Advanced Cryptography Exercises II

Mihai Prunescu

1 Public key cryptography

Exercise 1 *Show that in every field with $p = 4k + 1$ elements, where p is a prime number, the element -1 is a square. As an application, compute* $\sqrt{-1} \bmod 13$.

It is known that a prime number is a sum of two squares if and only if is of the form $4k + 1$. So modulo p, there are two elements $a, b \in \mathbb{F}_p^\times$ such that:

$$a^2 + b^2 = 0.$$

But this means that:

$$-1 = (ab^{-1})^2.$$

If $p = 13$, $13 = 4 + 9$ so $\sqrt{-1} = 3 \cdot 2^{-1} = 3 \cdot 7 = 8$. Indeed $8^2 + 1 = 65 = 0 \bmod 13$. Another square root of -1 is $-8 = 13 - 8 = 5$. Again $25 + 1 = 0 \bmod 13$.

Exercise 2 *Decide if* 8 *is a square modulo* 23.

We compute the symbol of Legendre. All computations below are modulo 23.

$$\left(\frac{8}{23}\right) = 8^{\frac{23-1}{2}} = 8^{11} = 8^{8+2+1}$$

By successive squaring we find:

$$8 \rightsquigarrow 8^2 = 64 = -5 \rightsquigarrow 8^4 = 25 = 2 \rightsquigarrow 8^8 = 4,$$

$$\left(\frac{8}{23}\right) = 8^{8+2+1} = 4 \cdot (-5) \cdot 8 = -(-3) \cdot 8 = 24 = 1.$$

So 8 is a square modulo 23.

Other solution, based on Gauss' Reciprocity Law:

$$\left(\frac{8}{23}\right) = \left(\frac{2^3}{23}\right) = \left(\frac{2}{23}\right)^3 = \left(\frac{2}{23}\right) = (-1)^{\frac{23^2-1}{8}} = (-1)^{\frac{528}{8}} = (-1)^{66} = 1.$$

Exercise 3 *Find the square roots of* 8 *modulo* 23.

We apply Cipolla's Algorithm. First we must find an a such that $a^2 - 8$ is NOT a square modulo 23. Try with $a = 1$:

$$\left(\frac{1-8}{23}\right) = \left(\frac{-7}{23}\right) = \left(\frac{16}{23}\right) = 1,$$

so this is a square. Try with $a = 2$:

$$\left(\frac{4-8}{23}\right) = \left(\frac{-4}{23}\right) = \left(\frac{19}{23}\right) = -\left(\frac{23}{19}\right) = -\left(\frac{4}{19}\right) = -1,$$

so this choice was good. Now let w be a symbol such that $w^2 = 19$ over $\mathbb{F}_{23}$. According to Cipolla's Algorithm,

$$x = (a+w)^{(p+1)/2} = (2+w)^{(23+1)/2} = (2+w)^{12},$$

in the field $\mathbb{F}_{23}[w]$. As 12 is $8+4$, we apply the fast exponentiation algorithm:

$$(2+w)^2 = 4 + 4w + w^2 = 4w,$$

$$(2+w)^4 = 16w^2 = (-7) \cdot (-4) = 28 = 5,$$

$$(2+w)^8 = 5^2 = 25 = 2.$$

Finally:

$$x = (2+w)^8(2+w)^4 = 2 \cdot 5 = 10.$$

Indeed, $10^2 = 100 = 100 - 92 = 8$ modulo 23. Another square root of 8 is $23 - 10 = 13$.

Exercise 4 *Find the square roots of* 31 *modulo* 69.

As $69 = 3 \cdot 23$, using the Chinese Remainder Theorem we express 31 in the ring $\mathbb{Z}_{69} = \mathbb{Z}_3 \times \mathbb{Z}_{23}$ as the pair $(31 \bmod 3, 31 \bmod 23) = (1 \bmod 3, 8 \bmod 23)$. As both elements in the pair are squares in their rings, it follows that 31 is indeed a square modulo 69. The square roots of 31 will be represented by the pairs $(\pm 1 \bmod 3, \pm 10 \bmod 23)$. We get four cases to apply the Chinese Remainder Theorem.

The case $(+,+)$ is given by:

$$\begin{aligned} x &= 1 \bmod 3, \\ x &= 10 \bmod 23, \end{aligned}$$

and has the trivial solution $x = 10$. Indeed, it fulfills the system, and moreover $10^2 = 100 = 31 \bmod 69$.

The case $(+,-)$ is given by:

$$\begin{aligned} x &= 1 \bmod 3, \\ x &= 13 \bmod 23, \end{aligned}$$

and has the trivial solution $x = 13$. Indeed, it fulfills the system and moreover $13^2 = 169 = 100 = 31 \bmod 69$.

The case $(-,+)$ is given by:

$$\begin{aligned} x &= 2 \bmod 3, \\ x &= 10 \bmod 23, \end{aligned}$$

and has the solution $x = 56$. We see that $56 = -13 \bmod 69$, so it is surely a square root of 31.

The case $(-,-)$ is given by:

$$\begin{aligned} x &= 2 \bmod 3, \\ x &= 13 \bmod 23, \end{aligned}$$

and has the solution $x = 59$. We see that $59 = -10 \bmod 69$, so it is again a square root of 31.

Exercise 5 *Compute* $112^2 \bmod 225$ *using a pocket calculator.*

We compute $112^2 = 12544$ and $12544 : 225 = 55.751\ldots$. The integer part is 55. We compute $55 \cdot 225 = 12375$ and $12544 - 12375 = 169$. So we shown that:

$$112^2 \bmod 225 = 169.$$

So it happens also that $112^2 = 13^2 \bmod 225$.

Exercise 6 *Find a value for the expression* $\sqrt[7]{23} \bmod 77$.

We observe that $23 \in \mathbb{Z}_{77}^{\times}$ because is relatively prime with 77. We also observe that $|\mathbb{Z}_{77}^{\times}| = \varphi(77) = \varphi(7)\varphi(11) = 6 \cdot 10 = 60$. We interpret the expression as:

$$\sqrt[7]{23} \bmod 77 = 23^{\text{"}\frac{1}{7}\text{"}} \bmod 77 = 23^{[7^{-1} \bmod \varphi(77)]} \bmod 77 = 23^{[7^{-1} \bmod 60]} \bmod 77.$$

But how much is $7^{-1} \bmod 60$? It surely exists, because 7 and 60 are relatively prime, so we already suppose that the sense we gave to our expression is consistent. Now we apply the extended Euclid algorithm:

$$\begin{aligned}
60 &= \underline{7} \cdot 8 + \underline{4}, \\
&\to \underline{4} = (-8) \cdot \underline{7} \\
\underline{7} &= \underline{4} \cdot 1 + \underline{3}, \\
&\to \underline{3} = (1+8) \cdot \underline{7} = 9 \cdot \underline{7} \\
\underline{4} &= \underline{3} + 1 \\
&\to 1 = (-8-9) \cdot \underline{7} = (-17) \cdot \underline{7} = 43 \cdot \underline{7},
\end{aligned}$$

where the computations are done modulo 60.

So $7^{-1} \bmod 60 = 43 = 32 + 8 + 2 + 1$. In order to compute $23^{43} \bmod 77$, we apply successive squaring:

$$23 \rightsquigarrow 23^2 = 67 \rightsquigarrow 23^4 = 23 \rightsquigarrow 23^8 = 67 \rightsquigarrow 23^{16} = 23 \rightsquigarrow 23^{32} = 67 \mod 77.$$

$$23^{43} = 23^{32} 23^8 23^2 23 = 67 \cdot 67 \cdot 67 \cdot 23 = 23 \cdot 67 \cdot 23 = 67 \cdot 67 = 23 \mod 77.$$

In order to verify this, we must compute $23^7 \bmod 77$.

$$23^7 = 23^4 23^2 23 = 23 \cdot 67 \cdot 23 = 67 \cdot 67 = 23 \mod 77.$$

Exercise 7 *RSA modulo* 85*. Bob uses the public key* 3 *and encrypts the message* 80 *for Alice. Find out the encrypted message, the secret key, and show how Alice decrypts Bob's message. Use the classical RSA theory, which is based on the function* $\varphi(N)$*.*

The encrypted message is:

$$80^3 \bmod 85 = (-5)^3 \bmod 85 = -125 \bmod 85 = 45.$$

Now $\varphi(85) = (5-1)(17-1) = 4 \cdot 16 = 64$. To compute $3^{-1} \bmod 64$ we apply the extended Euclid algorithm:

$$64 = 21 \cdot \underline{3} + 1,$$

so $1 = 3 \cdot (-21) = 3 \cdot 43 \bmod 64$, and $3^{-1} \bmod 64 = 43$. We observe that $43 = 32 + 8 + 2 + 1$.

In order to compute $45^{43} \bmod 85$ we apply successive squaring:

$$45 \rightsquigarrow 45^2 = 70 \rightsquigarrow 45^4 = 55 \rightsquigarrow 45^8 = 50 \rightsquigarrow 45^{16} = 35 \rightsquigarrow 45^{32} = 35 \bmod 85,$$

so $45^{43} = 35 \cdot 50 \cdot 70 \cdot 45 \bmod 85 = 80$.

