 \rightsquigarrow$$

This is the cycle $(1, 8, 12, 6, 3)$.

$$\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = 2 \rightsquigarrow \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = 9 \rightsquigarrow \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = 4 \rightsquigarrow \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = 10 \rightsquigarrow \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = 5 \rightsquigarrow \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = 2 \rightsquigarrow$$

This is the cycle $(2, 9, 4, 10, 5)$.

$$\begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} = 7 \rightsquigarrow \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} = 11 \rightsquigarrow \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = 13 \rightsquigarrow \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = 14 \rightsquigarrow \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = 15 \rightsquigarrow \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} = 7 \rightsquigarrow$$

This is the cycle $(7, 11, 13, 14, 15)$.

There is still the trivial cycle of length 1 consisting alone of (0).

Exercise 32 *The function $f : \{0,1\}^8 \to \{0,1\}^8$ is given by the three-round Feistel net with the function $F : \{0,1\}^4 \to \{0,1\}^4$ given by $F(ab) = b\overleftarrow{a}$. Compute $f(10100110)$.*

The computation works as follows:

$$\begin{array}{cc} 1010 & 0110 \\ \downarrow & \swarrow\downarrow \\ \downarrow & 1010 \\ \rightarrow & \oplus \\ \swarrow & \downarrow \\ 0110 & 0000 \\ \downarrow & \swarrow\downarrow \\ \downarrow & 0000 \\ \rightarrow & \oplus \\ \swarrow & \downarrow \\ 0000 & 0110 \\ \downarrow & \swarrow\downarrow \\ \downarrow & 1010 \\ \rightarrow & \oplus \\ \swarrow & \downarrow \\ 0110 & 1010 \end{array}$$

So $f(10100110) = 01101010$.

Exercise 33 *Let $g, h : \{0,1\}^n \to \{0,1\}^n$ be arbitrary functions. The function $F : \{0,1\}^{2n} \to \{0,1\}^{2n}$ is defined by a two-round Feistel net using first the function g and then the function h.*

- Write down a formula expressing the function $F(a,b)$ with $a, b \in \{0,1\}^n$.

- Consider the function $G : \{0,1\}^{2n} \to \{0,1\}^{2n}$ given by

$$G(x,y) = (x \oplus g(y \oplus h(x)), y \oplus h(x)),$$

where $x, y \in \{0,1\}^n$. Compute $F \circ G(x,y)$ and $G \circ F(a,b)$.

In order to compute F, we look at the two-round Feistel net:

$$\begin{array}{cc} a & b \\ \downarrow & \swarrow\downarrow \\ \downarrow & g(b) \\ \rightarrow & \oplus \\ \swarrow & \downarrow \\ b & a \oplus g(b) \\ \downarrow & \swarrow\downarrow \\ \downarrow & h(a \oplus g(b)) \\ \rightarrow & \oplus \\ \swarrow & \downarrow \\ a \oplus g(b) & b \oplus h(a \oplus g(b)) \end{array}$$

It follows that:

$$F(a,b) = (a \oplus g(b), b \oplus h(a \oplus g(b))).$$

Now,

$$F \circ G(x,y) = F(x \oplus g(y \oplus h(x)), y \oplus h(x)) =$$
$$= (x \oplus g(y \oplus h(x)) \oplus g(y \oplus h(x)), y \oplus h(x) \oplus h(x \oplus g(y \oplus h(x)) \oplus g(y \oplus h(x)))) =$$
$$= (x, y \oplus h(x) \oplus h(x)) = (x,y).$$

Similarly,

$$G \circ F(a,b) = G(a \oplus g(b), b \oplus h(a \oplus g(b))) =$$
$$= (a \oplus g(b) \oplus g(b \oplus h(a \oplus g(b)) \oplus h(a \oplus g(b))), b \oplus h(a \oplus g(b)) \oplus h(a \oplus g(b))) =$$
$$= (a \oplus g(b) \oplus g(b), b) = (a,b).$$

So G is the inverse of F and both functions are bijective.

