Advanced Cryptography

24.11.2021

Exam

TARNU ILIE-CRISTIAN
410

1. Additive Elgamal

$m = 64, \quad g = 61$

a) $x = 10, \quad y = 11, \quad m = 12$

$h = g^x \bmod m = gx \bmod m = 610 \bmod 64 = 34$ - public key

For encryption compute (c_1, c_2)

$c_1 = g^y = gy = 671 \bmod 64 = 31$

$c_2 = m h^y = hy + m = 34 \cdot 11 + 12 = 386 \bmod 64 = 2$

For decryption use the secret key x and compute

$m = (c_1^x)^{-1} \cdot c_2 = -x \cdot c_1 + c_2$

$= -10 \cdot 31 + 12 = -308 \bmod 64 = 12 = m$

b) Since we're using additive Elgamal Eve can compute $g^{-1} \bmod n$ and find x, since $h = g^x = gx$, which is public

$\rightarrow x = g^{-1} \cdot h$

$g^{-1} \bmod n = 61^{-1} \bmod 64$

61^{-1} mod 64 using extended Euklid's Algorithm

$64 = 1 \cdot 61 + 3$ $\quad (\Leftrightarrow)$ $\quad 3 = 64 - 1 \cdot 61$

$61 = 20 \cdot 3 + 1$ $\quad\quad\quad\quad\quad\quad 1 = 61 - 20 \cdot 3$

$1 = 61 - 20 \cdot 3 \Leftrightarrow 1 = 61 - 20(64 - 61)$

$\Leftrightarrow 1 = -20 \cdot 64 + 21 \cdot 61$

$\Rightarrow 61^{-1} \bmod 64 = 21$

$x = g^{-1} \cdot h = 21 \cdot 34 = 714 \bmod 64 = \underline{10 = x}$

---

2. Multiplicative Elgamal

$p = 23$, $g = 2$

public key $h = 18$

encrypted message $(c_1, c_2) = (9, 10)$

To decrypt the message we need to find x s.t $g^x = h$. We do this by computing successive Powers of g

$2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 32 = 9$

$\underline{2^6 = 18} \rightarrow x = 6$

$m = (c_1^x)^{-1} \cdot c_2$

Compute $c_1^x = g^6 \bmod 23$

$6 = 4 + 2$

$g^2 = 81 = 12 \bmod 23$

$g^4 = 12^2 = 144 = 6 \bmod 23$

$\Rightarrow g^6 \bmod 23 = 12 \cdot 6 \bmod 23 = 3$

Now we need to compute

$3^{-1} \bmod 23$

$23 = 7 \cdot 3 + 2$ $\quad \Leftrightarrow \quad 2 = 23 - 7 \cdot 3$

$3 = 1 \cdot 2 + 1$ $\quad\quad\quad\quad 1 = 3 - 1 \cdot 2$

$1 = 3 - 1 \cdot 2 \Leftrightarrow 1 = 3 - 1(23 - 7 \cdot 3)$

$\Rightarrow 1 = -1 \cdot 23 + 8 \cdot 3$

$\Rightarrow 3^{-1} \bmod 23 = 8$

$m = (c_1^x)^{-1} \cdot c_2 = 8 \cdot 10 \bmod 23 = \underline{11}$

- RSA

$N = 85$; $e = 11$; $c = 12$

Decrypt with $\lambda(N)$

$N = 85 = 5 \cdot 17 \Rightarrow \lambda(N) = \text{lcm}(4, 16) = 16$

To decrypt c we need $d = e^{-1} \bmod \lambda(N)$

$d = 11^{-1} \bmod 16$

~~$16 = 1 \cdot 11 + 5$~~

~~$11 = 2 \cdot 5 + 1$~~

Observe that $3 \cdot 11 = 33 = 2 \cdot 16 + 1$

so $3 \cdot 11 \bmod 16 = 1$

$\Rightarrow 11^{-1} \bmod 16 = 3 = d$

$m = c^d \bmod N = 12^3 \bmod 85 = 12^2 \cdot 12$

$= 144 \cdot 12 \bmod 85 = 59 \cdot 12 \bmod 85 =$

$= 708 \bmod 85 = 28$

$\Rightarrow m = 28$

4. Goldwasser-Micali

$m = 3521 \qquad (2899, 622, 1971, 1550)$

$m = 3521 = 7 \cdot 503$

$7 \bmod 4 = 3$

$503 = 4 \cdot 125 + 3 \Rightarrow 503 \bmod 4 = 3$

$\left(\frac{2899}{7}\right) =$

$2899 = 2800 + 98 + 1 \bmod 7 = 1$

$\Rightarrow \left(\frac{2899}{7}\right) = \left(\frac{1}{7}\right) = +1 \Rightarrow m_1 = 0$

$\left(\frac{622}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{311}{7}\right) = (-1)^{\frac{48}{8}} \cdot \left(\frac{3}{7}\right)$