Exercise 8 *Agent Eve intercepts the encrypted message from the previous exercise and uses the function* $\lambda(N)$ *to compute the secret key. Find out what she does.*

For $N = pq$, product of prime numbers, the function $\lambda(N) = \mathrm{lcm}(p-1, q-1)$. In our case, $\lambda(85) = \mathrm{lcm}(5-1, 17-1) = \mathrm{lcm}(4, 16) = 16$. So we have to compute the inverse $3^{-1} \bmod 16 = 11$ and $11 = 8 + 2 + 1$. The decryption reads:

$$45^{11} \bmod 85 = 45^8 \cdot 45^2 \cdot 45 \bmod 85 = 50 \cdot 70 \cdot 45 \bmod 85 = 80.$$

Exercise 9 *Show that there are exactly* 7 *possible encryptions RSA modulo* 85 *and all the resulting permutations of the alphabet with* 85 *letters have as orders powers of* 2. *Which is the best key to use?*

As we have seen, $\lambda(85) = 16$ and $\varphi(16) = 16 - 8 = 8$, so there are 7 classes of encryption keys modulo 16 for RSA modulo 85, because we do not consider the identical encryption. The multiplicative group $\mathbb{Z}_{16}^\times$ is NOT cyclic and contains 8 elements. Their orders are 4, 2 and 1, exactly so are the encryptions seen as permutations. A possible encryption with maximal order 4 is given by the key $k = 3$ and was used in the last two exercises. The group generated by 3 in $\mathbb{Z}_{16}^\times$ is:

$$3, 9, 11, 1.$$

The key $k = 11$ leads as well to a permutation of order 4 and has the advantage that the number 11 is bigger. So this would be an example of best public key.

Exercise 10 *Alice an Bob practice* **additive** *Elgamal modulo* 1000 *with generator* $g = 67$. *Alice chooses the secret key* $k = 21$. *She computes the correspondent public key and communicates it to Bob. Bob chooses the temporary key* $t = 11$. *He uses the public key and encrypts the message* $m = 200$. *Alice uses the secret key and finds out the clear message. Make all computations.*

The cyclic group in question is $(\mathbb{Z}_{1000}, +, 0)$. The number $g = 67$ generates the group because $\gcd(1000, 67) = 1$. The public key, defined in general cyclic groups g^k, is now $h = gk \bmod 1000 = 67 \cdot 21 \bmod 1000 = 407$. Bob computes the message $(c_1, c_2) = (gt, ht + m) = (737, 407 \cdot 11 + 200) = (737, 477 + 200) = (737, 677)$.

In order to find m, Alice computes $m = c_2 - kc_1 = 677 - 21 \cdot 737 = 677 - 477 = 200$. All computations are made modulo 1000.

Exercise 11 *In the situation from the previous exercise, agent Eve knows that Alice and Bob practice Elgamal modulo* 1000 *with generator* $g = 67$. *Eve knows the public key* $h = 407$ *and she intercepts the message* $(737, 677)$ *sent by Bob. What does Eve in order to easily decrypt this message?*

A possibility for Eve is to compute $g^{-1} \bmod 1000$ and to multiply it with h in order to find out the secret key $k = g^{-1}h$. Once she has the secret key, she can directly decrypt the message, as Alice also had done before. The inverse $67^{-1} \bmod 1000$ is computed using the extended Euclid algorithm.

$$\begin{aligned}
1000 &= 14 \cdot \underline{67} + \underline{62} \\
&\to \underline{62} = (-14) \cdot \underline{67} \\
\underline{67} &= 1 \cdot \underline{62} + \underline{5} \\
&\to \underline{5} = 15 \cdot \underline{67} \\
\underline{62} &= 12 \cdot \underline{5} + \underline{2} \\
&\to \underline{2} = (-14 - 12 \cdot 15) \cdot \underline{67} = (-194) \cdot \underline{67} \\
\underline{5} &= 2 \cdot \underline{2} + 1 \\
&\to 1 = (15 - 2 \cdot (-194)) \cdot \underline{67} = 403 \cdot \underline{67},
\end{aligned}$$

where the computation is done modulo 1000. So $k = 403 \cdot 407 \bmod 1000 = 21$, and Eve can now decrypt the message. In order to find m, Eve computes $m = c_2 - kc_1 = 677 - 21 \cdot 737 = 677 - 477 = 200$. All computations are made modulo 1000.

Exercise 12 *Alice and Bob practice* **multiplicative** *Elgamal modulo* 101 *with generator* $g = 2$. *Alice chooses the secret key* $k = 58$. *Bob chooses the temporary key* $y = 59$ *and must encrypt the message* $m = 60$. *Describe completely the setup, the encryption and the decryption.*

Alice computes the public key $h = 2^{58} \bmod 101$. She writes $58 = 32 + 16 + 8 + 2$. By successive squaring, she gets:

$$2 \rightsquigarrow 2^2 = 4 \rightsquigarrow 2^4 = 16 \rightsquigarrow 2^8 = 54 \rightsquigarrow 2^{16} = 88 \rightsquigarrow 2^{32} = 68.$$

So $2^{58} = 68 \cdot 88 \cdot 54 \cdot 4 = 68 \cdot 88 \cdot 14 = (-33) \cdot 88 \cdot 14 = (-1) \cdot 3 \cdot 8 \cdot 20 \cdot 14 = (-1) \cdot 3 \cdot 59 \cdot 14 = (-1) \cdot 76 \cdot 14 = 25 \cdot 14 = 47 \bmod 101$. She publishes this key $h = 47$.

Bob computes first $c_1 = g^y = 2^{59} \bmod 101$. His computation is similar with this of Alice, the result will be $c_1 = 2 \cdot 47 = 94 \bmod 101$. He also computes $c_2 = mh^y = 60 \cdot 47^{59} \bmod 101$. In order to achieve this, he observes that $59 = 32 + 16 + 8 + 2 + 1$ and he computes by repeated squaring those powers of 47:

$$47 \rightsquigarrow 47^2 = 88 \rightsquigarrow 47^4 = 68 \rightsquigarrow 47^8 = 79 \rightsquigarrow 47^{16} = 80 \rightsquigarrow 47^{32} = 37.$$

So $47^{59} = 37 \cdot 80 \cdot 79 \cdot 88 \cdot 47 = 37 \cdot (-21) \cdot (-22) \cdot (-13) \cdot 47 = 37 \cdot 58 \cdot (-1) \cdot 5 = (-1) \cdot 84 \cdot 58 = 17 \cdot 58 = 77 \bmod 101$. Now $c_2 = 60 \cdot 77 = 41 \cdot 24 = 75 \bmod 101$. So Bob publishes $(c_1, c_2) = (94, 75)$.

Alice computes $m = c_2(c_1^k)^{-1} = 75 \cdot (94^{58})^{-1}$. She recalls that $58 = 32 + 16 + 8 + 2$ and again by successive squaring she gets:

$$94 \rightsquigarrow 94^2 = 7^2 = 49 \rightsquigarrow 94^4 = 78 \rightsquigarrow 94^8 = 23^2 = 24 \rightsquigarrow 94^{16} = 71 \rightsquigarrow 94^{32} = 30^2 = 92.$$

So $94^{58} = 92 \cdot 71 \cdot 24 \cdot 49 = 77$. She computes $77^{-1} \bmod 101$ with extended Euclid:

$$\begin{aligned}
101 &= \underline{77} + \underline{24} \\
&\to \underline{24} = -\underline{77} \\
\underline{77} &= 3 \cdot \underline{24} + \underline{5} \\
&\to \underline{5} = 4 \cdot \underline{77} \\
\underline{24} &= 4 \cdot \underline{5} + \underline{4} \\
&\to \underline{4} = (-17)\underline{77} \\
\underline{5} &= \underline{4} + 1 \\
&\to 1 = 21 \cdot \underline{77}.
\end{aligned}$$

So $m = 75 \cdot 21 \bmod 101 = 60$ and the decryption was successful.

Exercise 13 *Paillier cryptosystem for* $N = 35$. *Find a secret key, encrypt the message* $m = 24$ *and show how the decryption works.*

As $\varphi(35) = 4 \cdot 6 = 24$ we see that $\gcd(35, 24) = 1$, so $N = 35$ is a good choice. The secret key is a number d such that:

$$\begin{aligned}
d &= 1 \bmod 35, \\
d &= 0 \bmod 24.
\end{aligned}$$

If $x = 24^{-1} \bmod 35$ then $d = 24x$ is a good choice for d. We apply the extended Euclid algorithm:

$$\begin{aligned} 35 &= \underline{24} + \underline{11} \\ &\to \underline{11} = -\underline{24} \\ \underline{24} &= 2 \cdot \underline{11} + \underline{2} \\ &\to \underline{2} = 3 \cdot \underline{24} \\ \underline{11} &= 5 \cdot \underline{2} + 1 \\ &\to 1 = (-16) \cdot \underline{24} = 19 \cdot \underline{24}. \end{aligned}$$

So $d = 24 \cdot 19 = 456$ is a good secret key.

The encryption is done modulo $35^2 = 1225$. We need an $r \in \mathbb{Z}_{1225}^{\times}$ randomly chosen. We take $r = 22$. The encrypted message will be:

$$c = (1+N)^m r^N \bmod N^2 = 36^{24} 22^{35} \bmod 1225.$$

But $24 = 16 + 8$ and the special powers of 36 mod 1225 are:

$$36 \rightsquigarrow 36^2 = 71 \rightsquigarrow 36^4 = 141 \rightsquigarrow 36^8 = 281 \rightsquigarrow 36^{16} = 561.$$

It follows that $36^{24} = 561 \cdot 281 = 841 \bmod 1225$.

In order to compute $22^{35} \bmod 1225$, we observe that $35 = 32 + 2 + 1$ and the special powers of 30 are:

$$22 \rightsquigarrow 22^2 = 484 \rightsquigarrow 22^4 = 281 \rightsquigarrow 22^8 = 561 \rightsquigarrow 22^{16} = 1121 \rightsquigarrow 22^{32} = 1016.$$

It follows that $30^{35} = 1016 \times 484 \times 22 = 393 \bmod 1225$. So $c = 841 \times 393 \bmod 1225 = 988$.

