

Cryptology Homework #3

TCSS 581 - Autumn 2016

Kamatchi S. & Samir S. & Jonathan M.

Problem 1): Let $x, y, e, x^{-1} \in \mathcal{G}$ where $e \in \mathcal{G}$ is the identity element of \mathcal{G} and x^{-1} is such that both $xx^{-1} = e = x^{-1}x$ and $yx^{-1} = e = x^{-1}y$ hold. Therefore we have

$$xx^{-1} = yx^{-1} \tag{1.1}$$

$$xx^{-1} = x^{-1}y \tag{1.2}$$

$$x^{-1}x = yx^{-1} \tag{1.3}$$

$$x^{-1}x = x^{-1}y \tag{1.4}$$

By applying the cancelation rule ($ab = ac \Rightarrow b = c$ for $a, b, c \in \mathbb{G}$ for any group \mathbb{G}) to the expression in 1.1 and 1.4, it is clear that we have

$$x = y \tag{1.5}$$

Since \mathcal{G} is abelian, we may rewrite the expression in 1.2 as

$$xx^{-1} = x^{-1}x = x^{-1}y$$

or

$$xx^{-1} = yx^{-1} = x^{-1}y$$

From either expression, the application of the cancelation rule yields the same result as in expression 1.5. Similarly, we use the abelian property of \mathcal{G} to rewrite the expression in 1.3 as

$$x^{-1} x = x x^{-1} = y x^{-1}$$

or

$$x^{-1} x = x^{-1} y = y x^{-1}$$

Again, applying the cancelation rule to either expression yields the same result as in 1.5.

Therefore, every element in an abelian group must have a unique inverse.

□

Problem 2): Let \mathcal{G} be a finite group and $g \in \mathcal{G}$. Now define $\langle g \rangle \equiv g^0, g^1, g^2, \dots, g^k, \dots$, where $k \in \mathbb{N}$.

Beginning with the multiplicative case, let $m, n \in \mathbb{N}$ so that we have

$$g^m g^n = g^{m+n}$$

Since $m, n \in \mathbb{N}$ and \mathbb{N} is closed under addition, $(m+n) \in \mathbb{N}$, it is clear that $g^{m+n} \in \langle g \rangle$. Therefore, $\langle g \rangle$ is closed under its operation. From our definition of $\langle g \rangle$, we know that $g^0 \in \langle g \rangle$. Additionally, $g^0 \equiv e = 1$; therefore $\langle g \rangle$ contains the identity element. Now, let $m \in \mathbb{Z}^+$ and write $g^{-m} g^m$. Using $g^{-m} \equiv (g^{-1})^m$, this yields

$$g^{-m} g^m = (g^{-1})^m g^m = (g^{-1} g)^m = (e)^m = e = 1$$

which implies the existence of an inverse for each element in $\langle g \rangle$. Finally, let $m, n, k \in \mathbb{N}$, then we have

$$g^m (g^n g^k) = g^m (g^{n+k}) = g^{m+(n+k)} \quad (2.1)$$

Since \mathbb{N} is associative under addition, the expression in 2.1 may be rewritten as

$$g^{m+(n+k)} = g^{(m+n)+k} = (g^{m+n}) g^k = (g^m g^n) g^k$$

thereby demonstrating the associativity of operations in $\langle g \rangle$. Since \mathcal{G} is finite, it has order $m = |\mathcal{G}|$. Therefore, the elements of $\langle g \rangle$ will be repeats of elements in \mathcal{G} starting with g^{m+1} . Moreover, this means that $\langle g \rangle \subseteq \mathcal{G}$, thus satisfying the last condition for $\langle g \rangle$ to be a sub-group of \mathcal{G} .

Continuing with the additive case, let $m, n \in \mathbb{N}$ so that we have

$$m \times g n \times g = (m + n) \times g$$

Since $m, n \in \mathbb{N}$ and \mathbb{N} is closed under addition, $(m + n) \in \mathbb{N}$, it is clear that $(m + n) \times g \in \langle g \rangle$.

Therefore, $\langle g \rangle$ is closed under its operation. From our definition of $\langle g \rangle$, we know that $0 \times g \in \langle g \rangle$.

