**CS60065: Cryptography and Network Security** Total: 50 *points*

# Assignment 4

*Name: Anit Mangal* Due: *11.59 pm, Nov 07, 2024*

**Note**: The basic policies are stated in the course page. Using GPT (or similar tools) to solve problems from the assignment is **strictly prohibited**. Use of any other (possibly online) source(s) **must** be clearly stated in the solution. **Any dishonesty, if caught, will yield zero credits for the entire assignment.**

---

**A. [RSA and Primality Tests : $10 + 5 + 5 = 20$ points.]**

**Answers**

**A.1** We have $ed \equiv 1 \pmod{\lambda(n)}$

$$\begin{aligned}\lambda(n) &= \frac{\Phi(n)}{gcd(p-1, q-1)}\\ &= \frac{(p-1)(q-1)}{gcd(p-1, q-1)}\\ &= lcm(p-1, q-1) && [gcd(a,b) \times lcm(a,b) = a \times b]\end{aligned}$$

So, $\lambda(n) = k_1(p-1)$ and $\lambda(n) = k_2(q-1)$

Since $ed \equiv 1 \pmod{\lambda(n)}$,

$ed = t_1k_1(p-1) + 1$ and $ed = t_2k_2(q-1) + 1$

Now, decrypting ciphertext $c$,

$$\begin{aligned}c^d &\equiv (m^e)^d \pmod n\\ &\equiv m^{ed} \pmod n\end{aligned}$$

We need to prove that $m^{ed} \equiv m \pmod n$. By Chinese Remainder Theorem, it suffices to show that $m^{ed} \equiv m \pmod p$ and $m^{ed} \equiv m \pmod q$.

Case 1: $m$ and $p$ are not co-prime.
Since $p$ is prime, $m = rp$.
So, $m \equiv 0 \pmod p$ and $m^{ed} \equiv 0 \pmod p$
$\therefore m^{ed} \equiv m \pmod p$

Case 2: $m$ and $p$ are co-prime.

$$\begin{aligned}m^{ed} &\equiv m^{t_1k_1(p-1)+1} \pmod p\\ &\equiv \left(m^{p-1}\right)^{t_1k_1} m \pmod p\\ &\equiv 1^{t_1k_1} m \pmod p && \text{[By Fermat's Theorem]}\\ &\equiv m \pmod p\end{aligned}$$

$\therefore m^{ed} \equiv m \pmod p$
Similarly, $m^{ed} \equiv m \pmod q$
$\therefore m^{ed} \equiv m \pmod n$, which means encryption and decryption are still inverse operations.

**A.2a** We have $G(n) = \left\{a : a \in \mathbb{Z}_n^*, \left(\frac{a}{n}\right) \equiv a^{\frac{(n-1)}{2}} \pmod{n}\right\}$

First, we prove that $b \in G(n) \Rightarrow b^{-1} \in G(n)$.

$$\left(\frac{b}{n}\right)\left(\frac{b^{-1}}{n}\right) = \left(\frac{b.b^{-1}}{n}\right) \qquad \text{[Multiplicative Property of Jacobi symbol]}$$
$$= \left(\frac{1}{n}\right)$$
$$= 1 \qquad \text{[Property of Jacobi Symbol]}$$

Since Jacobi symbol can only take values -1, 0 and 1,

$$\Rightarrow \left(\frac{b}{n}\right) = \left(\frac{b^{-1}}{n}\right) \tag{1}$$

$$\text{Now, } b^{\frac{(n-1)}{2}}.\left(b^{-1}\right)^{\frac{(n-1)}{2}} \equiv \left(b.b^{-1}\right)^{\frac{(n-1)}{2}} \pmod{n}$$
$$\equiv 1^{\frac{(n-1)}{2}} \pmod{n}$$
$$\equiv 1 \pmod{n}$$

Also, $gcd(b, n) = 1 \Rightarrow gcd(b^{-1}, n) = 1$

So, $b^{n-1} \equiv 1 \pmod{n}$ and $\left(b^{-1}\right)^{n-1} \equiv 1 \pmod{n}$ (Fermat's Theorem)