For the decryption we first compute:

$$t = c^d \bmod N^2 = 988^{456} \bmod 1225.$$

We observe that $456 = 256 + 128 + 64 + 8$. The special powers of 1075 are:

$$988 \rightsquigarrow 988^2 = 1044 \rightsquigarrow 988^4 = 911 \rightsquigarrow 988^8 = 596 \rightsquigarrow 988^{16} = 1191 \rightsquigarrow 988^{32} = 1156 \rightsquigarrow$$

$$\rightsquigarrow 988^{64} = 1086 \rightsquigarrow 988^{128} = 946 \rightsquigarrow 988^{256} = 666.$$

So $t = 666 \cdot 946 \cdot 1086 \cdot 1191 \cdot 596 \bmod 1225 = 841$. Now we finally decrypt:

$$m = \frac{t-1}{N} = \frac{841-1}{35} = 24.$$

Exercise 14 *A message encrypted according to the cryptosystem Goldwasser-Micali modulo* 77 *starts with* 67, 37, 68, 60. *Decrypt this word.*

The secret key modulo 77 is the prime factor pair $(7, 11)$. Modulo 7, the sequence is 4, 2, 5, 4. Only 1, 4 and 2 are squares modulo 7, so the message is 0, 0, 1, 0.

Exercise 15 *How many generators has the cyclic group* $(\mathbb{F}_{p^n}^{\times}, \cdot, 1)$*? If g is a generator of the group* $(\mathbb{F}_{25}^{\times}, \cdot, 1)$*, find all its generators.*

The cyclic group $(\mathbb{F}_{p^n}^{\times}, \cdot, 1)$ has $p^n - 1$ elements, and so is isomorphic with the group $(\mathbb{Z}_{p^n-1}, +, 0)$. This group has $\varphi(p^n - 1)$ generators, where $\varphi(m)$ is Euler's function. If $p^n = 25$, the cyclic group $(\mathbb{Z}_{24}, +, 0)$ has $\varphi(24) = \varphi(3)\varphi(8) = 2 \cdot 4 = 8$ generators. They are $\{1, 5, 7, 11, 13, 17, 19, 23\}$. In conclusion, the set of generators of $(\mathbb{F}_{25}^{\times}, \cdot, 1)$ is $\{g, g^5, g^7, g^{11}, g^{13}, g^{17}, g^{19}, g^{23}\}$.

Exercise 16 *How many generators has the cyclic group $(\mathbb{Z}_{p^n}^{\times}, \cdot, 1)$, where $n \geq 2$ and p is an odd prime? If g is a generator of the group $(\mathbb{Z}_{25}^{\times}, \cdot, 1)$, find all its generators.*

The cyclic group $(\mathbb{Z}_{p^n}^{\times}, \cdot, 1)$ has $\varphi(p^n) = p^n - p^{n-1}$ elements, and so is isomorphic with the cyclic group $(\mathbb{Z}_{p^n - p^{n-1}}, +, 0)$. This group has $\varphi(p^n - p^{n-1}) = \varphi(p^{n-1}(p-1)) = (p^{n-1} - p^{n-2})\varphi(p-1)$. If $p^n = 25$ then $p^n - p^{n-1} = 20$. The cyclic group $(\mathbb{Z}_{20}, +, 0)$ has $\varphi(20) = \varphi(4)\varphi(5) = 2 \cdot 4 = 8$ generators. They are $\{1, 3, 7, 9, 11, 13, 17, 19\}$. In conclusion, the set of generators of $(\mathbb{Z}_{25}^{\times}, \cdot, 1)$ is $\{g, g^3, g^7, g^9, g^{11}, g^{13}, g^{17}, g^{19}\}$.

2 Attack methods

Exercise 17 *Find a factorisation of $N = 77$ knowing a pair of keys $(e, d) = (43, 7)$.*

The number $ed - 1 = 300 = 4 \cdot 75$. We choose $x = 2$ in $\mathbb{Z}_{77}$. We observe that $\gcd(2, 77) = 1$, so this choice does not directly produce a factorisation of 77. Now $75 = 64 + 8 + 2 + 1$ and the successive squares of 2 are:

$$2 \rightsquigarrow 2^2 = 4 \rightsquigarrow 2^4 = 16 \rightsquigarrow 2^8 = 25 \rightsquigarrow 2^{16} = 9 \rightsquigarrow 2^{32} = 4 \rightsquigarrow 2^{64} = 16.$$

So $b = 2^{75} = 16 \cdot 25 \cdot 4 \cdot 2 \bmod 77 = 3200 \bmod 77 = 43$. Hence $b - 1 = 42$ and $\gcd(77, 42)$ is computed as follows:

$$\begin{aligned} 77 &= \underline{42} + \underline{35} \\ \underline{42} &= \underline{35} + \underline{7} \\ \underline{35} &= 5 \cdot \underline{7} + 0. \end{aligned}$$

So $\gcd(77, 42) = 7$ and we get the factorisation $77 = 7 \cdot 11$.

Exercise 18 *Find a factorisation of $N = 77$ knowing that $\varphi(77) = 60$.*

We know that:

$$\varphi(N) = (p-1)(q-1) = pq - p - q + 1 = N - (p+q) + 1,$$

$$p + q = N + 1 - \varphi(N) = 78 - 60 = 18.$$

We consider the equation:

$$X^2 - 18X + 77 = 0.$$

Here $\Delta = 18^2 - 4 \cdot 77 = 324 - 308 = 16$, $\sqrt{\Delta} = 4$, $X_{1,2} = (18 \pm 4)/2 = \{11, 7\}$, so the factorisation is $77 = 11 \cdot 7$.

Exercise 19 *RSA modulo $N = 77$. One encrypts the unknown message m using the encryption key $e_1 = 7$ and gets $c = 47$ and the same message using the key $e_2 = 11$ produces the cypher $c = 38$. Find m without using the factorisation of N.*

As $\gcd(e_1, e_2) = \gcd(11, 7) = 1$, and because at least one cypher is prime with 77, one can apply the following method. We compute:

$$\begin{aligned} t_1 &= e_1^{-1} \bmod e_2, \\ t_2 &= \frac{e_1 t_1 - 1}{e_2}. \end{aligned}$$

It is more convenient to recall the keys $e_1 = 11$ and $e_2 = 7$, because it is easyer to compute modular inverses modulo 7. Then $t_1 = 11^{-1} \mod 7 = 4^{-1} \mod 7 = 2$ and $t_2 = (22-1)/7 = 3$. So $e_1 t_1 - e_2 t_2 = 1$. So:

$$m^1 = m^{e_1 t_1 - e_2 t_2} = (c_1^{t_1})(c_2^{t_2})^{-1} = 38^2 (47^3)^{-1} \bmod 77.$$

But $38^2 = 58$ and $47^3 = 27$. We compute now $27^{-1} \bmod 77$.

$$\begin{aligned}
77 &= 2 \cdot \underline{27} + \underline{23} \\
&\rightarrow \underline{23} = (-2) \cdot \underline{27} \\
\underline{27} &= \underline{23} + \underline{4} \\
&\rightarrow \underline{4} = 3 \cdot \underline{27} \\
\underline{23} &= 5 \cdot \underline{4} + \underline{3} \\
&\rightarrow \underline{3} = (-17) \cdot \underline{27} \\
\underline{4} &= \underline{3} + 1 \\
&\rightarrow 1 = 20 \cdot \underline{27}.
\end{aligned}$$

It follows $27^{-1} \bmod 77 = 20$ and $m = 58 \cdot 20 \bmod 77$ which yields $m = 5$. (This can be seen also without calculator: $58 \cdot 20 = 116 \cdot 10 = 39 \cdot 10 = 78 \cdot 5 = 1 \cdot 5 = 5 \bmod 77$.)

Exercise 20 *Perform Hastag's Broadcast Attack in the situation that a user encoded an unknown message m using the encryption key $e = 7$. In RSA modulo 988027 he gets $c = 505035$, and in RSA modulo 7387 he gets $c = 2801$. Find the value of m without using the factorisation of the moduli.*

It is interesting first if the moduli 988027 and 7387 are relatively prime. This is the case, because Euclid's algorithm reveals:

$$\begin{aligned}
988027 &= \underline{7387} \cdot 133 + \underline{5556} \\
\underline{7387} &= \underline{5556} + \underline{1831} \\
\underline{5556} &= \underline{1831} \cdot 3 + \underline{63} \\
\underline{1831} &= \underline{63} \cdot 29 + \underline{4} \\
\underline{63} &= \underline{4} \cdot 15 + \underline{3} \\
\underline{4} &= \underline{3} + 1
\end{aligned}$$

In order to solve the system of congruences:

$$\begin{aligned}
x &= 505035 \bmod 988027, \\
x &= 2801 \bmod 7387,
\end{aligned}$$

we must find out both $7387^{-1} \bmod 988027$ and $988027^{-1} \bmod 7387$. For both, the divisions with remainder from above are used.

It turns out $7387^{-1} \bmod 988027 = 250919$ and $988027^{-1} \bmod 7387 = 5556^{-1} \bmod 7387 = 5511$

Now recall that the solution of:

$$\begin{aligned}
x &= u \bmod A, \\
x &= v \bmod B,
\end{aligned}$$

where $\gcd(A, B) = 1$ is, by the effective Chinese Remainder Theorem,

$$x = [uB(B^{-1} \bmod A) + vA(A^{-1} \bmod B)] \bmod AB.$$

$$x = [505035 \cdot 7387 \cdot 250919 + 2801 \cdot 988027 \cdot 5511] \bmod 988027 \cdot 7387.$$

We cannot evaluate this expression using the pocket calculator. This can be done by hand, or using the value type BigInteger from the package System.Numerics in C# or from Java. We find out that:

$$x = 1280000000 = 2^7 \cdot 10^7,$$

which leads us to the supposition that $m = 20$. According to the theory of the Hastag Broadcast Attack, this value is sure only if, in this case, we had solved a system of 7 congruences with pairwise relatively prime moduli. As we solved only a system of two congruences, this has merely the value of a guess. What we need now, is to check that this message encodes as given, according to one of the moduli. If so, then we are done.

In other words, we must compute for example $c = 20^7 \bmod 7387$.

$$20 \rightsquigarrow 20^2 = 400 \rightsquigarrow 20^4 = 4873,$$

so $20^7 = 20 \cdot 400 \cdot 4873 = 2801$. So the guess $m = 20$ was correct.

Exercise 21 *Perform Wiener's attack for the public key* $(N, e) = (90581, 17993)$.