Additionally, $0 \times g \equiv e = 0$; therefore $\langle g \rangle$ contains the identity element. Now, let $m \in \mathbb{Z}^+$ and write $(-m) \times g m \times g$. Using $(-m) \times g \equiv m \times (-g)^m$, this yields

$$(-m) \times g m \times g = m \times (-g) m \times g = m \times (-g g) = m \times (e) = e = 0$$

which implies the existence of an inverse for each element in $\langle g \rangle$. Finally, let $m, n, k \in \mathbb{N}$, then we have

$$m \times g (n \times g k \times g) = m \times g ((n + k) \times g) = (m + (n + k)) \times g \quad (2.2)$$

Since \mathbb{N} is associative under addition, the expression in 2.2 may be rewritten as

$$(m + (n + k)) \times g = ((m + n) + k) \times g = (m + n) \times g k \times g = (m \times g n \times g) k \times g$$

thereby demonstrating the associativity of operations in $\langle g \rangle$. Since \mathcal{G} is finite, it has order $m = |\mathcal{G}|$. Therefore, the elements of $\langle g \rangle$ will be repeats of elements in \mathcal{G} starting with $(m + 1) \times g$. Moreover, this means that $\langle g \rangle \subseteq \mathcal{G}$, thus satisfying the last condition for $\langle g \rangle$ to be a sub-group of \mathcal{G} .

Problem 3): Since $\mathbb{Z}_p^* \equiv \{a \in \{1, 2, \dots, p-1\} \mid \gcd(a, p) = 1\}$, for any $p \in \mathbb{Z}^+$, the set of possible elements for $\mathbb{Z}_{p^e}^*$ is defined as

$$\mathbb{Z}_{p^e}^* \subset \{1, 2, \dots, p^e - 1\} \quad (3.1)$$

This implies the following relation between the cardinalities of these sets

$$|\mathbb{Z}_{p^e}^*| < |\{1, 2, \dots, p^e - 1\}|,$$

where $|\{1, 2, \dots, p^e - 1\}|$ has the value $|\{1, 2, \dots, p^e - 1\}| = (p^e - 1)$. It follows that the value of $|\mathbb{Z}_{p^e}^*|$ can be obtained by determining the set of all values in $\{1, 2, \dots, p^e - 1\}$ that do not satisfy the condition given in 3.1 and subtracting the cardinality of this set from $(p^e - 1)$. Since the common multiple is p , we will write this set in terms of p . Thus, the set of values in $\{1, 2, \dots, p^e - 1\}$ that do not satisfy the condition in 3.1 may be defined as

$$\{p, 2p, 3p, \dots, p p, 2p p, 3p p, \dots, p^2 p, \dots, (p^{e-1} - 1) p\}$$

This definition arises because only multiples of p do not satisfy the condition in 3.1 and because $(p^{e-1} - 1) p = p^e - p$ is the largest element of $\{1, 2, \dots, p^e - 1\}$ that does not satisfy the condition in

3.1. The cardinality of this set, $\{p, 2p, 3p, \dots, pp, 2pp, 3pp, \dots, p^2 p, \dots, (p^{e-1} - 1) p\}$ is clearly

$$|\{p, 2p, 3p, \dots, pp, 2pp, 3pp, \dots, p^2 p, \dots, (p^{e-1} - 1) p\}| = (p^{e-1} - 1)$$

Subtracting this value from $|\{1, 2, \dots, p^e - 1\}| = (p^e - 1)$ finally yields

$$\phi(p^e) = (p^e - 1) - (p^{e-1} - 1) = p^e - 1 - p^{e-1} + 1 = p^e - p^{e-1} = p^{e-1}(p - 1)$$

as desired.

To show that

$$\phi(pq) = \phi(p) \phi(q)$$

holds for any relatively prime p and q , we apply a similarly strategy to the one used above. The number of possible elements of \mathbb{Z}_{pq}^* is $pq - 1$. As before, we must take into account that some possible elements of \mathbb{Z}_{pq}^* will not satisfy the definition in 3.1. If we subtract the number of these elements, then we will have $\phi(pq) = |\mathbb{Z}_{pq}^*|$. Since there are $p - 1$ multiples of q that do not satisfy the condition in 3.1, we must subtract $p - 1$ from $pq - 1$. Similarly, since there are also $q - 1$ multiples of p that do not satisfy the same condition, we must also subtract $q - 1$ from $pq - 1$. Carrying out these subtractions gives

$$\begin{aligned}
\phi(pq) &= (pq - 1) - (p - 1) - (q - 1) \\
&= pq - 1 - p + 1 - q + 1 \\
&= pq - p - q + 1 \\
&= (p - 1)(q - 1) \\
&= \phi(p) \phi(q)
\end{aligned}$$

since $\phi(p)$ and $\phi(q)$ are defined as $\phi(p) = p - 1$ and $\phi(q) = q - 1$, respectively.

