Some exercises for the written exam*

January 1, 2021

Exercises

1. *Additive Elgamal* modulo $n = 2021$ with generator $g = 2020$.
   (a) Alice chooses the secret key $x = 2019$ while Bob chooses the temporary key $y = 2018$. Compute the public key of Alice. Show how Bob encrypts the message $m = 2017$ and how Alice decrypts the encrypted message.
   (b) Agent Eva computes $g^{-1} \bmod n$ and finds out the secret key of Alice using the public key of Alice. Show how she does this.
2. *Multiplicative Elgamal* modulo $p = 43$ in the group generated by $g = 2$. Alice has the public key $h = 11$. Bob sends the encrypted message $(c_1, c_2) = (4, 5)$. Decrypt the message.
3. *Polard Rho Algorithm.* Factorize $N = 2021$ working with start value $x_0 = y_0 = 5$.
4. *RSA.* Someone encrypted a message m modulo 2021 using the public key $e = 5$ and got $c = 6$. Decrypt the message using the function $\varphi(N)$.
5. *RSA.* Decrypt the message from Exercise 4 using the function $\lambda(N)$.
6. *Goldwasser-Micali Algorithm.* Someone receives a message modulo 2021 consisting of the numbers 1478, 1968, 1601, 1684. Decrypt the message.
7. *Shamir Secret Sharing.* Let $P \in \mathbb{Z}_{43}[X]$ be a polynomial of degree 2. Consider pairs $(\alpha, P(\alpha))$ where $\alpha \in \mathbb{Z}_{43} \setminus \{0\}$ and $P(\alpha) \in \mathbb{Z}_{43}$. If 3 such pairs are $(5, 23)$, $(10, 29)$ and $(42, 10)$, deduce the shared secret $s = P(0) \in \mathbb{Z}_{43}$.
8. *Cipolla Algorithm.* Find out the square roots of 13 modulo 43, if they exist.
9. *No Key Protocol of Shamir.* Using $p = 43$, Alice sends to Bob the message $m = 2$. Alice has the secret key $a = 5$ and Bob has the secret key $b = 11$. Run the protocol.

*7 from 8 exercises will follow patterns given here.

1

Additive Elgamal modulo $n = 2021$ with generator $g = 2020$.

1. Alice chooses the secret key $x = 2019$ while Bob chooses the temporary key $y = 2018$. Compute the public key of Alice. Show how Bob encrypts the message $m = 2017$ and how Alice decrypts the encrypted message.
2. Agent Eva computes $g^{-1} \bmod n$ and finds out the secret key of Alice using the public key of Alice. Show how she does this.

Solution: We are working in the additive group $(\mathbb{Z}_{2021}, +, 0)$. The meaning of exponentiation in this group is the repeated addition, which is the multiplication. The meaning of the multiplication (the standard group operation) is addition, and its inverse operation is subtraction.

The public key of Alice is:

$$h = g^x = gx \bmod 2021 = 2020 \cdot 2019 \bmod 2021 = (-1) \cdot (-2) \bmod 2021 = 2 \bmod 2021.$$

Bob computes the following numbers:

$$c_1 = g^y = gy \bmod 2021 = 2020 \cdot 2018 \bmod 2021 = (-1) \cdot (-3) \bmod 2021 = 3 \bmod 2021.$$

$$c_2 = mh^y = m + hy \bmod 2021 = 2017 + 2 \cdot 2018 \bmod 2021 =$$
$$= (-4) + 2 \cdot (-3) \bmod 2021 = -10 \bmod 2021 = 2011.$$

So Bob sends $(c_1, c_2) = (3, 2011)$ to Alice. Now Alice uses her secret key x and computes:

$$m = c_2(c_1^x)^{-1} = c_2 - c_1 \cdot x \bmod 2021 = 2011 - 3 \cdot 2019 \bmod 2021 = 2011 - 3 \cdot (-2) \bmod 2021 = 2017.$$

Agent Eva computes:

$$g^{-1} \bmod n = 2020^{-1} \bmod 2021 = (-1)^{-1} \bmod 2021 = (-1) \bmod 2021 = 2020.$$

She can now compute:

$$x = g^{-1}h \bmod 2021 = 2020 \cdot 2 \bmod 2021 = (-1) \cdot 2 \bmod 2021 = -2 \bmod 2021 = 2019,$$

so she found the secret key of Alice. □

2

Multiplicative Elgamal modulo $p = 43$ in the group generated by $g = 2$. Alice has the public key $h = 11$. Bob sends the encrypted message $(c_1, c_2) = (4, 5)$. Decrypt the message.