Exercise 34 *During the operation SubBytes in AES one needs the inverse of the element $x = w + 1$. Find it out.*

The AES arithmetic on the field with 256 elements is given by the irreducible polynomial over $\mathbb{F}_2$:

$$x^8 + x^4 + x^3 + x + 1,$$

which means the relation $w^8 = w^4 + w^3 + w + 1$. The condition:

$$(w+1)(aw^7 + bw^6 + cw^5 + dw^4 + ew^3 + fw^2 + gw + h) = 1,$$

$$a(w^4 + w^3 + w + 1) + bw^7 + cw^6 + dw^5 + ew^4 + fw^3 + gw^2 + hw +$$
$$+ aw^7 + bw^6 + cw^5 + dw^4 + ew^3 + fw^2 + gw + h = 1.$$

By identifying powers, this leads to the following system of linear equations over $\mathbb{F}_2$:

$$\begin{aligned} a+h &= 1 \\ a+h+g &= 0 \\ g+f &= 0 \\ a+f+e &= 0 \\ a+e+d &= 0 \\ c+d &= 0 \\ c+b &= 0 \\ a+b &= 0 \end{aligned}$$

From the last four equations, $a = b = c = d$ and $e = 0$. It follows:

$$\begin{aligned} a+h &= 1 \\ a+h+g &= 0 \\ g+f &= 0 \\ a+f &= 0 \end{aligned}$$

From the last two equations, $a = f = g$. Now:

$$\begin{aligned} a+h &= 1 \\ a+h+g &= 0 \end{aligned}$$

So $h = 0$ and $a = 1$. Finally:

$$x^{-1} = w^7 + w^6 + w^5 + w^4 + w^2 + w.$$

Indeed,

$$\begin{gathered} (w+1)(w^7 + w^6 + w^5 + w^4 + w^2 + w) = \\ = w^8 + w^7 + w^6 + w^5 + w^3 + w^2 + w^7 + w^6 + w^5 + w^4 + w^2 + w = \\ = w^8 + w^3 + w^4 + w = 1. \end{gathered}$$

Exercise 35 *The operation SubBytes in AES consists of the following steps:*
- If the byte $x \neq 0$ then $x = x^{-1} \bmod w^8 + w^4 + w^3 + w + 1$.
- The byte x is replaced by the result of the following linear application:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}.$$

Suppose we have a program computing SubBytes. What is the best way to use it? Is it better to write another program for the inverse operation SubBytes^{-1}, or we can use the same program?

About the direct function SubBytes: there are only $2^8 = 256$ bytes. So the most rational way to proceed is to compute a look-up list with all results at the beginning, when the program is started,

and then, in each step, just to read the look-up list. This look-up list can be even precomputed and displayed in the application code, such that it would be just initialised from the library as a constant.

About the inverse operation SubBytes^{-1}: it is not the case to invert the 8×8 matrix and to write down and run another program. The pairs $(x, SubBytes(x))$ buld the columns of a permutation of the set $\mathbb{F}_{256}$. In order to compute the inverse permutation, we revert all pairs like $(SubBytes(x), x)$, and we sort them lexicographically according to the first argument. The result will be the look-up list $(y, SubBytes^{-1}(y))$. In both look-up lists the results are got by binary search in time $O(1)$.

Exercise 36 *Reformulate the matrix multiplication from the SubBytes operation in one line.*

The operation:

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix}$$

can be written as:

$$y_i = x_i + x_{(i+4) \bmod 8} + x_{(i+5) \bmod 8} + x_{(i+6) \bmod 8} + x_{(i+7) \bmod 8},$$

for $i = 0, \ldots, 7$.

Exercise 37 *The operation MixColumns in AES consists in the multiplication of the state matrix with the matrix:*

$$M = \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix}.$$

This operation takes place in $M_{4\times4}(\mathbb{F}_{256})$. Show that during decryption, MixColumns consists in the multiplication of the state matrix with the matrix:

$$N = \begin{pmatrix} 14 & 11 & 13 & 9 \\ 9 & 14 & 11 & 13 \\ 13 & 9 & 14 & 11 \\ 11 & 13 & 9 & 14 \end{pmatrix},$$

in the same ring $M_{4\times4}(\mathbb{F}_{256})$.

