[redacted] 24.11.2021

410 - SAL

= Exam =

1) $n = 64$; $g = 61$

a) $x = 10$; $y = 11$; $m = 12$

$h = ?$; $c_1 = ?$; $c_2 = ?$; decryption = ?

$(\mathbb{Z}_{64}^{\#}, +, \odot) \to$ additive group

The public Key of Alice is:

$h = g^x = g \cdot x \bmod n = 61 \cdot 10 \bmod 64 = (-3) \cdot 10 \bmod 64 = (-30) \bmod 64 = 34 \bmod 64$

Bob computes:

$c_1 = g^y = g \cdot y \bmod n = 61 \cdot 11 \bmod 64 = (-3) \cdot 11 \bmod 64 = (-33) \bmod 64 = 31 \bmod 64$

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

Bob sends $(c_1; c_2) = (31; 2)$ to Alice. Alice uses her secret Key x for decryption:

$m = (c_1^x)^{-1} c_2 = c_2 - c_1 \cdot x \bmod n = 2 - 31 \cdot 10 \bmod 64 = 2 - 310 \bmod 64 = 2 - 54 \bmod 64 = -52 \bmod 64 = 12$

b) Eva $\to g^{-1} \bmod n$ and finds out x

computations = ?

Agent Eva computes:

$g^{-1} \bmod n = 61^{-1} \bmod 64 = (-3)^{-1} \bmod 64 = 21$

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

$61 = 20 \cdot 3 + 1 \Rightarrow 1 = 61 - 20 \cdot 3 = 61 - 20 \cdot (-1) \cdot 61 = 21 \cdot 61$

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

2) $p = 23$; $g = 2$; $h = 18$; $(c_1; c_2) = (9; 10)$

$\underline{\text{+}}$

$m = ?$

$\underline{\text{+}}$

$(\mathbb{Z}_{23}^{\times}, \cdot, 1) \to$ multiplicative group

$h = g^x \bmod p \Rightarrow$ we need x such as $18 = 2^x \bmod 23$

Powers of 2 modulo 23:

$2; 4; 8; 16 = -7; 32 = 9; 64 = \boxed{18} = h$

So $2^6 \bmod 23 = h \Rightarrow x = 6$

$m = (c_1^x)^{-1} \cdot c_2 \bmod p = 10 \cdot (9^6)^{-1} \bmod 23$

$6 = 4 + 2$, so we compute powers of 9 mod 23:

$9 \rightsquigarrow 9^2 = 81 \bmod 23 = 12 \rightsquigarrow 9^4 = 12^2 = 144 \bmod 23 = 6$

So, $9^6 \bmod 23 = 9^4 \cdot 9^2 \bmod 23 = 6 \cdot 12 \bmod 23 = 72 \bmod 23 = 3$

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

$23 = 7 \cdot 3 + 2 \Rightarrow 2 = (-7) \cdot 3$

$3 = 1 \cdot 2 + 1 \Rightarrow 1 = 3 - 2 = 3 + 7 \cdot 3 = 8 \cdot 3$

$m = 10 \cdot 8 \bmod 23 = 11$

$(c_1 = g^y \Rightarrow 9 = 2^y \bmod 23 \Rightarrow y = 5$

$c_2 = m \cdot h^y \Rightarrow 10 = 11 \cdot 18^5 \bmod 23 = 11 \cdot (-5)^5 \bmod 23 =$
$= -13 \bmod 23 = 10)$

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

$\underline{\text{+}}$

$m = ?$; $\lambda(N)$

$\underline{\text{+}}$

$N = 85 = 5 \cdot 17$

$\lambda(N) = \operatorname{lcm}(4; 16) = 16$

$d = e^{-1} \bmod \lambda(N) = 11^{-1} \bmod 16 = 3$

$16 = 1 \cdot 11 + 5 \Rightarrow 5 = (-1) \cdot 11$

$11 = 2 \cdot 5 + 1 \Rightarrow 1 = 11 - 2 \cdot 5 = 11 + 2 \cdot 11 = 3 \cdot 11$

$m = c^d \bmod N = 12^3 \bmod 85 = 12 \cdot 12^2 \bmod 85 = 12 \cdot 59 \bmod 85$