$= (-1)^6 \cdot -\left(\frac{7}{3}\right) = 1 \cdot -\left(\frac{1}{3}\right) = 1 \cdot -(+1)$

$= -1 \Rightarrow m_2 = 1$

$\left(\frac{1971}{7}\right) = \left(\frac{4}{7}\right) = 1 \Rightarrow m_3 = 0$

$\left(\frac{1550}{7}\right) = \left(\frac{3}{7}\right) = -\left(\frac{1}{3}\right) = -1 \Rightarrow m_4 = 1$

$\Rightarrow m = m_1 \| m_2 \| m_3 \| m_4 = 0101$

5. Shamir's No Key Protocol

$m = 10$, $p = 17$, $a = 7$, $b = 9$

Alice → Bob

$A = m^a \bmod p = 10^7 \bmod 17$

$7 = 4 + 2 + 1$

$10 = 10 \bmod 17$

$10^2 = 100 = 15 \bmod 17 = -2$

$10^4 = (-2)^2 = 4 \bmod 17$

$\Rightarrow 10^7 \bmod 17 = 10 \cdot (-2) \cdot 4 \bmod 17 = \underline{5}$

Bob → Alice

$B = A^b \bmod 17 = 5^9 \bmod 17$

$9 = 8 + 1$

$5^2 = 25 = 8 \bmod 17$

$5^4 = 8^2 = 64 \bmod 17 = 13$

$5^8 = (+4)^2 = 16 \bmod 17 = -1$

$\Rightarrow 5^9 \bmod 17 = 5 \cdot (-1) \bmod 17 = \underline{12}$

Alice computes $a^{-1} \bmod p-1$

$7^{-1} \bmod 16$

$16 \cdot 3 = 48$ and $7^2 = 49 = 48 + 1$

$\Rightarrow 7^{-1} \bmod 16 = 7$

Alice → Bob

$C = B^{a^{-1} \bmod p-1} = 12^7 \bmod 17$

$12^7 \bmod 17$

$7 = 4 + 2 + 1$

$12^2 = 144 \bmod 17 = 8 \bmod 17$

$12^4 = 8^2 = 64 \bmod 17 = 13 \bmod 17 = -4$

$\Rightarrow 12^7 \bmod 17 = 12 \cdot 8 \cdot (-4) \bmod 17 = \underline{7}$

$C = 7.$

Bob computes his inverse key

$b^{-1} \bmod p-1 = 9^{-1} \bmod 16$

$16 = 1 \cdot 9 + 7$ $\qquad$ $7 = 16 - 1 \cdot 9$

$9 = 1 \cdot 7 + 2$ $\qquad$ $2 = 9 - 1 \cdot 7$

$7 = 3 \cdot 2 + 1$ $\qquad$ $1 = 7 - 3 \cdot 2$

$1 = 7 - 3 \cdot 2 \Rightarrow 1 = 7 - 3(9 - 1 \cdot 7)$

$\Rightarrow 1 = -3 \cdot 9 + 4 \cdot 7 \Rightarrow 1 = -3 \cdot 9 + 4(16 - 1 \cdot 9)$

$\Rightarrow 1 = 4 \cdot 16 - 7 \cdot 9$

$\Rightarrow 9^{-1} \bmod 16 = -7 = 9 \bmod 16.$

Compute $C^{b^{-1} \bmod p-1} = 7^9 \bmod 17$

$9 = 8 + 1$

$7^2 = 49 = 15 \bmod 17 = -2$

~~$7^4 = 1 \bmod 16$~~

$7^8 = 1 \bmod 16 \Rightarrow$

$7^4 = (-2)^4 = 4 \bmod 17$

$7^8 = 16 \bmod 17 = (-1)$

$\Rightarrow 7^9 \bmod 17 = -1 \cdot 7 \bmod 17$

$= \underline{10 = M}$

6. Shamir's Secret Sharing

$P \in \mathbb{Z}_{23}[X]$ of degree 2

$(x, P(x)) \rightarrow (1, 20)\ ;\ (2, 16)\ ;\ (3, 10)$

deduce $S = P(0) \in \mathbb{Z}_{23}$

$P = ax^2 + bx + S$

$$\Rightarrow \begin{cases} 20 = a + b + S \\ 16 = 4a + 2b + S \\ 10 = 9a + 3b + S \end{cases}$$