We will now use the previous result to show that, for an integer $N = \prod_i \{p_i^{e_i}\}$ and p_i distinct primes, we have

$$\phi(N) = \prod_i \{p_i^{e_i-1} (p_i - 1)\}$$

To begin, we substitute $N = \prod_i \{p_i^{e_i}\}$ for N in the previous expression. This gives

$$\phi(N) = \phi\left(\prod_i \{p_i^{e_i}\}\right)$$

Using the result $\phi(pq) = \phi(p) \phi(q)$, we have

$$\phi(N) = \prod_i \{\phi(p_i^{e_i})\}$$

Finally, we apply the result $\phi(p^e) = p^{e-1} (p - 1)$ to obtain

$$\phi(N) = \prod_i \{p_i^{e_i-1} (p_i - 1)\}$$

as expected.

Problem 4): We denote the cross product of groups \mathcal{G} and \mathcal{H} as $\mathcal{G} \times \mathcal{H}$ and define it by

$$(g, h) \circ (g', h') \equiv (g \circ_{\mathcal{G}} g', h \circ_{\mathcal{H}} h') \quad (4.1)$$

To show that $\mathcal{G} \times \mathcal{H}$ is a group, we begin by proving closure under its operation. Since \mathcal{G} and \mathcal{H} are groups, then we have $(g \circ_{\mathcal{G}} g') \in \mathcal{G}$ and $(h \circ_{\mathcal{H}} h') \in \mathcal{H}$. Thus $\mathcal{G} \times \mathcal{H}$ is closed under its operation. Next, we must show the existence of an identity in $\mathcal{G} \times \mathcal{H}$. If we modify the expression in 4.1 so that $g' = e_{\mathcal{G}}$ and $h' = e_{\mathcal{H}}$, then we have

$$\begin{aligned} (g, h) \circ (e_{\mathcal{G}}, e_{\mathcal{H}}) &= (g \circ_{\mathcal{G}} e_{\mathcal{G}}, h \circ_{\mathcal{H}} e_{\mathcal{H}}) \\ &= (g, h) \end{aligned}$$

Therefore, $\mathcal{G} \times \mathcal{H}$ contains an identity element and it is defined as $(e_{\mathcal{G}}, e_{\mathcal{H}})$. Next, we must demonstrate the existence of inverses in $\mathcal{G} \times \mathcal{H}$. To do this, we again modify the expression in 4.1. This time we substitute $g' = g^{-1}$ and $h' = h^{-1}$. Applying this substitution to the expression in 4.1 gives

$$\begin{aligned} (g, h) \circ (g^{-1}, h^{-1}) &= (g \circ_{\mathcal{G}} g^{-1}, h \circ_{\mathcal{H}} h^{-1}) \\ &= (e_{\mathcal{G}}, e_{\mathcal{H}}) \end{aligned}$$

Thus, $\mathcal{G} \times \mathcal{H}$ contains inverses for each of its elements. Lastly, we show that associativity holds in $\mathcal{G} \times \mathcal{H}$. We begin with

$$\begin{aligned}
((g_1, h_1) \circ (g_2, h_2)) \circ (g_3, h_3) &= (g_1 \circ_{\mathcal{G}} g_2, h_1 \circ_{\mathcal{H}} h_2) \circ (g_3, h_3) \\
&= ((g_1 \circ_{\mathcal{G}} g_2) \circ_{\mathcal{G}} g_3, (h_1 \circ_{\mathcal{H}} h_2) \circ_{\mathcal{H}} h_3)
\end{aligned} \tag{4.2}$$

Using the associativity of \mathcal{G} and \mathcal{H} , we have

$$((g_1 \circ_{\mathcal{G}} g_2) \circ_{\mathcal{G}} g_3, (h_1 \circ_{\mathcal{H}} h_2) \circ_{\mathcal{H}} h_3) = (g_1 \circ_{\mathcal{G}} (g_2 \circ_{\mathcal{G}} g_3), h_1 \circ_{\mathcal{H}} (h_2 \circ_{\mathcal{H}} h_3))$$

Thus, the expression in 4.2 becomes

$$\begin{aligned}
((g_1, h_1) \circ (g_2, h_2)) \circ (g_3, h_3) &= ((g_1 \circ_{\mathcal{G}} g_2) \circ_{\mathcal{G}} g_3, (h_1 \circ_{\mathcal{H}} h_2) \circ_{\mathcal{H}} h_3) \\
&= (g_1 \circ_{\mathcal{G}} (g_2 \circ_{\mathcal{G}} g_3), h_1 \circ_{\mathcal{H}} (h_2 \circ_{\mathcal{H}} h_3))
\end{aligned}$$

which implies that associativity holds for $\mathcal{G} \times \mathcal{H}$.