We develop:

$$\frac{e}{N} = \frac{17993}{90581}$$

as a continuous fraction. In order to do this, we apply Euclid's algorithm to the pair $(N, e) = (90581, 17993)$.

$$\begin{aligned}
90581 &= 17993 \cdot \underline{5} + 616\\
17993 &= 616 \cdot \underline{29} + 129\\
616 &= 129 \cdot \underline{4} + 100\\
129 &= 100 \cdot \underline{1} + 29\\
100 &= 29 \cdot \underline{3} + 13\\
29 &= 13 \cdot \underline{2} + 3\\
13 &= 3 \cdot \underline{4} + 1
\end{aligned}$$

This can be written as:

$$\begin{aligned}
\frac{90581}{17993} &= 5 + \frac{616}{17993}\\
\frac{17993}{616} &= 29 + \frac{129}{616}\\
\frac{616}{129} &= 4 + \frac{100}{129}\\
\frac{129}{100} &= 1 + \frac{29}{100}\\
\frac{100}{29} &= 3 + \frac{13}{29}\\
\frac{29}{13} &= 2 + \frac{3}{13}\\
\frac{13}{3} &= 4 + \frac{1}{3}
\end{aligned}$$

This leads to the following continuous fraction:

$$\frac{e}{N} = \frac{17993}{90581} = 0 + \cfrac{1}{5 + \cfrac{1}{29 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{2 + \cfrac{1}{4 + \cfrac{1}{3}}}}}}}}.$$

The first three convergents are:

$$0, \frac{1}{5}, \cfrac{1}{5 + \cfrac{1}{29}} = \frac{29}{5 \cdot 29 + 1} = \frac{29}{146}.$$

The convergent 0 is of course of no use. If $\frac{k}{d} = \frac{1}{5}$ then let us try with a supposed value of:

$$\varphi(N) = \frac{ed - 1}{k} = 17993 \cdot 5 - 1 = 89964.$$

Then:

$$p + q = N - \varphi(N) + 1 = 90581 - 89964 + 1 = 618,$$

and we try to solve the equation:

$$X^2 - 618X + 90581 = 0.$$

$$\Delta = 618^2 - 4 \cdot 90581 = 381924 - 362324 = 19600,$$

$$\sqrt{19600} = 140,$$

$$X_{1,2} = (618 \pm 140)/2 = 309 \pm 70 = \{379, 239\}.$$

As $379 \cdot 239 = 90581$ this is the factorisation we were looking for.

Exercise 22 *Perform the Franklin-Reiter (Coppersmith) attack in the following situation. One encrypts a message m using RSA modulo $N = 391$ with public key $e = 3$ and gets the cypher $c_1 = 213$. He encrypts the message $m + 1$ using the same public key and gets $c_2 = 16$. Find out m without using the factorisation of* 391.

If we write down the RSA encryption in the two cases, they look like:

$$\begin{array}{rcl} m^3 & = & 213 \bmod 391 \\ (m+1)^3 & = & 16 \bmod 391 \end{array}$$

Consider the polynomials $(x+1)^3 - 16 = x^3 + 3x^2 + 3x + 376 \in \mathbb{Z}_{391}[X]$ and $x^3 - 213 = x^3 + 178 \in \mathbb{Z}_{391}[X]$. We compute the greatest common divisor of those polynomials using Euclid's algorithm in the ring $\mathbb{Z}_{391}[X]$. The corresponding norm, which decreases at every step, is the degree of the polynomials.

$$x^3 + 178 = (x^3 + 3x^2 + 3x + 376)(1) + (388x^2 + 388x + 193)$$

$$x^3 + 3x^2 + 3x + 376 = (388x^2 + 388x + 193)(130x + 260) + (326x + 244)$$

$$388x^2 + 388x + 193 = (326x + 244)(373x + 137) + (0)$$

The computation of these steps contain more modular inverses, that we do not present here in detail. The last non-zero polynomial is $326x + 244$. We observe that $326^{-1} \bmod 391 = 6$ and $6 \cdot 244 = 291 \bmod 391$, so $326x + 244 = 326(x + 291) = 326(x - 100) \bmod 391$. We conclude that $m = 100$ is the solution, which is true by verification.

Exercise 23 *Factorise the number $N = 1927$ using Pollard's Rho with start value $x = 10$.*

Let $x_0 = y_0 = 10$. For $f(x) = x^2 + 1 \bmod 1927$ we consider the sequences given by $x_i = f(x_{i-1})$ and $y_i = f(f(y_{i-1}))$. One gets:

$$\begin{aligned} x_1 &= 101 \\ y_1 &= 567 \\ \gcd(N, |x_1 - y_1|) &= 1 \end{aligned}$$

$$\begin{aligned} x_2 &= 567 \\ y_2 &= 1558 \\ \gcd(N, |x_2 - y_2|) &= 1 \end{aligned}$$

$$\begin{aligned} x_3 &= 1608 \\ y_3 &= 1232 \\ \gcd(N, |x_3 - y_3|) &= 47 \end{aligned}$$

The last step is maybe worth to be done in more detail. One has by repeated subtraction $\gcd(1927, 376) = \gcd(47, 376) = \gcd(47, 8 \cdot 47) = 47$. Repeated subtraction is very easy to be performed on a pocket calculator. Finally we get the factorisation $1927 = 41 \cdot 47$.

Exercise 24 *Factorise the number $N = 1927$ using Pollard's $p - 1$ with start value $x = 10$.*

We construct the sequence (x_n) with $x_1 = x$ and $x_{n+1} = x_n^{n+1} \mod N$. After every new computed x_n we check if $\gcd(N, x_n - 1) \neq 1$. In the moment that we get a gcd different of 1, we have a divisor. So we construct the sequence: $10^2 \bmod 1927 = 100$, $10^6 \bmod 1927 = 1814$, $10^{24} \bmod 1927 = 37$, $10^{120} \bmod 1927 = 862$. To this point, we observe that $\gcd(861, 1927) = \gcd(861, 205) = \gcd(41, 205) = \gcd(41, 5 \cdot 41) = 41$. We deduce the factorisation $1927 = 41 \cdot 47$.

Exercise 25 *Factorise the number $N = 697$ using Fermat's deterministic algorithm.*

We start with $x = [\sqrt{697}] + 1 = 27$ and $z = x^2 - N = 32$. At every step x is increased with 1 and z is increased with $2x + 1$, where the old value of x is considered. We observe that the difference $x^2 - z$ remains constant N. This happens untill z becomes a perfect square. So we have the pairs $(28, 32 + 54 + 1 = 87)$, $(29, 87 + 56 + 1 = 144)$. But now $144 = 12^2$ and:

$$697 = 29^2 - 12^2 = (29 - 12)(29 + 12) = 17 \cdot 41.$$

Exercise 26 *Show that $g = 3$ is a generator for the cyclic group $(\mathbb{F}_{43}^\times, \cdot, 1)$. Use the method Baby Step - Giant Step to find the discrete logarithm of the element $x = 11$ according to this generator.*

The group has $42 = 2 \cdot 3 \cdot 7$ elements. The maximal divisors of 42 are $21 = 16 + 4 + 1$, $14 = 8 + 4 + 2$ and $6 = 4 + 2$. The special powers of 3 mod 43 are the following:

$$3 \rightsquigarrow 3^2 = 9 \rightsquigarrow 3^4 = 38 = -5 \rightsquigarrow 3^8 = 25 = -18 \rightsquigarrow 3^{16} = 4 \cdot (-5) = 23.$$

Attention, computations are done modulo 43.

Now $3^{21} = (-20) \cdot (-5) \cdot 3 = 14 \cdot 3 = 42 = -1$, $3^{14} = 25 \cdot (-5) \cdot 9 = (-18) \cdot (-1) \cdot 2 = 36$ and $3^6 = (-5) \cdot 9 = 3$. As none of them is 1, $g = 3$ has order 42 and generates this cyclic group.

The square root $L = [\sqrt{42}] + 1$ is $L = 7$. The generator g to the power L is:

$$h = 3^7 \bmod 43 = (-5) \cdot 9 \cdot 3 \bmod 43 = (-2) \cdot 3 \bmod 43 = -6 \bmod 43 = 37 \bmod 43.$$

The first list L_1 consists of the powers of $h = 37$ from 0 to 6. They are:

$$1, 37, 36, 42, 6, 7, 1$$

The inverse of the generator $z = 3^{-1} \bmod 43 = 29$ because $43 = 3 \cdot 14 + 1$ so modulo 43 one has $1 = (-14) \cdot 3 = 29 \cdot 3$. We produce elements of the second list $11 \cdot 29^k$ untill we find a collision with the first list:

$$11, 18, 6$$

The 4-th element of the first list and the 2-nd element of the second list are equal. So the discrete logarithm is $7 \cdot 4 + 2 = 30$. Indeed, $3^{30} \bmod 43 = 3^{16}3^8 3^4 3^2 = (-20) \cdot (-18) \cdot (-5) \cdot 9 \bmod 43 = 14 \cdot (-18) \cdot 9 \bmod 43 = 15 \cdot (-5) \bmod 43 = -75 + 86 \bmod 43 = 11$.

Exercise 27 *Shanks' algorithm is modified in the following way: instead of multiplications, additions modulo $n = 2k$ are computed. The number z which was supposed not to be a square modulo p is replaced by 1. The function $x^{2^i} \bmod p$ is replaced with $2^i x \bmod n$. The numbers Q and S are chosen such that Q is odd and $n = 2^s Q$. The tests* **untill** $(t = 1)$ **do** *are now replaced by tests* **untill** $(t = 0)$ **do** *. What does the algorithm compute for some input x?*

The algorithm normally finds square roots in the cyclic group $(\mathbb{Z}_p^\times, \cdot, 1)$ - that means, that for given x it finds an element y such that $y \cdot y = x$, if such an element does exist. Now the algorithm works in the cyclic group $(\mathbb{Z}_n, +, 0)$ and to given element x it finds an element y such that $y + y = x$, if such an element does exist. As $y + y = 2 \cdot y$, the existence of the half depends on the parity of n. If n is even, then the homomorphism $t : \mathbb{Z}_n \to \mathbb{Z}_n$ given by $t(x) = 2x$ has a kernel consisting of two elements: $Ker\ t = \{0, n/2\}$. It follows that only a half of the elements are in the image of t, and for the other elements the algorithm gives a negative answer.