What we really must show, is that the second matrix is the inverse of the first one. As the matrices are over $\mathbb{F}_{256}$ and its arithmetic is defined by the polynomial $w^8 + w^4 + w^3 + w + 1$, it is important to understand which are the elements present in these matrices. This is easier to understand for the original matrix:

$$\begin{aligned} 1 &= 1, \\ 2 &= 10 = w, \\ 3 &= 11 = w + 1. \end{aligned}$$

As to the new matrix,

$$\begin{aligned} 14 &= 1110 = w^3 + w^2 + w, \\ 11 &= 1011 = w^3 + w + 1, \\ 13 &= 1101 = w^3 + w^2 + 1, \\ 9 &= 1001 = w^3 + 1. \end{aligned}$$

The first line of N times the first column of M means:

$$14 \cdot 2 + 11 \cdot 1 + 13 \cdot 1 + 9 \cdot 3 = w(w^3 + w^2 + w) + w^3 + w + 1 + w^3 + w^2 + 1 + (w+1)(w^3+1) =$$
$$= w^4 + w^3 + w^2 + w + w^2 + w^4 + w + w^3 + 1 = 1.$$

The first line of N times the second column of M means:

$$14 \cdot 3 + 11 \cdot 2 + 13 \cdot 1 + 9 \cdot 1 = (w^3 + w^2 + w)(w+1) + (w^3 + w + 1)w + w^3 + w^2 + 1 + w^3 + 1 =$$
$$= w^4 + w^3 + w^2 + w^3 + w^2 + w + w^4 + w^2 + w + w^2 = 0.$$

The reader is encouraged to compute also the remaining 14 elements of the product matrix.

Exercise 38 *Explain why the operations ShiftRows and MixColumns, as like all operations containing circulant matrices, can be defined as product of polynomials modulo $X^4 + 1$.*

Fie o relatie:

$$b_0 + b_1X + b_2X^2 + b_3X^3 = (a_0 + a_1X + a_2X^2 + a_3X^3)(c_0 + c_1X + c_2X^2 + c_3X^3) \mod (X^4 + 1).$$

The computation yields:

$$a_0c_0 + a_0c_1X + a_0c_2X^2 + a_0c_3X^3 +$$
$$+a_1c_0X + a_1c_1X^2 + a_1c_2X^3 + a_1c_3 +$$
$$+a_2c_0X^2 + a_2c_1X^3 + a_2c_2 + a_2c_3X +$$
$$+a_3c_0X^3 + a_3c_1 + a_3c_2X + a_3c_3X^2.$$

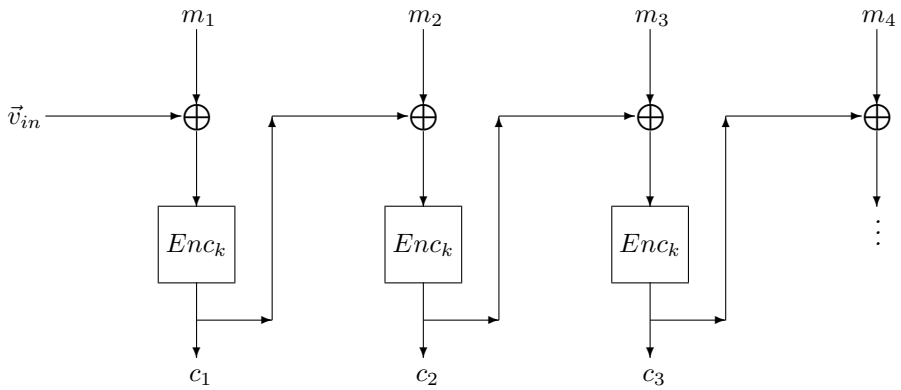
This expression is sorted as a polynomial.