□

Problem 5): First, we will show that if $x \in \mathbb{Z}_N$, then $\forall x \in \mathbb{Z}_N^*$, $f(x) = (x_p, x_q)$ where $x_p \in \mathbb{Z}_p$ & $x_q \in \mathbb{Z}_q$ and $x_p \in \mathbb{Z}_p^*$ & $x_q \in \mathbb{Z}_q^*$. To do this, we assume, to the contrary, that $x_p \notin \mathbb{Z}_p^*$. This assumption implies that $\gcd([x \bmod p], p) \neq 1$ and, by extension, that $\gcd(x, p) \neq 1$. Moreover, this leads to the conclusion that $\gcd(x, N) \neq 1$. This cannot be, otherwise we would have $x \notin \mathbb{Z}_N^*$, violating the definition of \mathbb{Z}_N^* we started with. Therefore, $x_p \in \mathbb{Z}_p^*$ *must* hold. To show that $x_q \in \mathbb{Z}_q^*$ *must* also hold, we make the similar contrary assumption (that $x_q \notin \mathbb{Z}_q^*$) and arrive at a similar contradiction, thereby requiring that $x_q \in \mathbb{Z}_q^*$.

Next, we will show that f is an isomorphism. We begin by showing that f is one-to-one. To begin, let

$$f(x) = (x_p, x_q) = f(x')$$

Then, we let

$$x = x_p = x' \pmod{p}$$

and

$$x = x_q = x' \pmod{q}$$

This implies that $(x - x')$ is divisible by both p and q . However, since $p|N$ & $q|N$ and $\gcd(p, q) = 1$, we must have $(x - x')$ divisible by $pq = N$. This implies that $x = x' \pmod{N}$ and $x' = x \pmod{N}$. Moreover, since $x, x' \in \mathbb{Z}_N$, we must have $x = x'$ so f must also be **one-to-one**.

Continuing, since $|\mathbb{Z}_p| = p$ and $|\mathbb{Z}_q| = q$, we must have

$$|\mathbb{Z}_p \times \mathbb{Z}_q| = |\mathbb{Z}_p| \cdot |\mathbb{Z}_q| = pq \tag{5.1}$$

Now, we have $N = pq$ and $|\mathbb{Z}_N| = N$, so the expression in 5.1 becomes

$$\begin{aligned} |\mathbb{Z}_p \times \mathbb{Z}_q| &= pq \\ &= N \\ &= |\mathbb{Z}_N| \end{aligned}$$

Therefore, f must also be onto and, by extension, bijjective.

Finally, we must show that

$$\begin{aligned}
 f((a+b) \bmod N) &= [(a+b) \bmod p] \circ_{\mathbb{Z}_N} [(a+b) \bmod q] \\
 &= [(a+b) \bmod p] \boxplus [(a+b) \bmod q] \\
 &= f(a) \boxplus f(b)
 \end{aligned}$$

Since we have defined $f(x) \equiv ([x \bmod p], [x \bmod q])$, we may write $f((a+b) \bmod N)$ as

$$f((a+b) \bmod N) = ([[(a+b) \bmod N] \bmod p], [[(a+b) \bmod N] \bmod q]) \quad (5.2)$$

Now, since $p|N$ and $q|N$, we have

$$\begin{aligned}
 [[X \bmod N] \bmod p] &= [[X \bmod p] \bmod p] \\
 &= [X \bmod p]
 \end{aligned}$$

and

$$\begin{aligned}
 [[X \bmod N] \bmod q] &= [[X \bmod q] \bmod q] \\
 &= [X \bmod q]
 \end{aligned}$$

Therefore, the expression in 5.2 becomes

$$\begin{aligned}
f((a+b) \bmod N) &= ([[(a+b) \bmod N] \bmod p], [(a+b) \bmod N] \bmod q]) \\
&= ([[(a+b) \bmod p] \bmod p], [(a+b) \bmod q] \bmod q]) \\
&= ([(a+b) \bmod p], [(a+b) \bmod q])
\end{aligned}$$

Separating this result according to a and b gives

$$\begin{aligned}
([(a+b) \bmod p], [(a+b) \bmod q]) &= ([a \bmod p], [a \bmod q]) \boxplus ([b \bmod p], [b \bmod q]) \\
&= f(a) \boxplus f(b)
\end{aligned}$$

as desired.