So, $b^{\frac{(n-1)}{2}} \equiv 1 \text{ or } -1 \pmod{n}$. Same for $b^{-1}$

$$\Rightarrow b^{\frac{(n-1)}{2}} \equiv \left(b^{-1}\right)^{\frac{(n-1)}{2}} \pmod{n} \tag{2}$$

$$\text{Also } \left(\frac{b}{n}\right) \equiv b^{\frac{(n-1)}{2}} \pmod{n} \tag{3}$$

From (1), (2) and (3),

$$\Rightarrow \left(\frac{b^{-1}}{n}\right) \equiv \left(\frac{b}{n}\right) \equiv b^{\frac{(n-1)}{2}} \equiv \left(b^{-1}\right)^{\frac{(n-1)}{2}} \pmod{n}$$

$\therefore b \in G(n) \Rightarrow b^{-1} \in G(n)$

So, $\forall a, b \in G(n)$,

$\left(\frac{a}{n}\right) \equiv a^{\frac{(n-1)}{2}} \pmod{n}$ and $\left(\frac{b^{-1}}{n}\right) \equiv \left(b^{-1}\right)^{\frac{(n-1)}{2}} \pmod{n}$

$\Rightarrow \left(\frac{a.b^{-1}}{n}\right) \equiv \left(a.b^{-1}\right)^{\frac{(n-1)}{2}} \pmod{n}$

$\therefore (a.b^{-1}) \in G(n)$

So, $G(n)$ is a subgroup of $\mathbb{Z}_n^*$.

Using Lagrange's theorem, $|G(n)|$ divides $|\mathbb{Z}_n^*|$.

$\therefore\ |G(n)| \leq \frac{|\mathbb{Z}_n^*|}{2} \leq \frac{(n-1)}{2}$.

**A.2b** We have $n = p^k q$ and $a = 1 + p^{k-1}q$

Let $t = \frac{(n-1)}{2}$. Since $n$ is odd (p and q are odd), $t \in \mathbb{N}$.

$$\begin{aligned}
a^{\frac{(n-1)}{2}} &\equiv \left(1 + p^{k-1}q\right)^t \pmod{n} \\
&\equiv 1 + \binom{t}{1}(p^{k-1}q) + \cdots + \binom{t}{t}\left(p^{k-1}q\right)^t \pmod{n} && \text{[Binomial Theorem]} \\
&\equiv 1 + t(p^{k-1}q) \pmod{n} && [n \mid \left(p^{k-1}q\right)^t \;\; \forall t \geq 2] \\
&\equiv 1 + (n-1)(2^{-1})(p^{k-1}q) \pmod{n} \\
&\equiv 1 - (p^{k-1}q)(2^{-1}) \pmod{n} \\
&\equiv 1 + p^{k-1}q \pmod{n} \\
&\equiv a \pmod{n}
\end{aligned}$$

Now,

$$\begin{aligned}
\left(\frac{a}{n}\right) &= \left(\frac{a}{p}\right)^k \left(\frac{a}{q}\right) && \text{[Property of Jacobi symbol]} \\
&= \left(\frac{a}{q}\right) && [a \equiv 1 \pmod{p}] \\
&= 1 && [a \equiv 1 \pmod{q}]
\end{aligned}$$

Since, $a = 1 + p^{k-1}q \not\equiv 1 \pmod{n}$,

$\therefore \left(\frac{a}{n}\right) \not\equiv a^{\frac{(n-1)}{2}}$.

**B.** [**ElGamal Encryption and Diffie-Hellman Problems: $10 + 10 = 20$ points**.]

**Answers**

**B.1** Assume that the same ephemeral secret $k$ is used to encrypt $m_1$ and $m_2$ to $(c_{11}, c_{12})$ and $(c_{21}, c_{22})$ respectively, using generator $g$ on prime $p$, and the attacker knows the message $m_1$.

$$c_{12} \equiv m_1 e^k \pmod p$$
$$\equiv m_1 g^{dk} \pmod p$$
$$\Rightarrow c_{12} m_2 \equiv m_1 m_2 g^{dk} \pmod p$$

Also, $c_{22} \equiv m_2 e^k \pmod p$

$$\equiv m_2 g^{dk} \pmod p$$
$$\Rightarrow c_{22} m_1 \equiv m_1 m_2 g^{dk} \pmod p$$

So, $c_{12} m_2 \equiv c_{22} m_1 \pmod p$ and hence, $m_2 \equiv c_{22} m_1 {c_{12}}^{-1} \pmod p$.
$\therefore$ With $m_1$ known, the attacker can obtain $m_2$ if the same ephemeral secret is used to encrypt both of them.