Solution: We are working in the multiplicative group $(\mathbb{Z}_{43}^{\times}, \cdot, 1)$. Here the secret key of Alice is protected by the discrete logarithm. However, the powers of 2 are easy to compute by successive multiplication with 2, and 43 is not a very big number. Compute the powers of 2 modulo 43:

$$2, 4, 8, 16, 32 = -11, -22 = 21, 42 = -1, -2, -4, -8, -16, -32 = 11.$$

So $2^{12} \bmod 43 = 11$, hence the secret key of Alice is $x = 12$.

$$m = c_2(c_1^x)^{-1} \bmod 43 = 5 \cdot (4^{12})^{-1} \bmod 43.$$

The exponent $12 = 4 + 8$, so we compute these powers of 4 modulo 43 by succesive squaring:

$$4 \rightsquigarrow 4^2 = 16 \rightsquigarrow 4^4 = 16^2 = 41 = (-2) \rightsquigarrow 4^8 = (-2)^2 = 4 \bmod 43.$$

$$4^{12} \bmod 43 = 4^4 4^8 \bmod 43 = (-2) \cdot 4 \bmod 43 = 35.$$

Now we must compute the inverse $35^{-1} \bmod 43$ by the extended Euclid algorithm.

$$43 = \underline{35} + \underline{8}, \quad \underline{8} = (-1) \cdot \underline{35},$$

$$\underline{35} = 4 \cdot \underline{8} + \underline{3}, \quad \underline{3} = \underline{35} - 4 \cdot (-1) \cdot \underline{35} = 5 \cdot \underline{35},$$

$$\underline{8} = 2 \cdot \underline{3} + \underline{2}, \quad \underline{2} = \underline{8} - 2 \cdot \underline{3} = (-1) \cdot \underline{35} - 2 \cdot 5 \cdot \underline{35} = (-11) \cdot \underline{35},$$

$$\underline{3} = \underline{2} + 1, \quad 1 = \underline{3} - \underline{2} = 5 \cdot \underline{35} - (-11) \cdot \underline{35} = 16 \cdot \underline{35}.$$

So $35^{-1} \bmod 43 = 16$ and $m = 5 \cdot 16 \bmod 43 = 80 \bmod 43 = 37$. Indeed, as the temporary key was $y = 2$,

$$c_2 = 37 \cdot 11^2 \bmod 43 = 5.$$

□

3

Polard Rho Algorithm. Factorize $N = 2021$ working with start value $x_0 = y_0 = 5$.

Solution: Consider $f(x) = (x^2 + 1) \bmod 2021$ and the sequences $x_{n+1} = f(x_n)$, $y_{n+1} = f(f(y_n))$. At every step we compute $\gcd(2021, |x_n - y_n|)$ until we find a nontrivial divisor.

So $x_1 = 26$, $y_1 = 677$, $y_1 - x_1 = 651$,

$\gcd(2021, 651) = \gcd(68, 651) = \gcd(68, 39) = \gcd(38, 39) = 1.$

$x_2 = 677$, $y_2 = 996$, $y_2 - x_2 = 319$,

$\gcd(2021, 319) = \gcd(319, 107) = \gcd(107, 105) = 1.$

$x_3 = 1584$, $y_3 = 1555$, $x_3 - y_3 = 29$,

$\gcd(2021, 29) = \gcd(29, 20) = 1.$

$x_4 = 996$, $y_4 = 1512$, $y_4 - x_4 = 516$,

$\gcd(2021, 516) = \gcd(516, 473) = \gcd(473, 43) = \gcd(11 \cdot 43, 43) = 43.$

So $2021 = 43 \cdot 47$ and both are prime numbers. □

4

RSA. Someone encrypted a message m modulo 2021 using the public key $e = 5$ and got $c = 6$. Decrypt the message using the function $\varphi(N)$.

Solution: If $N = 2021 = 43 \cdot 47$, $\varphi(N) = 42 \cdot 46 = 1932$. The secret key $d = e^{-1} \bmod \varphi(N) = 5^{-1} \bmod 1932$. We apply the extended Euclid algorithm.

$$1932 = 386 \cdot \underline{5} + \underline{2}, \quad \underline{2} = (-386) \cdot \underline{5},$$

$$\underline{5} = 2 \cdot \underline{2} + 1, \quad 1 = \underline{5} - 2 \cdot \underline{2} = \underline{5} - 2 \cdot (-386)\underline{5} = 773 \cdot \underline{5}.$$

So $d = 5^{-1} \bmod 1932 = 773$, and

$$m = 6^{773} \bmod 2021.$$

We observe that $773 = 512 + 256 + 4 + 1 = 2^9 + 2^8 + 2^2 + 1$. We compute the corresponding powers by successive squaring modulo 2021:

$$6 \rightsquigarrow 6^2 = 36 \rightsquigarrow 6^4 = 1296 \rightsquigarrow 6^8 = 165 \rightsquigarrow 6^{16} = 952 \rightsquigarrow 6^{32} = 896 \rightsquigarrow 6^{64} = 479 \rightsquigarrow$$

$$\rightsquigarrow 6^{128} = 1068 \rightsquigarrow 6^{256} = 780 \rightsquigarrow 6^{512} = 79.$$

So $m = 6^{773} \bmod 2021 = 79 \cdot 780 \cdot 1296 \cdot 6 \bmod 2021 = 251.$ □

5

RSA. Decrypt the message from Exercise 4 using the function $\lambda(N)$.