□

Problem 6): We begin by applying the function mapping \mathbb{Z}_N to $\mathbb{Z}_p \times \mathbb{Z}_q$ (denoted f) to $(x^e)^d$. This gives us

$$\begin{aligned}
f((x^e)^d) &= ([(x_p^e)^d \bmod p], [(x_q^e)^d \bmod q]) \\
&= ([(x_p^{ed}) \bmod p], [(x_q^{ed}) \bmod q])
\end{aligned}$$

We now substitute $ed = 1 \bmod \phi(N)$ into our previous result to obtain

$$\begin{aligned}
f((x^e)^d) &= ([(x_p^{ed}) \bmod p], [(x_q^{ed}) \bmod q]) \\
&= ([(x_p^{1 \bmod \phi(N)}) \bmod p], [(x_q^{1 \bmod \phi(N)}) \bmod q])
\end{aligned}$$

Using the definition of $\phi(\dots)$ as well as the fact that $N = pq$, where p and q are distinct primes, we note that $\phi(N) = \phi(p) \phi(q)$. Therefore, our previous result can be rewritten as

$$\begin{aligned}
f\left((x^e)^d\right) &= \left(\left[\left(x_p^1 \bmod \phi(N)\right) \bmod p\right], \left[\left(x_q^1 \bmod \phi(N)\right) \bmod q\right]\right) \\
&= \left(\left[\left(x_p^1 \bmod \phi(p)\phi(q)\right) \bmod p\right], \left[\left(x_q^1 \bmod \phi(p)\phi(q)\right) \bmod q\right]\right)
\end{aligned} \tag{6.1}$$

Using the relation $a^{\phi(N)} = 1 \bmod N$, we see that $\phi(q)$ will cancel from the exponent in the first part of the left-hand-term in 6.1. Similarly, $\phi(q)$ will also cancel from the second part of the left-hand-term in 6.1. Therefore, our expression in 6.1 can be simplified to give

$$\begin{aligned}
f\left((x^e)^d\right) &= \left(\left[\left(x_p^1 \bmod \phi(p)\phi(q)\right) \bmod p\right], \left[\left(x_q^1 \bmod \phi(p)\phi(q)\right) \bmod q\right]\right) \\
&= \left(\left[\left(x_p^1 \bmod \phi(q)\right) \bmod p\right], \left[\left(q^1 \bmod \phi(p)\right) \bmod q\right]\right)
\end{aligned}$$

Noting that $b \bmod p = [b \bmod c] \bmod c$, we modify our previous result to give

$$\begin{aligned}
f\left((x^e)^d\right) &= \left(\left[\left(x_p^1 \bmod \phi(q)\right) \bmod p\right], \left[\left(x_q^1 \bmod \phi(p)\right) \bmod q\right]\right) \\
&= \left(\left[\left(\left(x_p^1 \bmod \phi(q)\right) \bmod p\right) \bmod p\right], \left[\left(\left(x_q^1 \bmod \phi(p)\right) \bmod q\right) \bmod q\right]\right)
\end{aligned}$$

Again using the relation $a^{\phi(N)} = 1 \bmod N$, we are able to simplify our previous result as

$$\begin{aligned}
f\left((x^e)^d\right) &= \left(\left[\left(\left(x^1 \bmod \phi(q)\right) \bmod p\right) \bmod p\right], \left[\left(\left(x^1 \bmod \phi(p)\right) \bmod q\right) \bmod q\right]\right) \\
&= ([x_p \bmod (pq)] \bmod p, [x_q \bmod (qp)] \bmod q)
\end{aligned} \tag{6.2}$$

Finally, we note that $pq = qp = N$ and recall the definition of $f(\dots)$. These relations allow us to rewrite our result in expression 6.2 to give

$$\begin{aligned}
f\left((x^e)^d\right) &= ([(x_p \bmod (pq)) \bmod p], [(x_q \bmod (qp)) \bmod q]) \\
&= ([(x_p \bmod N) \bmod p], [(x_q \bmod N) \bmod q]) \\
&= f(x \bmod N)
\end{aligned}$$

We then take the inverse of $f(\dots)$ to ultimately give

$$f\left((x^e)^d\right) = f(x \bmod N) \implies (x^e)^d = x \bmod N$$

as desired.

□

Problem 7): We start with values for N and $\phi(N)$. For clarity, we will denote the numerical value for $\phi(N)$ by the symbol Φ_N . Further, we know both that $N = pq$ and

$$\begin{aligned}
\phi(N) &= \phi(p) \phi(q) \\
&= (p-1)(q-1) \\
&= pq - p - q + 1 = \Phi_N
\end{aligned} \tag{7.1}$$

Additionally, note that the result in 7.1 was obtained using the relations $\phi(p) = p-1$ and $\phi(q) = q-1$. The result in 7.1, along with $N = pq$, means that we have the system of equations

$$\Phi_N = pq - p - q + 1 \tag{7.1}$$

and

$$N = pq \tag{7.2}$$

Rewriting the expression in 7.2 as $N = pq \Rightarrow q = N/p$ and applying the result, along with $N = pq$ to the expression in 7.1, we have

$$\begin{aligned} \Phi_N &= N - p - \frac{N}{p} + 1 \\ p\Phi_N &= pN - p^2 - N + p \\ 0 &= p^2 + (\Phi_N - N - 1)p + N \end{aligned} \tag{7.3}$$

which is solvable for p in polynomial time (using the quadratic formula). Applying the result from solving 7.3 for p to the expression in 7.2 yields a value for q in polynomial time as well.