$3 = 2 + 1$ | $= 28$

$12 \rightsquigarrow 12^2 = 144 = 59$

4) $\underline{N} = 3521$; $2899, 622, 1971, 1550$

$\underline{m = ?}$

$3521 = 7 \cdot 503$ $\quad$ ($7 \bmod 4 = 503 \bmod 4 = 3$)

$2899 \bmod 7 = 1 \bmod 7$ $(= 1^2) \Rightarrow \boxed{m_1 = 0}$

$622 \bmod 7 = 6 \bmod 7 = (-1) \bmod 7 \Rightarrow \boxed{m_2 = 1}$

$$\left(\frac{6}{7}\right) = \left(\frac{2}{7}\right) \cdot \left(\frac{3}{7}\right) = (-1)^{\frac{7^2-1}{8}} \cdot (-1)^{\frac{2\cdot 6}{4}} \left(\frac{7}{3}\right) = (-1)\left(\frac{1}{3}\right) = -1$$

$1971 \bmod 7 = 4 \bmod 7$ $(= 2^2) \Rightarrow \boxed{m_3 = 0}$

$1550 \bmod 7 = 3 \bmod 7 \Rightarrow \boxed{m_4 = 1}$

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

5) $\underline{p} = 17$; $m = 10$; $a = 7$; $b = 9$

$\underline{\text{Compute the protocol}}$

Alice sends to Bob:

$$A = m^a \bmod p = 10^7 \bmod 17 = 5$$

$7 = 4 + 2 + 1$

$10 \rightsquigarrow 10^2 = 100 \bmod 17 = 15 = (-2) \rightsquigarrow 10^4 = (-2)^2 = 4$

$10^7 \overset{\bmod 17}{=} 10^4 \cdot 10^2 \cdot 10 \bmod 17 = 4 \cdot (-2) \cdot 10 \bmod 17 = (-8) \cdot 10$
$\bmod 17 = 90 \bmod 17 = 5$

Bob sends to Alice:

$$B = A^b \bmod p = 5^9 \bmod 17 = 12$$

$9 = 8 + 1$

$5 \rightsquigarrow 5^2 = 25 \bmod 17 = 8 \rightsquigarrow 5^4 = 8^2 \bmod 17 = 13 = (-4) \rightsquigarrow$
$\rightsquigarrow 5^8 = (-4)^2 \bmod 17 = 16 \bmod 17 = (-1)$

$5^9 \bmod 17 = 5 \cdot 5^8 \bmod 17 = 5 \cdot (-1) \bmod 17 = 12$

Inverse Key of Alice: $a^{-1} \bmod (p-1)$

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

$16 = 2 \cdot 7 + 2 \Rightarrow 2 = (-2) \cdot 7$

$7 = 3 \cdot 2 + 1 \Rightarrow 1 = 7 - 3 \cdot 2 = 7 + 6 \cdot 7 = 7 \cdot 7$

Alice sends to Bob:

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

$7 = 4+2+1$

~~$12 \rightsquigarrow 12^2 = 144 \bmod$~~

$12 = (-5) \rightsquigarrow 12^2 = (-5)^2 = 25 \bmod 17 = 8 \rightsquigarrow 12^4 = 8^2 = 64 \bmod 17 =$

$= 13$

$12^7 \bmod 17 = (-5)\cdot 8 \cdot 13 \bmod 17 = (-5)\cdot 8\cdot(-4) \bmod 17 =$

$= (+20)\cdot 8 \bmod 17 = (+3)\cdot 8 \bmod 17 = +24 \bmod 17 = +7.$

For decryption, the inverse Key of Bob: $b^{-1} \bmod (p-1)$

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

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

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

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

Bob computes:

$m = C^{(b^{-1} \bmod p-1)} = 7^9 \bmod 17 = 10$

$9 = 8+1$

$7 \rightsquigarrow 7^2 = 49 \bmod 17 = 15 = (-2) \rightsquigarrow 7^4 = (-2)^2 = 4 \rightsquigarrow 7^8 = 4^2 =$

$= 16 = (-1)$

$7^9 \bmod 17 = (-1)\cdot 7 \bmod 17 = -7 \bmod 17 = 10$

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

$(\alpha, P(\alpha))$; where $\alpha \in \mathbb{Z}_{23} - \{0\}$ and $P(\alpha) \in \mathbb{Z}_{23}$