Solution: We compute $\lambda(2021) = \text{lcm}\ (42, 46) = 42 \cdot 46/2 = 966$. Now we compute 5^{-1} mod 966 by extended Euclid.

$$966 = 193 \cdot \underline{5} + 1, \quad 1 = (-193) \cdot \underline{5} = (966 - 193) \cdot \underline{5} = 773.$$

So 5^{-1} mod $966 = 773$ and as before:

$$m = 6^{773} \bmod 2021 = 251,$$

because the computation was already done.

In many situations one get another number for e^{-1} mod $\lambda(N)$ and the computation of m must be done again. □

6

Goldwasser-Micali Algorithm. Someone receives a message modulo 2021 consisting of the numbers 1478, 1968, 1601, 1684. Decrypt the message.

Solution: We observe that $2021 = 43 \times 47$ is a good module for Goldwasser - Micali, because $43 = 3 \bmod 4$ and $47 = 3 \bmod 4$. So we must reduce the numbers modulo 43 and then we must decide if they are quadratic residues or not. Quadratic residues correspond with 0, non-residues correspond with 1.

1478 mod 43 = 16 mod 43 = 4^2 mod 43 so $m_1 = 0$.

1968 mod 43 = 33 mod 43. One has:

$$\Big(\frac{33}{43}\Big) = \Big(\frac{3}{43}\Big)\Big(\frac{11}{43}\Big) = (-1)\Big(\frac{43}{3}\Big)(-1)\Big(\frac{43}{11}\Big) = \Big(\frac{1}{3}\Big)\Big(\frac{-1}{11}\Big) = 1 \cdot (-1) = -1,$$

so $m_2 = 1$.

1601 mod 43 = 10. One has:

$$\Big(\frac{10}{43}\Big) = \Big(\frac{2}{43}\Big)\Big(\frac{5}{43}\Big) = (-1)^{\frac{43^2-1}{8}}\Big(\frac{43}{5}\Big) = (-1)^{\frac{42\cdot 44}{8}}\Big(\frac{3}{5}\Big) =$$

$$= (-1)^{21\cdot 11}\Big(\frac{5}{3}\Big) = (-1)\Big(\frac{2}{3}\Big) = (-1)(-1) = 1,$$

so $m_3 = 0$.

1684 mod 43 = 7. One has:

$$\Big(\frac{7}{43}\Big) = (-1) \cdot \Big(\frac{43}{7}\Big) = (-1) \cdot \Big(\frac{1}{7}\Big) = -1,$$

so $m_4 = 1$.

Finally,

$$m = m_1||m_2||m_3||m_4 = 0101.$$

□

7

Shamir Secret Sharing. Let $P \in \mathbb{Z}_{43}[X]$ be a polynomial of degree 2. Consider pairs $(\alpha, P(\alpha))$ where $\alpha \in \mathbb{Z}_{43} \setminus \{0\}$ and $P(\alpha) \in \mathbb{Z}_{43}$. If 3 such pairs are $(5, 23)$, $(10, 29)$ and $(42, 10)$, deduce the shared secret $s = P(0) \in \mathbb{Z}_{43}$.

Solution: Let $P(x) = s + ax + bx^2$. Our mission is find the coefficients. We observe that $42 = -1 \bmod 43$, so it makes sense to put the corresponding equation at the beginning. We get the following system of linear equations over the field $\mathbb{Z}_{43}$:

$$\begin{aligned} s - a + b &= 10 \\ s + 5a + 25b &= 23 \\ s + 10a + 14b &= 29 \end{aligned}$$

where we already observed that $100 \bmod 43 = 14$. Now we subtract the first equation from the other equations, to get:

$$\begin{aligned} s - a + b &= 10 \\ 6a + 24b &= 13 \\ 11a + 13b &= 19 \end{aligned}$$

We would like to get rid of the coefficient 11 of a in the last equation. We observe that $11^{-1} \bmod 43 = 4$ so we multiply the last equation with 4 modulo 43, to get: $a + 52b = 76$, $a + 9b = 33$. We write this equation as second equation:

$$\begin{aligned} s - a + b &= 10 \\ a + 9b &= 33 \\ 6a + 24b &= 13 \end{aligned}$$

Now we can multiply the second equation with 6 and subtract it from the last equation. The last equation becomes:

$$-30b = 30,$$

so $b = -1$. From the second equation $a - 9 = 33$ so $a = 33 + 9 = 42 = -1$ modulo 43. From first equation $s = 10$. This is the shared secret. □

8

Cipolla Algorithm. Find out the square roots of 13 modulo 43, if they exist.