Problem 8): For a public key encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$, we define **CPA** security according to the probability obtaining a secure result, as defined in the privacy experiment $\text{PubK}_{\mathcal{A}, \Pi}^{\text{LR-cpa}}$. This experiment goes as follows

The LR-oracle experiment $\text{PubK}_{\mathcal{A}, \Pi}^{\text{LR-cpa}}(n)$

1. $\text{Gen}(1^n)$ is run to obtain keys (pk, sk) .
2. A uniform bit $b \in \{0, 1\}$ is chosen.
3. The adversary \mathcal{A} is given input pk and oracle access to $\text{LR}_{pk, b}(\cdot, \cdot)$.
4. The adversary \mathcal{A} outputs a bit b' .
5. The adversary \mathcal{A} is defined to be 1 if $b' = b$, and 0 otherwise. If $\text{PubK}_{\mathcal{A}, \Pi}^{\text{LR-cpa}}(n) = 1$, we say that \mathcal{A} **succeeds**.

Using this definition for the experiment $\text{PubK}_{\mathcal{A}, \Pi}^{\text{LR-cpa}}$, we say that the encryption scheme Π is secure if the probability of \mathcal{A} succeeding, $\Pr [\text{PubK}_{\mathcal{A}, \Pi}^{\text{LR-cpa}}(n) = 1]$ satisfies the condition

$$\Pr [\text{PubK}_{\mathcal{A}, \Pi}^{\text{LR-cpa}}(n) = 1] \leq \frac{1}{2} + \text{negl}(n) \quad (8.1)$$

where $\text{negl}(n)$ is a function/value which is negligible on the order of n .

In detail, what we are seeking is indistinguishability of multiple encryptions. That is to say, if we have the plain-text of two different messages (*denote them m_1 and m_2*), which we encrypt using a public key (*denote it pk*), then an adversary \mathcal{A} having access to the cipher-text of both messages **and** the public key should not be able to distinguish the cipher-text of the messages under any circumstances. Using pk , the encryption algorithm (*denoted Enc_{pk}*) generates cipher-text from messages m_1 and m_2 . We use

$$\text{Enc}_{pk}(m_1) \quad \textbf{and} \quad \text{Enc}_{pk}(m_2)$$

to denote the cipher-text generated for these messages, respectively.

We denote both the information ($pk, \text{Enc}_{pk}(m_1), \& \text{Enc}_{pk}(m_2)$) available/provided to the adversary \mathcal{A} by

$$\mathcal{A}(pk, \text{Enc}_{pk}(m_1), \text{Enc}_{pk}(m_2)) \quad (8.2)$$

furthermore, we also use this notating to represent the outcome of running PubK on \mathcal{A} . When \mathcal{A} succeeds, then the expression in 8.2 yields the result

$$\mathcal{A}(pk, \text{Enc}_{pk}(m_1), \text{Enc}_{pk}(m_2)) = 1 \quad (8.3)$$

The expression in 8.2 yields

$$\mathcal{A}(pk, \text{Enc}_{pk}(m_1), \text{Enc}_{pk}(m_2)) = 0 \quad (8.4)$$

otherwise.

Since **CPA** security requires security over multiple encryptions using the same public key, we will formally define this security using **two** pairs of messages that are all being encrypted using the same public key. We denote the first pair of messages by $m_{1,0}$ and $m_{2,0}$. Similarly, the second pair of messages are denoted by $m_{1,1}$ and $m_{2,1}$. We now use the same notation as in 8.2 with these message pairs (*and their associated public key pk*) to represent the attack by \mathcal{A} . This gives

$$\mathcal{A}(pk, \text{Enc}_{pk}(m_{1,0}), \text{Enc}_{pk}(m_{2,0})), \quad (8.2 \text{ a})$$

for the first message pair; and

$$\mathcal{A}(pk, \text{Enc}_{pk}(m_{1,1}), \text{Enc}_{pk}(m_{2,1})), \quad (8.2 \text{ b})$$

for the second message pair.