$$(a_0c_0 + a_1c_3 + a_2c_2 + a_3c_1) + (a_0c_1 + a_1c_0 + a_2c_3 + a_3c_2)X +$$
$$+(a_0c_2 + a_1c_1 + a_2c_0 + a_3c_3)X^2 + (a_0c_3 + a_1c_2 + a_2c_1 + a_3c_0)X^3.$$

This can be rewritten as action of a circulant matrix:

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} c_0 & c_3 & c_2 & c_1 \\ c_1 & c_0 & c_3 & c_2 \\ c_2 & c_1 & c_0 & c_3 \\ c_3 & c_2 & c_1 & c_0 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix}.$$

Exercise 39 *Recall the CBC mode:*



Call collision *a pair* (i, j) *such that* $i \neq j$ *and* $c_i = c_j$.

- Show that a collision reveals informations about the clear message m.

- What is the probability of a collision?

Indeed, if $c_i = c_j$, this means $c_{i-1} \oplus m_i = c_{j-1} \oplus m_j$. So $m_i \oplus m_j = c_{i-1} \oplus c_{j-1}$. This means that we have informations about the clear message without knowing the key.

In order to estimate the probability of observing one collision, we use the Birthdate Paradox. If $|m_i| = 64$ and n is the number of blocks, we define θ as:

$$\theta = \frac{n}{\sqrt{2^{64}}}.$$

In this case the probability of a collision is approximated by the expression:

$$P \simeq 1 - e^{-\frac{\theta^2}{2}}.$$

Here are some examples:

1 MB, $n = 2^{17}$, $P = 4.66 \cdot 10^{-10}$.

1 GB, $n = 2^{27}$, $P = 5 \cdot 10^{-4}$.

32 GB, $n = 2^{32}$, $P = 0.39$.

64 GB, $n = 2^{33}$, $P = 0.865$.

128 GB, $n = 2^{34}$, $P = 0.9997$.

So for a message of 128 GB there are almost sure some collisions, but a loss of information of around 64 bits is a very small one if compared with the message. So CBC is considered a secure mode.

Exercise 40 *This exercise introduces an unusual operation with bytes. Observe that the number* 257 *is prime. Show that the function:*

$$f(x) = (45^x \bmod 257) \bmod 256$$

is a permutation of the set $\{0, 1, \ldots, 255\}$.

Because 257 is prime, $\mathbb{Z}_{257} = \mathbb{F}_{257}$ and $\mathbb{F}_{257}^{\times}$ is cyclic. The sequence below represent the successive squares $45^{2^i} \rightsquigarrow 45^{2^{i+1}}$.

$$45 \rightsquigarrow 226 \rightsquigarrow 190 \rightsquigarrow 120 \rightsquigarrow 8 \rightsquigarrow 64 \rightsquigarrow 241 \rightsquigarrow 256 \rightsquigarrow 1.$$

So $\mathrm{ord}(45) = 256$ in the multiplicative group of $\mathbb{F}_{257}$, this means that 45 is a generator of this group. The expression $45^x \bmod 257$ is a surjection on $\{1, \ldots, 256\}$, and modulo 256, it becomes surjective on $\{0, 1, \ldots, 255\}$.

Recall the fact that $\mathbb{F}_{256}$ is another field. Its addition is the same as $\oplus$ on bytes, and its cyclic multiplicative group has 255 elements. So when working with bytes, excepting $\oplus$, we can use also other operations like $(a + b) \bmod 256$, $45^x \bmod 257 \bmod 256$ or the corresponding inverse permutation which can be denoted ad hoc $\log_{45} x$. The cryptosystem SAFER K uses all these operations.