**B.2** We have $E_i \equiv g^{x_i} h_i^r \pmod p$ and $h_i = h^{t_i} g^{s_i}, \forall i \in [l]$

$$\Rightarrow E_i \equiv g^{x_i} \left(h^{t_i} g^{s_i}\right)^r \pmod p$$
$$\equiv g^{x_i} \left(h^{rt_i} g^{rs_i}\right) \pmod p$$
$$\equiv g^{x_i + rs_i} h^{rt_i} \pmod p$$

We are given $p, C, D, \{E_1, E_2, \ldots, E_l\}, \vec{\mathbf{y}}, s_{\vec{\mathbf{y}}}, t_{\vec{\mathbf{y}}}$.

Now, to decrypt, compute $m' := \left(\prod_{i=1}^{l} E_i^{y_i}\right) . \left(C^{s_{\vec{\mathbf{y}}}} . D^{t_{\vec{\mathbf{y}}}}\right)^{-1} \pmod p$

$$\begin{aligned}
\left(\prod_{i=1}^{l} E_i^{y_i}\right) . \left(C^{s_{\vec{\mathbf{y}}}} . D^{t_{\vec{\mathbf{y}}}}\right)^{-1} &\equiv \left(\prod_{i=1}^{l} \left(g^{x_i + rs_i} h^{rt_i}\right)^{y_i}\right) . \left(\left(g^r\right)^{s_{\vec{\mathbf{y}}}} . \left(h^r\right)^{t_{\vec{\mathbf{y}}}}\right)^{-1} \pmod p \\
&\equiv \left(\prod_{i=1}^{l} g^{x_i y_i + r y_i s_i} h^{r y_i t_i}\right) . \left(g^{r s_{\vec{\mathbf{y}}}} . h^{r t_{\vec{\mathbf{y}}}}\right)^{-1} \pmod p \\
&\equiv \left(g^{\sum_{i=1}^{l} (x_i y_i + r y_i s_i)} h^{\sum_{i=1}^{l} r y_i t_i}\right) . \left(g^{\sum_{i=1}^{l} r s_i y_i} . h^{\sum_{i=1}^{l} r t_i y_i}\right)^{-1} \pmod p \\
&\equiv g^{\sum_{i=1}^{l} (x_i y_i)} \left(g^{\sum_{i=1}^{l} r y_i s_i} h^{\sum_{i=1}^{l} r y_i t_i}\right) . \left(g^{\sum_{i=1}^{l} r s_i y_i} . h^{\sum_{i=1}^{l} r t_i y_i}\right)^{-1} \pmod p \\
&\equiv g^{\sum_{i=1}^{l} (x_i y_i)} \pmod p \\
&\equiv g^{\langle \vec{\mathbf{x}}, \vec{\mathbf{y}} \rangle} \pmod p
\end{aligned}$$

So, $\left(\prod_{i=1}^{l} E_i^{y_i}\right) . \left(C^{s_{\vec{\mathbf{y}}}} . D^{t_{\vec{\mathbf{y}}}}\right)^{-1}$ yields $g^{\langle \vec{\mathbf{x}}, \vec{\mathbf{y}} \rangle} \pmod p$

**C. [Elliptic Curves: $5 + 5 = 10$ points.]**

**Answers**

**C.1** For curve $y^2 \equiv x^3 + 2x + 2$ over $\mathbb{Z}_{17}$,

$$\begin{aligned}
\text{Discriminant } \Delta &\equiv -16(4a^3 + 27b^2) \pmod{17} && \text{(For curve } y^2 = x^3 + ax + b\text{)} \\
&\equiv -16.(4.2^3 + 27.2^2) \pmod{17} \\
&\equiv -16.(15 + 6) \pmod{17} \\
&\equiv -16.4 \pmod{17} \\
&\equiv -13 \pmod{17} \\
&\equiv 4 \pmod{17}
\end{aligned}$$

