Exercises*

December 30, 2023

Exercises

1. *RSA.* A message is encrypted using RSA modulo 35 with public key $e = 5$. The encrypted message is $c = 33$. Find the original message.

2. *Additive Elgamal* modulo $n = 1000$ with generator $g = 667$. The public key is $h = 21$ and the encrypted message is $(c_1, c_2) = (81, 27)$. Find the clear message m.

3. *Multiplicative Elgamal* modulo $p = 29$ in the group generated by $g = 2$. The public key is $h = 24$, the encrypted message is $(c_1, c_2) = (7, 21)$. Find the clear message m.

4. *Shamir Secret Sharing.* Let $P \in \mathbb{Z}_{29}[X]$ be a polynomial of degree 2. Consider pairs $(\alpha, P(\alpha))$ where $\alpha \in \mathbb{Z}_{29} \setminus \{0\}$ and $P(\alpha) \in \mathbb{Z}_{29}$. If 3 such pairs are $(1, 15)$, $(2, 6)$ and $(3, 7)$, deduce the shared secret $s = P(0) \in \mathbb{Z}_{29}$.

5. *Cipolla.*

   (a) Show that 3 is a square modulo 23. Also, show that for $a = 1$, $a^2 - 3 = 21$ is not a square modulo 23.

   (b) Using this fact, find the square roots of 7 modulo 23 working in the ring $\mathbb{Z}_{23}[\sqrt{21}]$.

*5 from 6 exam exercises will follow this pattern.

1

RSA A message is encrypted using RSA modulo 35 with public key $e = 5$. The encrypted message is $c = 33$. Find the original message.

Solution: The number 35 has an evident factorisation. So $\lambda(35) = \mathrm{lcm}(5-1, 7-1) = 12$. As $5 \cdot 5 = 25 = 24 + 1$, the private key is $d = e^{-1} \bmod \lambda(N) = 5^{-1} \bmod 12 = 5$. The clear message is:

$$m = 33^5 \bmod 35 = (-2)^5 \bmod 35 = -32 \bmod 35 = 3,$$

so $m = 3$ is the clear message. □

2

Additive Elgamal modulo $n = 1000$ with generator $g = 667$. The public key is $h = 21$ and the encrypted message is $(c_1, c_2) = (81, 27)$. Find the clear message m.

Solution: The encryption works over the group $(\mathbb{Z}_{1000}, +, 0)$. So the group operation is $+$, the meaning of a^b is ab and the meaning of a^{-1} is $-a$. In such groups, one can easily find out the secret key or the temporary key by computing $g^{-1} \bmod N$. Observe that g is a generator of $\mathbb{Z}_N$ is $\gcd(g, N) = 1$, which is equivalent with the existence of $g^{-1} \bmod N$.

$$\begin{aligned} 1000 &= \underline{667} + \underline{333} \\ \underline{667} &= 2 \cdot \underline{333} + 1 \end{aligned}$$

$$1 = \underline{667} - 2 \cdot \underline{333} = \underline{667} - 2(-\underline{667}) = 3 \cdot 667,$$

so $667^{-1} \bmod 1000 = 3$.

First method: One finds out the secret key x:

$$x = g^{-1}h = (3 \cdot 21) \bmod 1000 = 63,$$

and then one finds m:

$$m = c_2 - xc_1 = (27 - 63 \cdot 81) \bmod 1000 = 924.$$

Second method: One finds the temporary key y:

$$y = g^{-1}c_1 = (3 \cdot 81) \bmod 1000 = 243,$$

and then one finds m:

$$m = c_2 - yh = (27 - 243 \cdot 21) \bmod 1000 = 924.$$

It does not matter, which method you choose. It is sufficient to solve it by one method. □

3

Multiplicative Elgamal modulo $p = 29$ in the group generated by $g = 2$. The public key is $h = 24$, the encrypted message is $(c_1, c_2) = (7, 21)$. Find the clear message m.

Solution: We are working in the multiplicative group $(\mathbb{Z}_{29}^{\times}, \cdot, 1)$. 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 29 is not a very big number. We compute the powers of 2 modulo 29.

First method: One finds out the secret key x:

$$2^n \bmod 29 = 2, 4, 8, 16, 3, 6, 12, 24 = h.$$

So $x = 8$.

$$m = c_2 c_1^{(-x)} = 21 \cdot (7^8)^{-1}.$$

By successive squaring we find:

$$7 \rightsquigarrow 7^2 = 20 = -9 \rightsquigarrow 7^4 = 81 = -6 \rightsquigarrow 7^8 = 36 = 7,$$

where all computations are modulo 29. It follows:

$$m = 21 \cdot 7^{-1} = 3 \cdot 7 \cdot 7^{-1} = 3.$$

Second method: One finds out the temporary key y:

$$2^n \bmod 29 = 2, 4, 8, 16, 3, 6, 12, 24, 19, 9, 18, 7 = c_1.$$

So $y = 12$.