Exercise 41 *Consider a natural number* $m \in \mathbb{N}$ *such that* $2^m + 1$ *is prime. Let* $g \in \mathbb{Z}_{2^m+1}^{\times}$ *be a generator of the cyclic multiplicative group. Consider the following exponential function* $E : \mathbb{Z}_{2^m} \to \mathbb{Z}_{2^m}$, *given by:*

$$E(x) = (g^x \bmod (2^m + 1)) \bmod 2^m.$$

Show that:

$$Pr[E(x) = x \bmod 2] = \frac{1}{2}.$$

As the multiplicative group generated by g has 2^m elements, and $(g^{2^{m-1}})^2 = g^{2^m}$, it follows that:

$$g^{2^{m-1}} = -1 \bmod (2^m + 1),$$

so that:

$$E(2^{m-1} + a) = (-g^a \bmod (2^m + 1)) \bmod 2^m.$$

As $2^m + 1$ is odd, it follows that $E(a)$ is even if and only $E(2^{m-1} + a)$ is odd. One can do the following partition of $\mathbb{Z}_{2^m}$:

$$A = \{x \in \mathbb{Z}_{2^m} \,|\, x \text{ even } \wedge \ E(x) \text{ even}\},$$

$$B = \{x \in \mathbb{Z}_{2^m} \,|\, x \text{ even } \wedge \ E(x) \text{ odd}\},$$

$$C = \{x \in \mathbb{Z}_{2^m} \,|\, x \text{ odd } \wedge \ E(x) \text{ even}\},$$

$$D = \{x \in \mathbb{Z}_{2^m} \,|\, x \text{ odd } \wedge \ E(x) \text{ odd}\}.$$

Of course $A \cup B = \{x \,|\, x \text{ even}\}$ and $C \cup D = \{x \,|\, x \text{ odd}\}$. So both unions have exactly 2^{m-1} elements. But every pair $(x, x + 2^{m-1})$, with $0 \leq x < 2^{m-1}$, contains exactly one element in A and one element in B. So A and B have both 2^{m-2} elements, and the same happens with C and D. Finally,

$$Pr[E(x) = x \bmod 2] = Pr[A \cup D] = \frac{2^{m-2} + 2^{m-2}}{2^m} = \frac{1}{2}.$$

Definition: *Let X be a finite set and $f : X^p \to X^q$ a function. The function is a (p, q)-multipermutation if and only if for every two different tuples $(x_1, \ldots, x_{p+q})$ with $f(x_1, \ldots, x_p) = (x_{p+1}, \ldots, x_{p+q})$, at least $q + 1$ different coordinates have different values.*

Exercise 42 *What is a $(1, 1)$-multipermutation?*

It is a function $f : X \to X$ such that for every different tuples $(x, f(x))$ and $(y, f(y))$, at least two coordinates are different. So f is injective. But as X is finite, f is surjective as well. So a $(1, 1)$-multipermutation is a permutation.

Exercise 43 *In the algorithm MD4 following functions are used:*

$$\begin{aligned} f_1(a, b, c) &= \textbf{if } a \textbf{ then } b \textbf{ else } c, \\ f_2(a, b, c) &= \textbf{if } c \textbf{ then } a \textbf{ else } b, \\ f_3(a, b, c) &= a \oplus b \oplus c. \end{aligned}$$

- Show that the functions f_1 and f_2 are not $(3, 1)$-multipermutations.

- Show that f_3 is a $(3, 1)$-multipermutation.

Observe that $f_1(0, 1, 1) = 1$ and that $f_1(1, 1, 1) = 1$. So the tuples $(0, 1, 1, 1)$ and $(1, 1, 1, 1)$ are different but should differ in two coordinates and differ just in one coordinate. The function f_2 is just f_1 computed with a permutation of variables, and has the same behavior as f_1.

Let $(a, b, c, a \oplus b \oplus c)$ and $(a', b', c', a' \oplus b' \oplus c')$ be two tuples corresponding to the function f_3. It is easy to see that if they differ in one coordinate, then they differ in two coordinates. Indeed, every one of the conditions $a \neq a'$, $b \neq b'$ and $c \neq c'$ implies $a \oplus b \oplus c \neq a' \oplus b' \oplus c'$, so they differ already in two coordinates. Also, if $a \oplus b \oplus c \neq a' \oplus b' \oplus c'$ then $(a, b, c) \neq (a', b', c')$ and differ in at least one coordinate.