subtract the first eq. from the rest

$$\Rightarrow \begin{cases} 3a + b = -4 \\ 8a + 2b = -10 \end{cases}$$

multiply the first eq by 2 and subtract it from the second

$$\Rightarrow \begin{cases} 6a + 2b = -8 \\ 8a + 2b = -10 \end{cases}$$

$\Rightarrow 2a = -2 \rightarrow a = -2 \cdot 2^{-1}$

Notice that $12 \cdot 2 = 24 = 1 \bmod 23$

$\Rightarrow 2^{-1} \bmod 23 = 12$

$\Rightarrow a = -2 \cdot 12 = -24 \bmod 23 = -1 = 22$

$3a + b = -4 \Rightarrow 3 \cdot (-1) + b = -4$

$\Rightarrow b = -1$

$a + b + S = 20 \Rightarrow -1 - 1 + S = 20$

$\Rightarrow S = 22 = -1$

7. Cipolla

a) 2 is a quadratic residue mod 23

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

→ 2 is a square mod 23

b) $\sqrt{2}$ mod 23

choose $a = 0$

$$a^2 - 2 = -2 = 21$$

$$\left(\frac{21}{23}\right) = \left(\frac{7}{23}\right)\left(\frac{3}{23}\right) = -\left(\frac{23}{7}\right)\left(-\left(\frac{23}{3}\right)\right)$$

$$= \left(\frac{2}{7}\right)\left(\frac{2}{3}\right) = (-1)^{\frac{48}{8}} \cdot (-1) = -1$$

→ $a^2 - 2 \notin sq(\mathbb{F}_{23})$

So $a = 0$ is a good choice

$$w^2 = a^2 - 2 = -2$$

$$\sqrt{2} = x = (w+a)^{\frac{23+1}{2}} = w^{12} = (w^2)^6 = (-2)^6$$

$$= 64 \bmod 23 = \underline{18}$$

Another solution is $-18 = \underline{5} \bmod 23$

. RSA

$p \neq q$ primes ; $N = pq$; $\varphi = (p-1)(q-1)$

$\lambda = lcm(p-1, q-1)$

e - lead beg if $\forall m \in \mathbb{Z}_N \quad m^e = m \bmod N$

Δ - set of lead begs in the interval $[1, \varphi]$

a) $\cdot$ - multiplication mod φ. $(\Delta, \cdot)$ - group.

Let $a, b \in \Delta$ then $m^a = m \bmod N$

$m^b = m \bmod N$

$m^a = m \bmod N \mid ()^b \Rightarrow m^{ab} = m^b \bmod N$ (take modulus of exponent)

$\Rightarrow m^{ab \bmod \varphi} = m^{b \bmod \varphi} = m \bmod N$

$\Rightarrow \forall a, b \in \Delta \Rightarrow ab \bmod \varphi \in \Delta$

$1 \in \Delta$ and it's obvious that $\forall x \in \Delta \quad x \cdot 1 = 1 \cdot x = x$

and $m^1 = m \bmod N$ so 1 is neutral element

Associativity is also obvious $\forall a, b, c \in \Delta$

$(ab)c = a(bc) \bmod \varphi$ which is true

$\forall x \in x^{-1}$ if and only if $\gcd(x, \varphi) = 1$

This is true since x has to be a public key in RSA and is chosen as such.

$\Rightarrow (\Delta, \cdot)$ - group

) Show that $(a2+1)(b2+1) = ((a+b)2+1) \bmod 4$

$\forall\ a, b \in \mathbb{Z}$; $(\Delta, \cdot)$ - cyclic group

$(a2+1)(b2+1) = ab2^2 + (a+b)2 + 1$

~~2~~ 2^2 is a multiple of 4 because one 2 can be divided by $(p-1)$ and the other by $(q-1)$ $\rightarrow 4 \mid 2^2 \Rightarrow 2^2 \bmod 4 = 0$

$\rightarrow (ab2^2 + (a+b)2 + 1) \bmod 4 = ((a+b)2+1) \bmod 4$

$\forall\ a, b \in \mathbb{Z}$

$2+1 \in \Delta$

2 has the same properties as 4 so

$m^2 = 1 \bmod N \quad \forall\ m \in \mathbb{Z}_N$ where $\gcd(m, p) = 1$ and $\gcd(m, q) = 1$

so $m^{2+1} = m \bmod N \quad \forall\ m \in \mathbb{Z}_N$

We can choose $2+1$ as a generator

The above identity shows that $(\mathbb{Z}_{2^t}, +) \cong (\Delta, \cdot)$

where $f(a) = a2+1 \bmod 4$, so $f(a+b) = (a2+1)(b2+1) \bmod 4$

$= ((a+b)2+1) \bmod 4$ which is generated by $2+1$

$\Rightarrow (2+1) = \Delta$

$\rightarrow (\Delta, \cdot)$ is a cyclic group

c) For $N = 85$, write down the group $(\Delta, \cdot)$ and verify it is cyclic.

$N = 85 = 5 \cdot 17$, so $\varphi = 64$ and $2 = 16$

$\langle 2+1 \rangle = \Delta$ so $2+1 = 17$

$(2+1)(2+1) = 2^2+1 \bmod 4 = 33$

$(2^2+1)(2+1) = 2^3+1 \bmod 4 = 49$

$(3^2+1)(2+1) = 4^2+1 = 65 = 1 \bmod 4$

So Δ is cyclic