Exercise 28 *Shanks' algorithm is modified in the following way: instead of multiplications modulo a prime p, multiplications modulo 98 are computed. The function $x^{2^i} \bmod p$ is replaced with $x^{2^i} \bmod 98$. The numbers Q and S are chosen such that Q is odd and $42 = 2^s Q$. The number z, which was not supposed to be a square modulo p, is chosen $z = 3$. What does the algorithm compute for the input $x = 71$?*

We recall that the ring $\mathbb{Z}$ modulo $98 = 2 \cdot 49$ has a cyclic multiplicative group of units, and this group $(\mathbb{Z}_{98}^\times, \cdot, 1)$ has $\varphi(98) = (2-1)(49-7) = 42$ elements. The number $z = 3$ belongs to this cyclic group and is not a square modulo 98. Indeed, $42 = 2 \cdot 21$, and $21 = 16 + 4 + 1$. The following computations are done modulo 98:

$$3 \rightsquigarrow 3^2 = 9 \rightsquigarrow 3^4 = 81 = (-17) \rightsquigarrow 3^8 = 93 = (-5) \rightsquigarrow 3^{16} = 25,$$
$$3^{21} = 25 \cdot (-17) \cdot 3 = -1,$$

so indeed 3 is not a square modulo 98.

As the input 71 is not divisible by 2 or by 7, it belongs to the cyclic group, $z = 3$ belongs to the cyclic group as well, and all multiplication results will remain in this cyclic group. So the algorithm finds a square root of 71 modulo 98, which is 85. The element $-85 = 13$ is the other square root.

Exercise 29 *The baby step - giant step algorithm is modified in the following way: instead of multiplications modulo a prime p, additions modulo n are computed. Instead of $[\sqrt{p-1}]$, one computes $c = [\sqrt{n}]$. For generator g one takes a number g such that $\gcd(n, g) = 1$. Instead of $z = g^{-1} \bmod p$, it computes $z = -g \bmod n$. Let $h = g \cdot c \bmod n$. The list L_1 consists of the elements $jh \bmod n$ while the list L_2 consists of the arithmetic progression $(x + zj) \bmod n$, where x is the input. What does the algorithm compute?*

The algorithm in its original form worked over the cyclic group $(\mathbb{Z}_p^\times, \cdot, 1)$ and produced the discrete logarithm of x, that is an integer λ such that $g^\lambda = x$. All the modifications let the algorithm to work on the cyclic group $(\mathbb{Z}_n, +, 0)$ instead. If $a \cdot b$ is replaced by the operation $a + b$, the exponentiation a^b corresponds to the repeated addition, that is $a \cdot b$. So the number λ found by the algorithm has the property that $g \cdot \lambda = x$. This means that $\lambda = ((g^{-1} \bmod n) \cdot x) \bmod n$.

Exercise 30 *The baby step - giant step algorithm is modified in the following way: instead of multiplications modulo a prime p, multiplications modulo 98 are computed. Instead of $[\sqrt{p-1}]$, one computes $c = 7 = [\sqrt{42}] + 1$. For generator g one takes the number 3. Instead of $z = g^{-1} \bmod p$, one takes $z = 33$. Let $h = 3^7 \bmod 98 = 31$. Let the input x be $x = 37$. The list L_1 consists of the powers $31^j \bmod 98$ while the list L_2 consists of the geometric progression $(37 \cdot 33^j) \bmod 98$. What does the algorithm compute?*

We recall that the ring $\mathbb{Z}$ modulo $98 = 2 \cdot 49$ has a cyclic multiplicative group of units, and this group $(\mathbb{Z}_{98}^\times, \cdot, 1)$ has $\varphi(98) = (2-1)(49-7) = 42$ elements. The number $z = 3$ belongs to this cyclic group and is a generator of the cyclic multiplicative group. Indeed, $42 = 2 \cdot 3 \cdot 7$, the maximal divisors are $21 = 16 + 4 + 1$, $14 = 8 + 4 + 2$ and $6 = 4 + 2$. With the special powers computed in the exercise above, it is not difficult to see that $3^{42} \neq 1$, $3^{14} \neq 1$ and $3^6 \neq 1$, so 3 is a generator of the cyclic group. Moreover, 33 is the multiplicative inverse of 3 modulo 98. The algorithm computes the discrete logarithm of 37 in the basis 3 modulo 98, and this is 32.

3 Signatures and key exchange protocols

Exercise 31 *Compute an example of DSA with $p = 83$ and $q = 41$. Use $H(m) = m$ for simplicity. The message is $m = 70$.*

Indeed 41 is a divisor of $(83 - 1)$. We must find an element $g \bmod 83$ that generates a cyclic group of order 41. Consider $u = 60$.

$$60^2 \bmod 83 = 31 \neq 1,$$

so $g = 31 \bmod 83$ generates a group G of order 41 inside $(\mathbb{Z}_{83}^\times, \cdot, 1)$. Recall that $h = H(m) = H(70) = 70$. The signer choose the secret key $x = 10$ and publishes the public key:

$$y = 31^{10} \bmod 83 = 27.$$

She also chooses a temporary key $0 < k < 41$. She takes $k = 16$ and computes:

$$r = (g^k \bmod p) \bmod q = (31^{16} \bmod 83) \bmod 41 = 59 \bmod 41 = 18.$$

$$s = (h + xr)k^{-1} \bmod q = (70 + 10 \cdot 18) \cdot 16^{-1} \bmod 41 = 250 \cdot 18 \bmod 41 = 4 \cdot 18 \bmod 41 = 31.$$

The signer sends $(r, s) = (18, 31)$ together with the message $m = 70$.

The verifier first computes $h = H(m) = 70$. She also computes:

$$a = hs^{-1} \bmod q = 70 \cdot 31^{-1} \bmod 41 = 29 \cdot 4 \bmod 41 = (-12) \cdot 4 \bmod 41 = -48 \bmod 41 = 34,$$

$$b = rs^{-1} \bmod q = 18 \cdot 31^{-1} \bmod 41 = 18 \cdot 4 \bmod 41 = 72 \bmod 41 = 31.$$

Finally she uses the public key of the sender, $y = 27$ and she computes:

$v = (g^a y^b \bmod p) \bmod q = (31^{34} 27^{31} \bmod 83) \bmod 41 = (9{\cdot}25 \bmod 83) \bmod 41 = 59 \bmod 41 = 18.$

As $v = 18 = r$, the verifier ACCEPTS.

Exercise 32 *Compute an instance of the key-exchange protocol MQV using* $g = 60$, *which is a generator of the cyclic group* $(\mathbb{Z}_{83}^{\times}, \cdot, 1)$.

Alice and Bob have long-lasting pairs (public key, secret key), like:

$$(A = g^a, a) \;\; ; \;\; (B = g^b, b).$$

For a new key-exchange, they generate some temporary keys:

$$(C = g^c, c) \;\; ; \;\; (D = g^d, d).$$

In our case, Alice chooses $a = 10$ and $c = 11$. She computes $A = 44$ and $C = 67$. Bob chooses $b = 12$ and $d = 13$. He computes $B = 36$ and $D = 2$. Bob knows A and C. Alice knows B and D. The number L is defined as:

$$L = \left\lceil \frac{[\log_2 |G|] + 1}{2} \right\rceil = \left\lceil \frac{6+1}{2} \right\rceil = 4.$$

The number $2^L = 16$. Alice computes:

$$s_A = 2^L + (C \bmod 2^L) = 16 + (67 \bmod 16) = 19,$$
$$t_A = 2^L + (D \bmod 2^L) = 16 + (2 \bmod 16) = 18,$$
$$h_A = c + s_a a = 11 + 19 \cdot 10 = 201,$$
$$P_A = (DB^{t_A})^{h_A} = (2 \cdot 36^{18})^{201} \bmod 83 = (2 \cdot 16)^{201} \bmod 83 = 32^{201} \bmod 83 = 74.$$

On his turn, Bob computes:

$$s_B = 2^L + (D \bmod 2^L) = 16 + (2 \bmod 16) = 18,$$
$$t_B = 2^L + (C \bmod 2^L) = 16 + (67 \bmod 16) = 19,$$
$$h_B = d + s_B b = 13 + 18 \cdot 12 = 13 + 216 = 229,$$
$$P_B = (CA^{t_B})^{h_B} = (67 \cdot 44^{19})^{229} \bmod 83 = (67 \cdot 4)^{229} \bmod 83 = 268^{229} \bmod 83 = 74.$$

So Bob and Alice independently compute the same private key.

4 Advanced protocols

Exercise 33 *Shamir secret sharing in the field* $\mathbb{Z}_{41}$. *An unknown degree two polynomial* $f \in \mathbb{Z}_{41}[x]$ *is evaluated, and three users get on their memory sticks the following pairs* $(x, f(x)) \in \mathbb{Z}_{41}^2$ *which are respectively* $(1, 10)$, $(2, 26)$ *and* $(3, 14)$. *Find out the shared secret* $f(0)$.

Denote the polynomial $f(x) = a + bx + cx^2$. We write the conditions in the form of a system of linear equations:

$$\begin{aligned} a + \;\; b + \;\; c &= 10 \\ a + 2b + 4c &= 26 \\ a + 3b + 9c &= 14 \end{aligned}$$

We solve the system using Gauss' method. All computations are done modulo 41.