Exercise 44 *Consider the function $f : \mathbb{Z}_{256} \times \mathbb{Z}_{256} \to \mathbb{Z}_{256} \times \mathbb{Z}_{256}$ given by:*

$$f(a, b) = (2a + b, a + b) \bmod 256.$$

Show that f is not a $(2, 2)$-multipermutation, but is a $(1, 1)$-multipermutation.

We observe that $f(0,0) = (0,0)$ and that $f(128,0) = (0,128)$. The tuples $(0,0,0,0)$ and $(128,0,0,128)$ differ in two coordinates but not in three. On the other hand, the determinant of this linear application is equal 1, and is invertible modulo 256, so this linear application is bijective, so it is a $(1,1)$-multipermutation.

Definition: *A function $\sigma : \{0,1\}^n \to \{0,1\}^n$ is called a XOR-orthomorphism if and only if σ is a bijection and $\sigma' : \{0,1\}^n \to \{0,1\}^n$ given as $\sigma'(x) = x \oplus \sigma(x)$ is bijective as well.*

Exercise 45 *Consider the function $\omega : \{0,1\}^8 \to \{0,1\}^8$ given as:*

$$\omega(x) = ROT^4(x \oplus (x >> 4)),$$

where

$$b_7 b_6 \dots b_1 b_0 >> 4 = 0000 b_7 b_6 b_5 b_4$$

and

$$ROT(b_7 b_6 \dots b_1 b_0) = b_0 b_7 \dots b_1.$$

Show that ω is a XOR-orthomorphism.

Let $x = b_7 \dots b_0 \in \{0,1\}^8$ be an element.

$$\omega(x) = ROT^4(b_7, b_6, b_5, b_4, b_3 \oplus b_7, b_2 \oplus b_6, b_1 \oplus b_5, b_0 \oplus b_4) =$$
$$= (b_3 \oplus b_7, b_2 \oplus b_6, b_1 \oplus b_5, b_0 \oplus b_4, b_7, b_6, b_5, b_4).$$

On the other hand, we observe that:

$$\omega(x) \oplus x = (b_3, b_2, b_1, b_0, b_7 \oplus b_3, b_6 \oplus b_2, b_5 \oplus b_1, b_4 \oplus b_0).$$

So:

$$(\omega(y) \oplus y) \circ \omega(x) = (\omega(y) \oplus y)(b_3 \oplus b_7, b_2 \oplus b_6, b_1 \oplus b_5, b_0 \oplus b_4, b_7, b_6, b_5, b_4) =$$
$$= (b_7, b_6, b_5, b_4, b_3 \oplus b_7 \oplus b_7, b_2 \oplus b_6 \oplus b_6, b_1 \oplus b_5 \oplus b_5, b_0 \oplus b_4 \oplus b_4) = x,$$

and:

$$\omega(\omega(x) \oplus x) = \omega(b_3, b_2, b_1, b_0, b_7 \oplus b_3, b_6 \oplus b_2, b_5 \oplus b_1, b_4 \oplus b_0) =$$
$$(b_7 \oplus b_3 \oplus b_3, b_6 \oplus b_2 \oplus b_2, b_5 \oplus b_1 \oplus b_1, b_4 \oplus b_0 \oplus b_0, b_3, b_2, b_1, b_0) = x.$$

Evidently both applications are invertible, so both are bijections. It follows that ω is a XOR-orthomorphism.

Exercise 46 *Let $c \in \{0,1\}^8$ be the byte $c = 0xAA = 1010\ 1010$. Consider the function $\pi : \{0,1\}^8 \to \{0,1\}^8$ given as:*

$$\pi(x) = (x \wedge c) \oplus ROT(x).$$

Show that π is a XOR-orthomorphism.