Before proceeding, we point out that we can equivalently use the expression from 8.3 in place of the $\text{PubK}_{\mathcal{A}, \Pi}^{\text{LR-cpa}}(n) = 1$ term from 8.1. More clearly, we may formally write this equivalence as

$$\text{PubK}_{\mathcal{A}, \Pi}^{\text{LR-cpa}}(n) = 1 \quad \longleftrightarrow \quad \mathcal{A}(pk, \text{Enc}_{pk}(m_1), \text{Enc}_{pk}(m_2)) = 1$$

This allows us to write a version of 8.1 for both and . For the first message pair (*represented in*),

this gives the result

$$\Pr [\mathcal{A}(pk, \text{Enc}_{pk}(m_{1,0}), \text{Enc}_{pk}(m_{2,0})) = 1] \leq \frac{1}{2} + \text{negl}_0(n), \quad (8.3)$$

where negl_0 represents the negligible function required to satisfy this expression as applied to this message pair (*we are making allowances in case the results in and use different negl functions*). Writing our expression for the second message pair In a similar fashion yields

$$\Pr [\mathcal{A}(pk, \text{Enc}_{pk}(m_{1,1}), \text{Enc}_{pk}(m_{2,1})) = 1] \leq \frac{1}{2} + \text{negl}_1(n) \quad (8.4)$$

where negl_1 represents the negligible function required to satisfy this expression as applied to this message pair just as before (*we will see later that any difference between these negl functions is inconsequential; however differentiating between the negl functions used in either case is required for mathematical rigor*).

To continue the equation in 8.4 is subtracted from the equation in 8.3, after which the result *difference* will be simplified, thereby allowing us to obtain the following expressions for the initial and then the simplified results

$$\begin{aligned} & \left\{ \Pr [\mathcal{A}(pk, \text{Enc}_{pk}(m_{1,0}), \text{Enc}_{pk}(m_{2,0})) = 1] - \right. \\ & \quad \left. - \Pr [\mathcal{A}(pk, \text{Enc}_{pk}(m_{1,1}), \text{Enc}_{pk}(m_{2,1})) = 1] \right\} \leq \left(\frac{1}{2} + \text{negl}_0(n) \right) - \left(\frac{1}{2} + \text{negl}_1(n) \right) \\ & \left\{ \Pr [\mathcal{A}(pk, \text{Enc}_{pk}(m_{1,0}), \text{Enc}_{pk}(m_{2,0})) = 1] - \right. \\ & \quad \left. - \Pr [\mathcal{A}(pk, \text{Enc}_{pk}(m_{1,1}), \text{Enc}_{pk}(m_{2,1})) = 1] \right\} \leq \text{negl}_0(n) - \text{negl}_1(n) \end{aligned}$$

Taking the absolute value of this simplified expression allows us to obtain the result

$$\left| \Pr [\mathcal{A}(pk, \text{Enc}_{pk}(m_{1,0}), \text{Enc}_{pk}(m_{2,0})) = 1] - \Pr [\mathcal{A}(pk, \text{Enc}_{pk}(m_{1,1}), \text{Enc}_{pk}(m_{2,1})) = 1] \right| \leq |\text{negl}_0(n) - \text{negl}_1(n)| \quad (8.5)$$

Considering the right-hand-side of 8.5, we see that $|\text{negl}_0(n) - \text{negl}_1(n)|$ also negligible itself.

Therefore, we may define another negligible function, of order n , that satisfies the relation

$$|\text{negl}_0(n) - \text{negl}_1(n)| = \text{negl}(n),$$

where negl is another negligible function, of order n . Applying this to the expression in 8.5, we obtain the final result

$$\left| \Pr [\mathcal{A}(pk, \text{Enc}_{pk}(m_{1,0}), \text{Enc}_{pk}(m_{2,0})) = 1] - \Pr [\mathcal{A}(pk, \text{Enc}_{pk}(m_{1,1}), \text{Enc}_{pk}(m_{2,1})) = 1] \right| \leq \text{negl}(n) \quad (8.6)$$

which provides a formal definition for **CPA** security. In simple terms, the expression in 8.6 formally describes the requirement that a **CPA** secure encryption scheme be **non-deterministic**. That is to say, the expression in 8.6 mathematically quantifies the requirement that the cipher-text generated by any **CPA** secure encryption scheme be indistinguishable for any arbitrary pair of messages. It is the arbitrary nature of the messages that give rise to the requirement for non-determinism because the result in 8.6 must hold when the messages are **identical**. The only way for identical messages to be indistinguishably enciphered is for the encryption scheme used to encipher them to allow, with some non-zero probability, every possible message in the message space \mathcal{M} to be encrypted into any cipher-text in the cipher-text space, \mathcal{C} .