We subtract the first equation from the other two:

$$\begin{aligned} a+b+\ c &= 10 \\ b+3c &= 16 \\ 2b+8c &= 4 \end{aligned}$$

The second equation is multiplied with 2 and subtracted from the last one:

$$\begin{aligned} a+b+\ c &= 10 \\ b+3c &= 16 \\ 2c &= 13 \end{aligned}$$

As $2^{-1} \bmod 41 = 21$, $c = 13 \cdot 21 \bmod 41 = 39 \cdot 7 \bmod 41 = (-2) \cdot 7 \bmod 41 = 27$. If we replace c in the first two equations, we get:

$$\begin{aligned} a+b+27 &= 10 \\ b+81 &= 16 \end{aligned}$$

So $b = 17$ and $a + 44 = 10$, $a = 7$. The shared secret is $f(0) = a = 7$.

Exercise 34 *Compute an instance of the Oblivious Transfer protocol in the group* $(\mathbb{Z}_{61}^{\times}, \cdot, 1)$ *with generator* $g = 30$*. The Sender chooses* $c = 29$*, the Receiver chooses the secret bit* $b = 0$ *and the secret key* $x = 31$*, the Sender chooses the temporary key* $k = 32$ *and must send the messages* $m_0 = 33$ *and* $m_1 = 53$*. For simplicity consider the hash function* $H(x) = x$*.*

The Receiver computes the public keys:

$$h_0 = g^x = 30^{31} \bmod 61 = 31,$$

$$h_1 = c/h_0 = 29 \cdot 31^{-1} \bmod 61 = 29 \cdot 2 \bmod 61 = 58.$$

He sends $h_0 = 31$ to the Sender. The Sender computes $h_1 = 58$ exactly like the Receiver. He merely computes:

$$c_1 = g^k = 30^{32} \bmod 61 = 15,$$
$$h_0^k = 31^{32} \bmod 61 = 15,$$
$$h_1^k = 58^{32} \bmod 61 = 9.$$
$$e_0 = m_0 \oplus H(h_0^k) = 33 \oplus 15 = 100\,001 \oplus 001\,111 = 101\,110,$$
$$e_1 = m_1 \oplus H(h_1^k) = 53 \oplus 9 = 110\,101 \oplus 001\,001 = 111\,100,$$

The Sender sends c_1, e_0 and e_1 to the Receiver. The receiver computes:

$$c_1^x = 15^{31} \bmod 61 = 15,$$

$$m_0 = e_0 \oplus H(c_1^x) = 101\,110 \oplus 001\,111 = 100\,001 = 33.$$

Exercise 35 *Recall the fact that* $g = 31$ *generates a group* G *of order* 41 *in the group* $(\mathbb{Z}_{83}^{\times}, \cdot, 1)$*. Develop an instance of Schnorr's identification protocol in this group. Peggy's secret is the number* $x = 20$*. What is Peggy's public key? Peggy randomly chooses* $k = 11$*, and Victor sends the challenge* $e = 30$*. Compute the run step by step.*

Peggy's public key is the number:

$$y = 31^{20} \bmod 83 = 65.$$

Peggy randomly chooses $k = 11$ and sends to Victor:

$$r = 31^{11} \bmod 83 = 7.$$

Victor sends the challenge $e = 30$, Peggy answers with $s = k + xe = 11 + 20 \cdot 30 = 611$. Now Victor computes $g^s y^{-e}$. To this scope, he first compute $y^{-1} = 65^{-1} \bmod 83 = 23$. It follows that:

$$g^s y^{-e} = 31^{611} \cdot 23^{30} \bmod 83 = 31^{37} \cdot 23^{30} \bmod 83 = 29 \cdot 26 \bmod 83 = 7.$$

Victor got back the value of $r = 7$, so he ACCEPTS.

Exercise 36 *Recall the fact that $g = 31$ generates a group G of order 41 in the group $(\mathbb{Z}_{83}^{\times}, \cdot, 1)$. Develop an instance of the Pedersen Commitment in this group. Let $h \in G$ be $h = 48$. Peggy has the value $x = 1$. She chooses $a = 10$ and publishes the corresponding commitment $B_a(x) = h^x g^a$. For the protocol she chooses the values $(d, r, w) = (15, 20, 25)$ in $\mathbb{Z}_{41}$, and Victor sends the challenge $c = 27$. Compute the protocol step by step.*

We follow the protocol:

1. Peggy randomly chooses $d = 15$, $r = 20$, $w = 25$, all of them are considered mod 41.
2. Peggy publishes $B_a(x)$, α_1, α_2, where:

$$\alpha_1 = \begin{cases} g^r (B_a(x) h^{+1})^{-d}, & x = 1, \\ g^w, & x = -1. \end{cases}$$

$$\alpha_2 = \begin{cases} g^w, & x = 1, \\ g^r (B_a(x) h^{-1})^{-d}, & x = -1. \end{cases}$$

   In our case the secret is $x = 1$ so Peggy publishes:

$$B_a(x) = g^a h^x = 31^{10} 48^1 \bmod 83 = 27 \cdot 48 \bmod 83 = 51.$$

$$\alpha_1 = g^r (B_a(x) h^{+1})^{-d} = 31^{20} (51 \cdot 48)^{-15} \bmod 83 = 65 \cdot 44^{-1} \bmod 83 = 65 \cdot 17 \bmod 83 = 26.$$

$$\alpha_2 = g^w = 31^{25} \bmod 83 = 38.$$

3. Victor sends a random challenge $c = 27$.
4. Peggy computes:

$$d' = c - d = 27 - 15 = 12,$$

$$r' = w + ad' = 25 + 10 \cdot 12 = 145.$$

   and sends Victor:

$$(d_1, d_2, r_1, r_2) = \begin{cases} (d, d', r, r'), & x = 1, \\ (d', d, r', r), & x = -1. \end{cases}$$

   In our case, as $x = 1$, Peggy sends $(d_1, d_2, r_1, r_2) = (d, d', r, r') = (15, 12, 20, 145)$.

5. Victor verifies the following equalities:

$$\begin{aligned} c &= d_1 + d_2, \\ g^{r_1} &= \alpha_1 (B_a(x) h^{+1})^{d_1}, \\ g^{r_2} &= \alpha_2 (B_a(x) h^{-1})^{d_2}. \end{aligned}$$

   In our case,

$$c = 27 = 15 + 12 = d_1 + d_2,$$

$$g^{r_1} = 31^{20} \bmod 83 = 65 = 26 \times (51 \cdot 48)^{15} \bmod 83 = \alpha_1 (B_a(x) h^{+1})^{d_1},$$

$$g^{r_2} = 31^{145} \bmod 83 = 49 = 38 \cdot (51 \cdot 48^{-1})^{12} = \alpha_2 (B_a(x) h^{-1})^{d_2}.$$

6. Victor accepts Peggy's commitment only if all three equalities are verified. And so it is.

Exercise 37 *A commission of five senators decide to use an Electronic Vote protocol to take a decision. The senator i has a vote $v_i \in \{-1, 1\}$. He builds a degree 2 polynomial $f_i \in \mathbb{Z}_{101}[x]$ such that $f_i(0) = v_i$. There are three independent organisations which are the referees of the vote. They have the following RSA public keys $(143, 7)$, $(187, 11)$ and $(221, 5)$. Every senator $i = 1, 2, 3, 4, 5$ sends to the referee $j = 1, 2, 3$ the encrypted value of $f_i(j)$ using the public key of the referee. The referee will decrypt the messages but is allowed to communicate only the sum of the decrypted messages. The first referee gets the encrypted messages 42, 47, 47, 6, 48. The second referee gets the encrypted messages 150, 123, 17, 56, 40. The third referee gets the encrypted messages 13, 77, 120, 47 and 128. Did the commission accept or reject the resolution?*

First we must decrypt the messages got by the referees. The first referee makes RSA with $N = 143 = 11 \cdot 13$. So $\lambda = \mathrm{lcm}(10, 12) = 60$, and the private key is $7^{-1} \bmod 60 = 43$. Now he decrypts the messages:

$$42^{43} \bmod 143 = 3,$$

$$47^{43} \bmod 143 = 5,$$

$$47^{43} \bmod 143 = 5,$$

$$6^{43} \bmod 143 = 7,$$

$$48^{43} \bmod 143 = 9.$$

The first referee publishes $(3 + 5 + 5 + 7 + 9) \bmod 101 = 29$.

The second referee makes RSA with $N = 187 = 11 \cdot 17$. So $\lambda = \mathrm{lcm}(10, 16) = 80$, and the private key is $11^{-1} \bmod 80 = 51$. Now he decrypts the messages:

$$150^{51} \bmod 187 = 7,$$

$$123^{51} \bmod 187 = 13,$$

$$17^{51} \bmod 187 = 17,$$

$$56^{51} \bmod 187 = 23,$$

$$40^{51} \bmod 187 = 29.$$

The second referee publishes $(7 + 13 + 17 + 23 + 29) \bmod 101 = 89$.

The third referee makes RSA with $N = 221 = 13 \cdot 17$. So $\lambda = \mathrm{lcm}(12, 16) = 48$, and the private key is $5^{-1} \bmod 48 = 29$. Now he decrypts the messages:

$$13^{29} \bmod 221 = 13,$$

$$77^{29} \bmod 221 = 25,$$

$$120^{29} \bmod 221 = 35,$$
$$47^{29} \bmod 221 = 47,$$
$$128^{29} \bmod 221 = 59.$$

The third referee publishes $(13 + 25 + 35 + 47 + 59) \bmod 101 = 179 \bmod 101 = 78$.

Now senators and referees build the following system of linear equations modulo 101 using Gauss' method.

$$\begin{aligned} V + A + B &= 29, \\ V + 2A + 4B &= 89, \\ V + 3A + 9B &= 78. \end{aligned}$$

They subtract the first equation from the other two. The system becomes:

$$\begin{aligned} V + A + B &= 29, \\ A + 3B &= 60, \\ 2A + 8B &= 49. \end{aligned}$$

Two times the second equation means $2A + 6B = 120$, but $120 \bmod 101 = 19$. So the equation $2A + 6B = 19$ will be subtracted from the last one, and the system becomes:

$$\begin{aligned} V + A + B &= 29, \\ A + 3B &= 60, \\ 2B &= 30. \end{aligned}$$

The solution $B = 15$ implies immediately that $A = 15$ from the second equation, so $V = -1$ from the first equation. This is possible only if two senators were for the resolution and three senators were against the resolution. So the resolution was rejected.