$(1,20)$; $(2,16)$; $(3,10)$

$s = P(0) = ?\ (\in \mathbb{Z}_{23})$

$P(x) = s + ax + bx^2$

We get the system:

$s + a + b = 20$

$s + 2a + 4b = 16$

$s + 3a + 9b = 10$

Subtract the first equation from the others:

410 → SAL

6) We get the system:

$$s + a + b = 20$$
$$a + 3b = -4 = 19 \quad | \cdot 2 \Rightarrow 2a + 6b = -8 = 15$$
$$2a + 8b = -10 = 13$$

We subtract the second from the 3rd:

$$\left.\begin{array}{l} s + a + b = 20 \\ a + 3b = 19 \\ 2b = -2 \Rightarrow \boxed{b = -1} \end{array}\right\} \Rightarrow a - 3 = 19 \Rightarrow a = 22 \text{ mod } 23 \Rightarrow \boxed{a = -1}$$

$$s - 1 - 1 = 20 \Rightarrow s - 2 = 20 \Rightarrow \boxed{s = 22 \text{ mod } 23 = -1}$$

7) a) 2 is a quadratic residue mod 23

$$\left(\frac{2}{23}\right) = (-1)^{\frac{23^2-1}{8}} = (-1)^{\frac{22 \cdot 24}{8}} = 1 \; (= 1^2) \Rightarrow \text{yes, is a quadratic residue mod 23}$$

b) square roots of 2 mod 23

$$a = 0 \Rightarrow a^2 - 2 = -2 = 21 \; ; \; \left(\frac{-2}{23}\right) = \left(\frac{-1}{23}\right)\left(\frac{2}{23}\right) = (-1) \cdot (-1)^{\frac{23^2-1}{8}} =$$
$$= (-1) \cdot 1 = -1 \Rightarrow \text{it's not a square}$$

Let $w = \sqrt{21} \notin \mathbb{F}_{23}$. We are working in $\mathbb{F}_{23}[w]$ with $w^2 = 21$ and we know

$$\sqrt{2} = (w + a)^{\frac{23+1}{2}} = (w + 0)^{\frac{24}{2}} = w^{12}$$

$12 = 8 + 4$

$$w = \sqrt{21} \rightsquigarrow w^2 = 21 = (-2) \rightsquigarrow w^4 = (-2)^2 = 4 \rightsquigarrow w^8 = 4^2 = 16 = -7$$

$$\sqrt{2} = w^8 \cdot w^4 = (-7) \cdot 4 = -28 \text{ mod } 23 = -5 \text{ mod } 23 = 18$$

Solutions are $\begin{cases} +18 \\ -18 = 5 \end{cases}$

8) $p \neq q$ (primes); $N = pq$; $\varphi = (p-1)(q-1)$; $\lambda = lcm(p-1; q-1)$
Dead Key: for all $m \in \mathbb{Z}_N$, $m^e = m \mod N$
Δ = set of dead Keys $[1, \varphi]$
a) $(\Delta, \cdot)$ = group
b) $(a\lambda + 1)(b\lambda + 1) = ((a+b)\lambda + 1) \mod \varphi$; $a, b \in \mathbb{Z}$
$(\Delta, \cdot)$ = cyclic group
c) $N = 85$; $(\Delta; \cdot) = ?$; verify that is cyclic

a) We have to prove:
- associativity: $(\forall) x, y, z \quad (xy)z = x(yz)$
- Neutral element: $(\forall) x \quad x \cdot 1 = 1 \cdot x = x$
- Inversibility: $(\forall) x, (\exists) y \quad xy = yx = 1$

$GCD(e, \varphi) = 1$; $m^e = m \mod N$
$d = e^{-1} \mod \varphi \Rightarrow$ RSA Key $\Rightarrow d \cdot e = e \cdot d = 1$ (inv.el)
1 = neutral el.; $(\forall)\, d$

b) $(a\lambda + 1)(b\lambda + 1) = ab\lambda^2 + a\lambda + b\lambda + 1$
$\cancel{ab\lambda^2}$ $\lambda = lcm(p-1, q-1) \Rightarrow (p-1) \cdot x$ or
$\Rightarrow y \cdot (q-1)$

$ab \cdot (p-1)^2 \cdot x^2 \mod (p-1)(q-1)$
$ab \cdot y^2 \cdot (q-1)^2 \mod (p-1)(q-1)$