Solution: We first decide if 13 is a quadratic rest modulo 43. We compute again the Legendre Symbol:

$$\left(\frac{13}{43}\right) = \left(\frac{43}{13}\right) = \left(\frac{4}{13}\right) = 1,$$

so the answer is yes. Now we must find an $a \in \mathbb{F}_{43}^{\times}$ such that $a^2 - 13$ is not a square.

Try $a = 1$, $a^2 - 13 = -12 = 31$.

$$\left(\frac{31}{43}\right) = (-1) \cdot \left(\frac{43}{13}\right) = (-1)\left(\frac{4}{13}\right) = -1.$$

Bad luck. Try $a = 2$, $a^2 - 13 = -9$ which is not a square, because 9 is a square but -1 is not a square modulo $p = 4k + 3$. So we work with $a = 2$ and $a^2 - 13 = -9 = 34$. Let the symbol $w = \sqrt{34} \notin \mathbb{F}_{43}$. We are working now in the quadratic extension $\mathbb{F}_{43}[w]$ with $w^2 = 34$ and we know that:

$$\sqrt{13} = (w + a)^{\frac{p+1}{2}} = (2 + w)^{22}.$$

Observe that $22 = 16 + 4 + 2$. We compute these powers of $2 + w$ working in the field $\mathbb{F}_{43}[w]$.

$$(2+w)^2 = 4 + 4w + 34 = 4w - 5,$$

$$(2+w)^4 = 16 \cdot 34 - 40w + 25 = -40w + 10,$$

$$(2+w)^8 = 100 \cdot (-4w+1)^2 = 14 \cdot (16 \cdot 34 - 8w + 1) = 14 \cdot (29 - 8w),$$

$$(2+w)^{16} = 14^2(24 + 9w + 64 \cdot 34) = 24 \cdot (7 + 9w).$$

Finally,

$$\sqrt{13} = 24 \cdot (7+9w) \cdot 10 \cdot (1-4w) \cdot (4w-5) = 240 \cdot (7 - 28w + 9w - 36 \cdot 34)(4w-5) =$$

$$= 240(30 + 24w)(4w-5) = 480(15 + 12w)(4w-5) =$$

$$= 480(60w - 5 \cdot 15 + 48 \cdot 34 - 60w) = 20.$$

So the solutions are $+20 = 20$ and $-20 = 23$ modulo 43. □

9

No Key Protocol of Shamir. Using $p = 43$, Alice sends to Bob the message $m = 3$. Alice has the secret key $a = 5$ and Bob has the secret key $b = 11$. Run the protocol.

Solution: Alice sends to Bob:

$$A = m^a \bmod p = 3^5 \bmod 43 = 9 \cdot 9 \cdot 3 \bmod 43 = -15 = 28.$$

Bob sends to Alice:

$$B = A^b \bmod p = 28^{11} \bmod 43 = 12.$$

We must find out the inverse key of Alice. In order to compute $5^{-1} \bmod 42$,

$$42 = 8 \cdot \underline{5} + \underline{2}, \quad \underline{2} = (-8) \cdot \underline{5},$$

$$\underline{5} = 2 \cdot \underline{2} + 1, \quad 1 = \underline{5} - 2 \cdot (-8)\underline{5} = 17 \cdot \underline{5}.$$

So Alice sends to Bob:

$$C = B^{(a^{-1} \bmod p-1)} = 12^{17} \bmod 43 = 30.$$

In order to decrypt the message, Bob has to compute his inverse key $11^{-1} \bmod 42$:

$$42 = 3 \cdot \underline{11} + \underline{9}, \quad \underline{9} = (-3) \cdot \underline{11},$$

$$\underline{11} = \underline{9} + \underline{2}, \quad \underline{2} = 4 \cdot \underline{11},$$

$$\underline{9} = 4 \cdot \underline{2} + 1, \quad 1 = (-3) \cdot \underline{11} - 4 \cdot 4 \cdot \underline{11} = (-19) \cdot \underline{11} = 23 \cdot \underline{11}.$$

So $11^{-1} \bmod 42 = 23$ and Bob computes:

$$m = C^{(b^{-1} \bmod p-1)} = 30^{23} \bmod 43 = 3.$$