$\therefore$ Discriminant is 4 (mod 17).
$P = (13, 7), Q = (6, 3)$

$$\begin{aligned}
\text{Slope } \lambda &\equiv (y_2 - y_1).(x_2 - x_1)^{-1} \pmod{17} && \text{(Line at points } (x_1, y_1), (x_2, y_2)\text{)} \\
&\equiv (3 - 7).(6 - 13)^{-1} \pmod{17} \\
&\equiv 13.(-7)^{-1} \pmod{17} \\
&\equiv 13.(10)^{-1} \pmod{17} \\
&\equiv 13.12 \pmod{17} && (10.12 \equiv 1 \pmod{17}) \\
&\equiv 3 \pmod{17}
\end{aligned}$$

Equation of line through P and Q is $y \equiv 3.x + 3 - 3.6 \equiv 3.x + 2$ over $\mathbb{Z}_{17}$
Finding intersection point R$(x_3, y_3)$ of the line with the curve.

$$\begin{aligned}
&(3x + 2)^2 \equiv x^3 + 2x + 2 \\
\Rightarrow &9x^2 + 12x + 4 \equiv x^3 + 2x + 2 \\
\Rightarrow &x^3 + 8x^2 + 7x + 15 \equiv 0
\end{aligned}$$

$\Rightarrow x_3 = -8 - 13 - 6 \pmod{17} = 7 \pmod{17}$
Using equation of line, $y_3 = 3.7 + 2 \pmod{17} = 6 \pmod{17}$. The required point has $y = -6 \pmod{17} = 11 \pmod{17}$.
So, point $P + Q = (7, 11)$.

**C.2** $E: y^2 \equiv x^3 + 3x + 2$ over $\mathbb{Z}_7$. Finding points

$x = 0 \Rightarrow y^2 \equiv 2 \pmod 7 \Rightarrow y = 4 \pmod 7$ & $y = 3 \pmod 7$
$x = 1 \Rightarrow y^2 \equiv 6 \pmod 7$(No solution)
$x = 2 \Rightarrow y^2 \equiv 2 \pmod 7 \Rightarrow y = 4 \pmod 7$ & $y = 3 \pmod 7$
$x = 3 \Rightarrow y^2 \equiv 3 \pmod 7$(No solution)
$x = 4 \Rightarrow y^2 \equiv 1 \pmod 7 \Rightarrow y = 1 \pmod 7$ & $y = 6 \pmod 7$
$x = 5 \Rightarrow y^2 \equiv 2 \pmod 7 \Rightarrow y = 4 \pmod 7$ & $y = 3 \pmod 7$
$x = 6 \Rightarrow y^2 \equiv 5 \pmod 7$(No solution)

So, points on the curve are $(0,4), (0,3), (2,4), (2,3), (4,1), (4,6), (5,4), (5,3)$ and $\mathcal{O}$ (point in infinity).
The order of the group is 9.
$\alpha = (0,3) \Rightarrow x_1 = 0, y_1 = 3$, Computing $2\alpha = (0,3) + (0,3)$

$$\begin{aligned}\lambda &= (3.0^2 + 3)(2.3)^{-1} \pmod 7\\ &= 3.6^{-1} \pmod 7\\ &= 3.6 \pmod 7\\ &= 4 \pmod 7\end{aligned}$$

So,

$$\begin{aligned}x_2 &= 4^2 - 0 - 0 \pmod 7\\ &= 16 \pmod 7\\ &= 2 \pmod 7\end{aligned}$$

$$\begin{aligned}y_2 &= 4(0 - 2) - 3 \pmod 7\\ &= 3 \pmod 7\end{aligned}$$

Hence, $2\alpha = (2,3)$. Calculating $3\alpha$.

$$\begin{aligned}\lambda &= (3.2^2 + 3)(2.3)^{-1} \pmod 7\\ &= 6 \pmod 7\end{aligned}$$

So, $x_3 = 6^2 - 2 - 2 = 4 \pmod 7$
$y_3 = 6.(2 - 4) - 3 = 6 \pmod 7$
Hence, $3\alpha = (4,6)$. Calculating $4\alpha$.
$\lambda = (3.4^2 + 3)(2.6)^{-1} = 6 \pmod 7$
$x_4 = 6^2 - 4 - 4 = 0 \pmod 7$
$y_4 = 4.(4 - 0) - 6 = 3 \pmod 7$
Hence, $4\alpha = (0,3) = \alpha$.
So, the order of $\alpha$ is 4 and $\alpha$ does not generate the group.