Exercise 38 *Show that there is a recombination vector $\vec{r} = (r_1, r_2, r_3) \in \mathbb{Z}^3$ such that for all polynomial $f \in \mathbb{Z}[x]$ of degree at most 2,*

$$f(0) = r_1 f(1) + r_2 f(2) + r_3 f(3).$$

Check this recombination vector over a finite field, for at least one polynomial of degree 2 and one polynomial of degree 1.

If $f(x) = a + bx + cx^2$ then the following matrix equality takes place:

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} f(1) \\ f(2) \\ f(3) \end{pmatrix},$$

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{pmatrix}^{-1} \begin{pmatrix} f(1) \\ f(2) \\ f(3) \end{pmatrix}.$$

It follows that the coefficient $a = f(0)$ is equal with the scalar product between the first row of the inverse Vandermonde matrix and the vector consisting of the values computed at 1, 2 and 3. Let (r_1, r_2, r_3) the first row of the inverse Vandermonde matrix. This vector satisfies the relation:

$$\begin{pmatrix} r_1 & r_2 & r_3 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix},$$

$$\begin{aligned} r_1 + \ \ r_2 + \ \ r_3 &= 1, \\ r_1 + 2r_2 + 3r_3 &= 0, \\ r_1 + 4r_2 + 9r_3 &= 0. \end{aligned}$$

We solve this system by the Gauss method. We subtract the first equation from the other two:

$$\begin{aligned} r_1 + \ \ r_2 + \ \ r_3 &= +1, \\ r_2 + 2r_3 &= -1, \\ 3r_2 + 8r_3 &= -1. \end{aligned}$$

We subtract 3× the second equation from the last:

$$\begin{aligned} r_1 + \ \ r_2 + \ \ r_3 &= +1, \\ r_2 + 2r_3 &= -1, \\ 2r_3 &= +2. \end{aligned}$$

We find $r_3 = 1$, and by climbing the system back, $r_2 = -3$ and $r_1 = 3$. So the recombination vector is:

$$\vec{r} = (r_1, r_2, r_3) = (3, -3, 1).$$

Consider the polynomial $f(x) = 10 + 2x + 3x^2 \in \mathbb{Z}_{19}$. We see that $f(1) = 15$, $f(2) = 7$ and $f(3) = 5$. Then:

$$3 \cdot 15 - 3 \cdot 7 + 1 \cdot 5 = 45 - 21 + 5 = 29 = 10 \bmod 19,$$

and indeed $f(0) = 10$. For the polynomial $f(x) = 15 + 4x \in \mathbb{Z}_{19}$, we see that $f(1) = 0$, $f(2) = 4$ and $f(3) = 8$. Then:

$$3 \cdot 0 - 3 \cdot 4 + 1 \cdot 8 = -4 = 15 \bmod 19,$$

and indeed $f(0) = 15$.

Exercise 39 *Let $f \in \mathbb{Z}[X]$ be a polynomial of degree $d \leq n - 1$. Show that the polynomial fulfills the following relation:*

$$f(0) = \binom{n}{1} f(1) - \binom{n}{2} f(2) + \binom{n}{3} f(3) + \cdots + (-1)^{n-1} \binom{n}{n} f(n).$$

According to Lagrange's Interpolation formula,

$$f(x) = \sum_{k=1}^{n} f(k) \delta_k(x),$$

$$\delta_k(x) = \frac{(1-x) \ldots (k-1-x)(k+1-x) \ldots (n-x)}{(1-k) \ldots (k-1-k)(k+1-k) \ldots (n-k)}.$$

We evaluate $\delta_k(0)$:

$$\delta_k(0) = \frac{1 \cdot 2 \cdot \ldots (k-1)(k+1) \cdot \cdots \cdot n}{(-1)^{k-1}(k-1)!(n-k)!} = (-1)^{k-1} \frac{n!}{k!(n-k)!} = (-1)^{k-1} \binom{n}{k}.$$

We conclude that the vector:

$$\vec{r} = (r_1, r_2, \ldots, r_n) = \left(\binom{n}{1}, -\binom{n}{2}, \binom{n}{3}, \ldots, (-1)^{n-1} \binom{n}{n} \right)$$

is a general recombination vector for all polynomials of degree $d \leq n - 1$.

Exercise 40 *Alice's secret number is $x_1 = 5$, Bob's secret number is $x_2 = 10$, and Cesar's secret number is $x_3 = 51$, all of them modulo 101. They want to compute together $x_1x_2 + x_3$, without revealing their own secret numbers. For sharing values, they use only linear polynomials. In order to share their secret numbers, Alice uses the linear factor 10, Bob uses the linear factor 20 and Cesar uses the linear factor 40. For sharing the local multiplications, Alice uses the linear factor 17, Bob uses the linear factor 27 and Cesar uses the linear factor 71. Describe the protocol numerically.*

We know that the degree t of the sharing polynomials satisfy $2t \leq n - 1$. For $n = 3$ we get $t = 1$.

First Alice shares her value $x_1 = 5$ using the polynomial $5 + 10x$. She keeps the value 15 for herself, she sends Bob the value 25 and she sends Cesar the value 35. Bob shares his value $x_2 = 10$ using the polynomial $10 + 20x$. He sends 30 to Alice, keeps 50 for himseld and sends 70 to Cesar.

We first handle the **multiplicative** gate.

Alice has the values 15 and 30. She computes $15 \cdot 30 \bmod 101 = 46$ and she shares this product using the polynomial $46 + 17x$. So she keeps the value 63, sends Bob the value 80 and sends Cesar the value 97.

Bob has the values 25 and 50. He computes $25 \cdot 50 \bmod 101 = 38$ and he shares this product using the polynomial $38 + 27x$. So he sends 65 to Alice, he keeps 92 for himself and he sends 18 to Cesar.

Cesar has the values 35 and 70. He computes $35 \cdot 70 \bmod 101 = 26$ and he shares this product using the polynomial $26 + 71x$. So he sends 97 to Alice, 67 to Bob and keeps 37 for himself.

Alice has the values 63, 65 and 97 and computes her share from the final answer by applying the recombinatiuon vector $(3, -3, 1)$, which works for polynomials of degree ≤ 2. She gets:

$$3 \cdot 63 - 3 \cdot 65 + 97 = 91 \bmod 101.$$

Bob has the values 80, 92 and 67 and computes his share from the final answer. He gets:

$$3 \cdot 80 - 3 \cdot 92 + 67 = 31 \bmod 101.$$

Cesar has the values 97, 18 and 37 and computes his share from the final answer:

$$3 \cdot 97 - 3 \cdot 18 + 37 = 72 \bmod 101.$$

Now we handle the **additive** gate.

Cesar distributes his secret number $x_3 = 51$ using the polynomial $51 + 40x$. He sends Alice the value 91, he sends Bob the value 30 and he keeps for himself the value 70.

Alice computes her share from the sum, by adding her shares from the two terms:

$$91 + 91 = 81 \bmod 101.$$

Bob and respectively Cesar do the same thing:

$$31 + 30 = 61 \bmod 101,$$

$$72 + 70 = 41 \bmod 101.$$

Now it is the moment of the **collaborative disclosure**.

At this point Alice, Bob and Cesar announce their shares and compute together the final result:

$$3 \cdot 81 - 3 \cdot 61 + 41 = 60 + 41 = 0 \bmod 101,$$

which is of course $x_1x_2 + x_3 = 5 \cdot 10 + 51 = 101 = 0 \bmod 101$, but the secret numbers were never disclosed. We can observe that if Cesar discloses his secret, then Alice and Bob will directly compute x_1x_2, and because every one knows his secret number, they will both know the secret of the other. So Cesar's contribution is essential in keeping the general secret in this protocol.

Exercise 41 *A short analysis of the proof of the method called multiparty computation shows that this method works also directly in the ring of integers $\mathbb{Z}$ instead of the finite fields $\mathbb{F}_p$. Solve again the exercise 40, this time working with integers.*

We know that the degree t of the sharing polynomials satisfy $2t \leq n-1$. For $n = 3$ we get $t = 1$.

We first handle the **multiplicative** gate.

First Alice shares her value $x_1 = 5$ using the polynomial $5 + 10x$. She keeps the value 15 for herself, she sends Bob the value 25 and she sends Cesar the value 35. Bob shares his value $x_2 = 10$ using the polynomial $10 + 20x$. He sends 30 to Alice, keeps 50 for himseld and sends 70 to Cesar.

Alice has the values 15 and 30. She computes $15 \cdot 30 = 450$ and she shares this product using the polynomial $450 + 17x$. So she keeps the value 467, sends Bob the value 484 and sends Cesar the value 501.

Bob has the values 25 and 50. He computes $25 \cdot 50 = 1250$ and he shares this product using the polynomial $1250 + 27x$. So he sends 1277 to Alice, he keeps 1304 for himself and he sends 1331 to Cesar.

Cesar has the values 35 and 70. He computes $35 \cdot 70 = 2450$ and he shares this product using the polynomial $2450 + 71x$. So he sends 2521 to Alice, 2592 to Bob and keeps 2663 for himself.

Alice has the values 467, 1277 and 2521 and computes her share from the final answer by applying the recombination vector $(3, -3, 1)$, which works for polynomials of degree ≤ 2. She gets:

$$3 \cdot 467 - 3 \cdot 1277 + 2521 = 91.$$

Bob has the values 484, 1304 and 1331 and computes his share of the product. He gets:

$$3 \cdot 484 - 3 \cdot 1304 + 2592 = 132.$$

Cesar has the values 501, 1331 and 2663 and computes his share of the product:

$$3 \cdot 501 - 3 \cdot 1331 + 2663 = 173.$$

Now we handle the **additive** gate.