Now, we will define **CCA** security, again, in terms of an indistinguishability experiment. We will continue to denote the encryption scheme in question as $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$; however, we will

denote the experiment by $\text{PubK}_{\mathcal{A}, \Pi}^{\text{cca}}$. We describe *this* experiment as follows

The CCA indistinguishability experiment $\text{PubK}_{\mathcal{A}, \Pi}^{\text{cca}}(n)$

1. $\text{Gen}(1^n)$ is run to obtain keys (pk, sk) .
2. The adversary \mathcal{A} is given pk and access to a decryption oracle, $\text{Dec}_{sk}(\cdot)$. The adversary, \mathcal{A} , outputs a pair of messages, m_0, m_1 , which have the same length. (The messages must be in the message space, \mathcal{M} , that is associated with pk .)
3. A uniform bit $b \in \{0, 1\}$ is chosen, and then a cipher-text $c \leftarrow \text{Enc}_{pk}(m_b)$ is computed and given to \mathcal{A} .
4. The adversary \mathcal{A} continues to interact with the decryption oracle, but may not request a decryption of c itself. Finally, \mathcal{A} outputs a bit b' .
5. The output of the experiment is defined to be 1 if $b' = b$ (the adversary \mathcal{A} **succeeds**), and 0 otherwise.

Similar to how we arrived at the expression in 8.1, this definition of $\text{PubK}_{\mathcal{A}, \Pi}^{\text{cca}}$ can be used to show that the encryption scheme Π is secure by requiring that the probability of \mathcal{A} succeeding, $\Pr[\text{PubK}_{\mathcal{A}, \Pi}^{\text{cca}}(n) = 1]$ satisfy the condition

$$\Pr[\text{PubK}_{\mathcal{A}, \Pi}^{\text{cca}}(n) = 1] \leq \frac{1}{2} + \text{negl}(n) \quad (8.7)$$

Unfortunately, without serious modification, public key cryptograph is **NOT** secure under the **CCA** paradigm.

Problem 9): To begin, consider an arbitrary cyclic group \mathbb{G} and a generator $g \in \mathcal{G}$. Then, given any two group elements h_1 and h_2 , we define the function $\text{DH}(h_1, h_2)$ as

$$\text{DH}(h_1, h_2) = g^{\log_g h_1 \cdot \log_g h_2} \quad (9.1)$$

The **DDH** Assumption is that the result of $\text{DH}(h_1, h_2)$, on any uniform group elements h_1 and h_2 , is indistinguishable from any other uniform element of the group.

Now, we define the **El Gamal** encryption algorithm according to

- Accept input public key $pk = \langle \mathbb{G}, q, g, h \rangle$.
- Chose $y \leftarrow \mathbb{Z}_q$
- Output the cipher text $c = \langle c_1, c_2 \rangle$ determined according to

$$c = \langle c_1, c_2 \rangle = \langle g^y, h^y \cdot m \rangle$$

We also note that the **El Gamal** encryption algorithm uses the private key $sk = \langle \mathbb{G}, q, g, x \rangle$. Where $(\mathbb{G}, q, g,)$ is obtained from a generator and h is defined $h \equiv g^x$. Therefore, cipher-text may be encrypted according to the relation

For cipher-text $c = \langle c_1, c_2 \rangle$ decrypt using $m \equiv \frac{c_2}{c_1^x}$

Problem 10): Any **RSA** implementation where the modulus N is prime will always be insecure.

There are two reasons for this insecurity. These reasons are rooted in the fundamental mathematics that underlies *all* **RSA** based crypto-systems. While each of these reasons is sufficient to cause a break in security on its own, choosing the modulus as N a prime forces both of these to occur.

The first reason has to do with the elements in the group defined by N and used in any **RSA** crypto-system, $\mathbb{G} = \mathbb{Z}_N^*$. When N is prime, then \mathbb{Z}_N^* , is automatically known because $\mathbb{Z}_N = \mathbb{Z}_N^*$, by the definition of primality. The problem is that this every element in $[0, N]$ will be in the group eliminating the ambiguity about which elements belong to the group in use. Furthermore, this choice of N eliminates the ability to use any element of the group as a generator. This makes the *Discrete Logarithm Problem* easier to solve. Since the difficulty of the *Discrete Logarithm Problem* constitutes a critical part of the fundamental mathematical assumptions relied upon by all **RSA** crypto-systems, this choice of N causes any implementation using it to be insecure.

The other reason setting the modulus N as a prime is problematic has to do with the order of \mathbb{Z}_N^* , $|\mathbb{Z}_N^*|$. When N is prime, then $|\mathbb{Z}_N^*|$ cannot be prime for any $N > 3$, by the definition primality. The problem here is that the *Decisional Diffie-Hellman Problem* is not hard for groups with a non-prime order. The security **RSA** relies upon the fundamental mathematical difficulty of solving the *Decisional Diffie-Hellman Problem*. Since this choice of N makes the *Decisional Diffie-Hellman Problem* easier to solve, it will also break the security of any **RSA** implementation using that choice.

Problem 11):

Problem 12):

Problem 14):

Problem 15):

Problem 16):

Problem 17):

Problem 18):