$$m = c_2 h^{-y} = 21 \cdot (24^{12})^{-1}.$$

By successive squaring we find:

$$24 = -5 \rightsquigarrow 24^2 = 25 = -4 \rightsquigarrow 24^4 = 16 = -13 \rightsquigarrow 24^8 = 13^2 = 24,$$

where all computations are modulo 29. It follows that:

$$24^{12} = 24^8 \cdot 24^4 = 24 \cdot 16 = 48 \cdot 8 = -10 \cdot 8 = 7.$$

$$m = 21 \cdot 7^{-1} = 3 \cdot 7 \cdot 7^{-1} = 3.$$

It does not matter, which method you choose. It is sufficient to solve it by one method. □

4

Shamir Secret Sharing. Let $P \in \mathbb{Z}_{29}[X]$ be a polynomial of degree 2. Consider pairs $(\alpha, P(\alpha))$ where $\alpha \in \mathbb{Z}_{29} \setminus \{0\}$ and $P(\alpha) \in \mathbb{Z}_{29}$. If 3 such pairs are $(1, 15)$, $(2, 6)$ and $(3, 7)$, deduce the shared secret $s = P(0) \in \mathbb{Z}_{29}$.

Solution: Let $P(x) = s + ax + bx^2$. We have to find the coefficients. We get the following system of linear equations over the field $\mathbb{Z}_{29}$:

$$\begin{aligned} s + a + b &= 15 \\ s + 2a + 4b &= 6 \\ s + 3a + 9b &= 7 \end{aligned}$$

We subtract the first equation from the other equations, to get:

$$\begin{aligned} s + a + b &= 15 \\ a + 3b &= 20 \\ 2a + 8b &= 21 = -8 \end{aligned}$$

The last equation can be simplified with 2 and becomes:

$$a + 4b = -4.$$

The last two equations build together the system:

$$\begin{aligned} a + 4b &= -4 \\ a + 3b &= 20 \end{aligned}$$

By subtraction we get $b = -24 = 5$. We substitute b in the second equation to get $a + 15 = 20$, so $a = 5$. We substitute a and b in the first equation to get $s + 5 + 5 = 15$, so $s = 5$. This is the shared secret. □

5

Cipolla.

1. Show that 3 is a square modulo 23. Also, show that for $a = 1$, $a^2 - 3 = 21$ is not a square modulo 23.
2. Using this fact, find the square roots of 7 modulo 23 working in the ring $\mathbb{Z}_{23}[\sqrt{21}]$.

(1) We use Legendre symbols. We observe that:

$$(\frac{3}{23}) = (-1)(\frac{23}{3}) = (-1)(\frac{2}{3}).$$

We observe that x^2 mod 3 might be only 0 and 1, so:

$$(\frac{2}{3}) = -1,$$

$$(\frac{3}{23}) = (-1)(-1) = 1.$$

For $a = 1$, $a^2 - 3 = -2 = 21$ mod 23.

$$(\frac{21}{23}) = (\frac{3}{23})(\frac{7}{23}) = (-1)(\frac{23}{3})(-1)(\frac{23}{7}) = (\frac{2}{3})(\frac{2}{7}).$$

We recall that:

$$(\frac{2}{3}) = -1.$$

Also, we observe that $x^2 \bmod 7 = \{0, 1, 4, 2\}$, so:

$$(\frac{2}{7}) = 1.$$

It follows that:

$$(\frac{21}{23}) = -1.$$

(2) According to Cipolla's Alorithm,

$$\sqrt{3} \bmod 23 = \big(a + \sqrt{a^2 - 3}\big)^{\frac{p+1}{2}} = \big(1 + \sqrt{21}\big)^{12}.$$

We compute this power by the Fast Exponentiation Algorithm. We observe that $12 = 8 + 4$.

$$\big(1 + \sqrt{21}\big)^2 = 1 + 2\sqrt{21} + 21 = 22 + 2\sqrt{21} = -1 + 2\sqrt{21} \mod 23,$$

$$\big(1 + \sqrt{21}\big)^4 = \big(-1 + 2\sqrt{21}\big)^2 = 1 - 4\sqrt{21} + 4 \cdot 21 = 1 - 4\sqrt{21} + 4 \cdot (-2) = -7 - 4\sqrt{21} \mod 23,$$

$$\big(1 + \sqrt{21}\big)^8 = \big(-7 - 4\sqrt{21}\big)^2 = 49 + 56\sqrt{21} + 16 \cdot (-2) = 3 + 10\sqrt{21} - 32 = -6 + 10\sqrt{21} \mod 23.$$

All together,

$$\big(1 + \sqrt{21}\big)^{12} = \big(-7 - 4\sqrt{21}\big)\big(-6 + 10\sqrt{21}\big) = 2\big(-7 - 4\sqrt{21}\big)\big(-3 + 5\sqrt{21}\big) =$$

$$= 2\big(21 - 35\sqrt{21} + 12\sqrt{21} - 20 \cdot 21\big) = 2\big(-19 \cdot 21 - 23\sqrt{21}\big) =$$

$$= 2\big(-19 \cdot (-2)\big) = 4 \cdot (-4) = -16 = 7 \mod 23.$$

Indeed, 7^2 mod $23 = 3$ and 16^2 mod $23 = 3$.