We compute:

$$\pi(x) = (b_7, 0, b_5, 0, b_3, 0, b_1, 0) \oplus (b_0, b_7, b_6, b_5, b_4, b_3, b_2, b_1) =$$
$$= (b_0 \oplus b_7, b_7, b_6 \oplus b_5, b_5, b_4 \oplus b_3, b_3, b_2 \oplus b_1, b_1),$$
$$\pi(x) \oplus x = (b_0 \oplus b_7, b_7, b_6 \oplus b_5, b_5, b_4 \oplus b_3, b_3, b_2 \oplus b_1, b_1) \oplus (b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0) =$$
$$= (b_0, b_7 \oplus b_6, b_6, b_5 \oplus b_4, b_4, b_3 \oplus b_2, b_2, b_1 \oplus b_0),$$

These functions are similar. We show that π is a bijection, the proof for $\pi(x) \oplus x$ is analogous. Suppose $\pi(x) = y$. Coordinate-wise this means:

$$(b_0 \oplus b_7, b_7, b_6 \oplus b_5, b_5, b_4 \oplus b_3, b_3, b_2 \oplus b_1, b_1) = (c_7, c_6, c_5, c_4, c_3, c_2, c_1, c_0).$$

It follows directly that $(b_7, b_5, b_3, b_1) = (c_6, c_4, c_2, c_0)$. Further $b_0 \oplus b_7 = c_7$ implies $b_0 \oplus c_6 = c_7$ so $b_0 = c_6 \oplus c_7$. Also $b_6 \oplus b_5 = c_5$ implies $b_6 \oplus c_4 = c_5$ so $b_6 = c_4 \oplus c_5$. From $b_4 \oplus b_3 = c_3$ follows $b_4 \oplus c_2 = c_3$ so $b_4 = c_2 \oplus c_3$. Finally, from $b_2 \oplus b_1 = c_1$ follows $b_2 \oplus c_0 = c_1$ so $b_2 = c_0 \oplus c_1$. So there is a unique solution $x = \psi(y)$ and the functions π and ψ are invertible, so bijective.

Exercise 47 *Consider two functions* $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n \times \{0,1\}^n$ *and* $\sigma : \{0,1\}^n \to \{0,1\}^n$ *connected by the following relation:*

$$f(a,b) = (a \oplus b, a \oplus \sigma(b)).$$

Show that f *is a* $(2,2)$*-multipermutation if and only if* σ *is a XOR-orthomorphism.*

We consider two 4-tuples $(a, b, a \oplus b, a \oplus \sigma(b))$ and $(a', b', a' \oplus b', a' \oplus \sigma(b'))$.

Suppose that f is a $(2,2)$-multipermutation. Choose $b \neq b'$ and $a = 0$. It follows that the tuples $(0, b, b, \sigma(b))$ and $(0, b', b', \sigma(b'))$ differ in 3 coordinates, so $\sigma(b) \neq \sigma(b')$. It follows that σ is injective, and as its domain, identical with its codomain, is finite, σ is bijective. Now choose $a = b$, $a' = b'$ and $a \neq a'$. Again the tuples $(a, a, 0, a \oplus \sigma(a))$ and $(a', a', 0, a' \oplus \sigma(a'))$ must differ in 3 coordinates, so $a \oplus \sigma(a) \neq a' \oplus \sigma(a')$, so the function $\theta(x) = \sigma(x) \oplus x$ is bijective as well. So it follows that σ is an XOR-orthomorphism.

Now suppose that σ is a XOR-orthomorphism. We look again at the two tuples $(a, b, a \oplus b, a \oplus \sigma(b))$ and $(a', b', a' \oplus b', a' \oplus \sigma(b'))$. If $a = a'$ but $b \neq b'$ then $a \oplus b \neq a \oplus b'$ and $a \oplus \sigma(b) \neq a \oplus \sigma(b')$ because σ and $\sigma \oplus id$ are bijective. So the tupples differ in three positions. The case $a \neq a'$ and $b = b'$ is similar.

Consider the case $a \neq a'$ and $b \neq b'$. If $a \oplus b \neq a' \oplus b'$ then the tuple already differ in 3 coordinates. Suppose that $a \oplus b = a' \oplus b'$ and $a \oplus \sigma(b) = a' \oplus \sigma(b')$. We add these relations together and we get $b \oplus \sigma(b) = b' \oplus \sigma(b')$. But as we know that σ is a XOR-orthomorphism, it follows that $b = b'$, which is a contradiction. So the tuples always differ in at least three coordinates, so f is a $(2,2)$-multipermutation.