Exercises*

November 15, 2022

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. *Secret Multiparty Computation.* Alice, Bob and Cathy have secret values $x = 2$, $y = 3$ and $z = 4$ respectively. They want to compute together the value $xz + yz$ in a way they trust, but without displaying the clear values of x, y and z. For sharing initial values, they use polynomials of the shape $X + a$, $2X + b$ and $3X + c$ respectively. For multiplication shares, they use polynomials of the shape $3X + a$, $2X + b$ and $X + c$ respectively. Run the whole protocol.

*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:

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

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:

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

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

Secret Multiparty Computation. Alice, Bob and Cathy have secret values $x = 2$, $y = 3$ and $z = 4$ respectively. They want to compute together the value $xz + yz$ in a way they trust, but without displaying the clear values of x, y and z. For sharing initial values, they use polynomials of the shape $X + a$, $2X + b$ and $3X + c$ respectively. For multiplication shares, they use polynomials of the shape $3X + a$, $2X + b$ and $X + c$ respectively. Run the whole protocol.

Solution: As $xz + yz = (x + y)z$, the partners decide to make just two operations, first the addition, and then the multiplication.

Distribution of initial values:

Alice computes the values of $X + 2$, Bob the values of $2X + 3$ and Cathy the values of $3X + 4$. They share the following values:

$$\begin{pmatrix} & A & B & C \\ X+2 & 3 & 4 & 5 \\ 2X+3 & 5 & 7 & 9 \\ 3X+4 & 7 & 10 & 13 \end{pmatrix}$$

The columns indicate the initial values possessed by every participant.

Local additions: Every participant computes $x + y$ locally, and gets:

Alice $3 + 5 = 8$.

Bob $4 + 7 = 11$.

Cathy $5 + 9 = 14$.

Local multiplications: Every participant computes $(x + y)z$ locally, and gets:

Alice $8 \cdot 7 = 56$.

Bob $11 \cdot 10 = 110$.

Cathy $14 \cdot 13 = 182$.

Collaborative multiplication: The partners share their local multiplication results. Alice uses the polynomial $3X + 56$, Bob uses the polynomial $2X + 110$ and Cathy uses the polynomial $X + 182$:

$$\begin{pmatrix} & A & B & C \\ 3X+56 & 59 & 62 & 65 \\ 2X+110 & 112 & 114 & 116 \\ X+182 & 183 & 184 & 185 \end{pmatrix}$$

The columns indicate the values got by every participant.

Local recombinations: Every participant recombine its own multiplication share from the values got in the last round.

Alice $3 \cdot 59 - 3 \cdot 112 + 183 = 24$.

Bob $3 \cdot 62 - 3 \cdot 114 + 184 = 28$.

Cathy $3 \cdot 65 - 3 \cdot 116 + 185 = 32$.

Final recombination: The partners disclose their local shares and recombine the final result:

$$3 \cdot 24 - 3 \cdot 28 + 32 = 20.$$

This corresponds indeed to the value $2 \cdot 4 + 3 \cdot 4$ which was to compute. The protocol ran successfully.

□