Cesar distributes his secret number $x_3 = 51$ using the polynomial $51 + 40x$. He sends Alice the value 91, he sends Bob the value 131 and he keeps for himself the value 171.

Alice computes her share from the sum, by adding her shares from the two terms:

$$91 + 91 = 182.$$

Bob and respectively Cesar do the same thing:

$$132 + 131 = 263,$$

$$173 + 171 = 344.$$

Now it is the moment of the **collaborative disclosure**.

At this point Alice, Bob and Cesar announce their shares and compute together the final result:

$$3 \cdot 182 - 3 \cdot 263 + 344 = 101,$$

which is of course $x_1x_2 + x_3 = 5 \cdot 10 + 51 = 101$, but the secret numbers were never disclosed. We can observe that if Cesar discloses his secret, then Alice and Bob will directly compute x_1x_2, and because every one knows his secret number, they will both know the secret of the other. So Cesar's contribution is essential in keeping the general secret in this protocol.

Exercise 42 *Show that for p prime number, the set $G_p = p\mathbb{Z}_p + 1$ builds a cyclic group with the multiplication modulo p^2. Show that this group is isomorphic with $(\mathbb{Z}_p, +, 0)$. Observing that* $10201 = 101^2$*, find the following: (a)* $5152^{-1} \bmod 10201$ *and (b)* $\log_{5152} 2021 \bmod 10201$.

Indeed, $(ap + 1)(bp + 1) = (a + b)p + 1 \bmod p^2$. So $f : (\mathbb{Z}_p, +_{\bmod p}, 0) \to (G_p, \times_{\bmod p^2}, 1)$, given by $f(a) = ap + 1$, is an isomorphism of groups. As $\mathbb{Z}_p$ is cyclic, G_p is cyclic as well. Moreover, every element different from 1 is a generator of G_p.

Now consider the isomorphism $f : \mathbb{Z}_{101} \to G_{101}$ given by $f(a) = 101a + 1$, where $p = 101$ is prime. We observe that $5152 = f(51)$ and the additive inverse of 51 is $-51 \bmod 101 = 50$. So $5152^{-1} \bmod 10201 = f(50) = 5051$, which is also easy to check by computation.

As $5152 = f(51)$ and $2021 = f(20)$, we see that $g = 51$ is a generator of $(\mathbb{Z}_{101}, +, 0)$. We shall find g^{-1} and multiply it with $x = 20$. So $51^{-1} \bmod 101 = 2$ and $2 \times 20 = 40$. It follows $40 \cdot 51 = 20 \bmod 101$. Write multiplication with 40 as repeated addition 40 times, and apply the isomorphism f. It follows that $5152^{40} \bmod 10201 = 2021$, so $\log_{5152} 2021 \bmod 10201 = 40$.

We observe as well that for $a, b \in G_p$ the following identity holds:

$$a^{b-1} = b^{a-1} \bmod p^2.$$

Exercise 43 *Alice earns* 10000 *euro while Bob earns* 8000 *euro. They both know that they earn between* 5000 *and* 15000 *and want to know who earns more without disclosing the real amount. Describe a protocol of undisclosed comparison.*

Bob observes that the values of RSA modulo 221 with public key 5 do not contain consecutive numbers when computed in the interval $\{55, 56, \dots, 65\}$. Indeed, those values are:

$$191, 218, 109, 28, 128, 8, 159, 95, 20, 64, 182$$

Here the value $28 = RSA_5(58)$ corresponds to his income of 8000 euro. He preserves the values 191, 218, 109, 28 corresponding to incomes less or equal to his own, and he increases with 1 the codes corresponding to bigger incomes. So he gets the list:

$$191, 218, 109, 28, 129, 9, 160, 96, 21, 65, 183$$

He permutes the list randomly and gets:

$$183, 191, 65, 218, 21, 109, 96, 28, 160, 129, 9$$

He tells to Alice: *Add 50 to your income expressed in thousands of euro and apply RSA modulo* 221 *with public key* 5. *If you find the result in this sequence, then I earn more. But if you find the result plus* 1, *then you earn more.* Alice computes $60^5 \bmod 221 = 8$ and announces the result. They both find 9 in the sequence, and they know that Alice earns more then Bob. In the best case, a program takes Bob's income as an input and presents this list, such that Bob also does not know what the number 9 signifies.

Exercise 44 *Alice and Bob are engaged in a No Key communication protocol. They are using* $p = 101$ *and the secret encryption keys* $k_A = 7$ *and* $k_B = 11$. *Alice sends the clear message* $m = 50$. *Expose the protocol numerically.*

First Alice sends to Bob $50^7 \bmod 101 = 86$. Then Bob sends Alice $86^{11} \bmod 101 = 48$. Now Alice computes her secret decryption key $7^{-1} \bmod 100 = 43$, and sends Bob $48^{43} \bmod 101 = 18$. Bob computes his own decryption key $11^{-1} \bmod 100 = 91$ and then he computes $18^{91} \bmod 101 = 50$. Now Bob has the clear message.

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:*

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

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:

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

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

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

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

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:

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

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:

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

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:*

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

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 powers of the cycle $(1\ 2\ \dots\ n)$.

Exercise 7 *Show the following identity:*

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

Just figure out how every object $1, 2, \dots, n$ 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 $(a_1, \dots, a_k)$ be a cycle. Show that:*

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

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

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

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

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 build 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 two elements. 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 and 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:

$$ABC \dots XYZZZ \dots Z$$

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

$$ZZZ \dots ZABC \dots XYZZZ \dots Z$$

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 pairwise 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 for the generator 2. 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, $\omega+1$, $\omega^2+\omega$, $\omega^2+\omega+1$, ω^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 [for example $X^5+X^2+1 = (X+1)(X^4+X^3+X^2)+1$], so it is irreducible. Further we observe that:

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

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

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 us consider an alphabet with* $|\mathcal{A}| = 26$ *letters 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 $(6x, 5x) \bmod 26$.

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 $m \to \infty$.

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

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-letter alphabet $\mathcal{A}$, starting with A, B, C, ..., Z and ending with Ă, Â, Î, 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 $Enc_k(k) = k \oplus k = 0^{25} = AAAAA$. 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-letter 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 descendent trees with roots in S_0.

Indeed, for every $x \in S$, the sequence x, $f(x)$, $f^2(x)$, $f^3(x)$, $\dots$, 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:

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

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

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

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 3, $(6, 11, 13)$. 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 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:

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

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 register 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.*

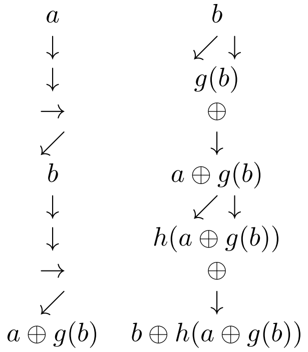
- Write down a formula expressing the function $F(a, b)$ with $a, b \in \{0,1\}^n$.

- 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:



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,

$$(w+1)(w^7 + w^6 + w^5 + w^4 + w^2 + w) =$$
$$= w^8 + w^7 + w^6 + w^5 + w^3 + w^2 + w^7 + w^6 + w^5 + w^4 + w^2 + w =$$
$$= w^8 + w^3 + w^4 + w = 1.$$

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 $(x, SubBytes(x))$ build 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:

$$y_i = (x_i + x_{(i+4) \bmod 8} + x_{(i+5) \bmod 8} + x_{(i+6) \bmod 8} + x_{(i+7) \bmod 8}) \mod 2,$$

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

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 $X^4 + 1$.*

Consider the polynomial multiplication:

$$b_0 + b_1 X + b_2 X^2 + b_3 X^3 = (a_0 + a_1 X + a_2 X^2 + a_3 X^3)(c_0 + c_1 X + c_2 X^2 + c_3 X^3) \mod (X^4 + 1).$$

The computation yields:

$$\begin{gathered} a_0c_0 + a_0c_1X + a_0c_2X^2 + a_0c_3X^3 + \\ +a_1c_0X + a_1c_1X^2 + a_1c_2X^3 + a_1c_3 + \\ +a_2c_0X^2 + a_2c_1X^3 + a_2c_2 + a_2c_3X + \\ +a_3c_0X^3 + a_3c_1 + a_3c_2X + a_3c_3X^2. \end{gathered}$$

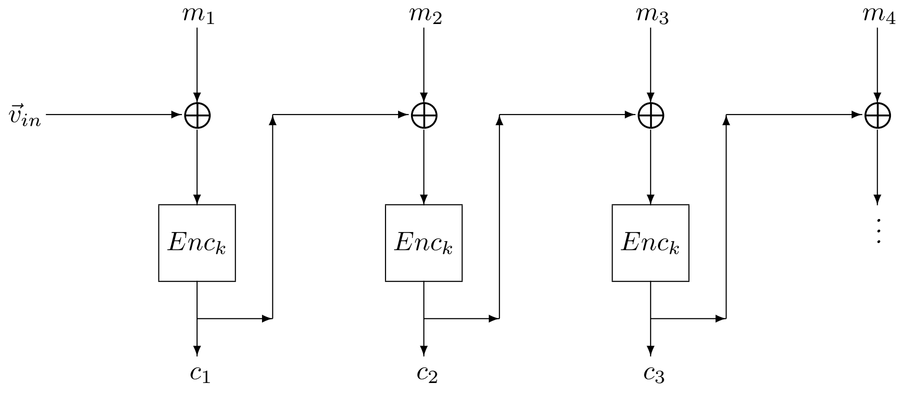
This expression is sorted as a polynomial.

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

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 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 $\{0, 1, \dots, 255\}$.

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 $\text{ord}(45) = 256$ 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 $\{1, \dots, 256\}$, and modulo 256, it becomes surjective on $\{0, 1, \dots, 255\}$.

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 $g \in \mathbb{F}_{2^m+1}^{\times}$ 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 $(x_1, \dots, x_{p+q})$ with*

$$f(x_1, \dots, x_p) = (x_{p+1}, \dots, x_{p+q}),$$

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 (as function in only one variable).

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 $a = a' = 0$. 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.