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 $x\,x^{-1} = e = x^{-1}\,x$ and $y\,x^{-1} = e = x^{-1}\,y$ hold. Therefore we have

$$x\,x^{-1} = y\,x^{-1} \tag{1.1}$$

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

$$x^{-1}\,x = y\,x^{-1} \tag{1.3}$$

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

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

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

or

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

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 $\langle g\rangle \equiv g^0, g^1, g^2, \ldots, g^k, \ldots$, 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 $g^{-m} \equiv \left(g^{-1}\right)^m$, this yields

$$g^{-m}\,g^m = \left(g^{-1}\right)^m\,g^m = \left(g^{-1}\,g\right)^m = (e)^m = e = 1$$

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

$$g^m\,\left(g^n\,g^k\right) = g^m\,\left(g^{n+k}\right) = g^{m+(n+k)} \tag{2.1}$$

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

$$g^{m+(n+k)} = g^{(m+n)+k} = \left(g^{m+n}\right)\, g^k = (g^m\, g^n)\, g^k$$

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

$$m \times g\ (n \times g\, k \times g) = m \times g\ ((n + k) \times g) = (m + (n + k)) \times g \tag{2.2}$$

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 $\mathbb{Z}_{\mathfrak{p}}^{\star} \equiv \{a \in \{1, 2, \ldots, \mathfrak{p}-1\} \mid \gcd(a, \mathfrak{p}) = 1\}$, for any $\mathfrak{p} \in \mathbb{Z}^{+}$, the set of possible elements for $\mathbb{Z}_{p^e}^{\star}$ is defined as

$$\mathbb{Z}_{p^e}^{\star} \subset \{1, 2, \ldots, p^e - 1\} \tag{3.1}$$

This implies the following relation between the cardinalities of these sets

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

where $|\{1, 2, \ldots, p^e - 1\}|$ has the value $|\{1, 2, \ldots, p^e - 1\}| = (p^e - 1)$. It follows that the value of $|\mathbb{Z}_{p^e}^{\star}|$ can be obtained by determining the set of all values in $\{1, 2, \ldots, p^e - 1\}$ that do not satisfy the conition 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 be. Thus, the set of values in $\{1, 2, \ldots, p^e - 1\}$ that do not satisfy the condition in 3.1 may be defined as

$$\left\{p, 2p, 3p, \ldots, p\,p, 2p\,p, 3p\,p, \ldots, p^2\,p, \ldots, \left(p^{e-1} - 1\right)\, p\right\}$$

This definition arises becuase only multiples of p do not satistfy the condition in 3.1 and because $\left(p^{e-1} - 1\right)\, p = p^e - p$ is the largest element of $\{1, 2, \ldots, p^e - 1\}$ that does not satisfy the confition in 3.1. The cardinality of this set, $\left\{p, 2p, 3p, \ldots, p\,p, 2p\,p, 3p\,p, \ldots, p^2\,p, \ldots, \left(p^{e-1} - 1\right)\, p\right\}$ is clearly

$$|\left\{p, 2p, 3p, \ldots, p\,p, 2p\,p, 3p\,p, \ldots, p^2\,p, \ldots, \left(p^{e-1} - 1\right)\, p\right\}| = \left(p^{e-1} - 1\right)$$

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

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

as desired.

To show that

$$\phi\left(pq\right) = \phi\left(p\right)\,\phi\left(q\right)$$

holds for any relatively prime p and q, we apply a similarly strategy to the one used above. The number of possible elements of $\mathbb{Z}^{\star}_{pq}$ is $pq - 1$. As before, we must take into account that some possible elements of $\mathbb{Z}^{\star}_{pq}$ will not satisfy the definition in 3.1. If we subtract the number of these elements, then we will have $\phi\left(pq\right) = |\mathbb{Z}^{\star}_{pq}|$. 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

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

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

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

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

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

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

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

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

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, the we have $(g \circ_{\mathcal{G}} g') \in \mathcal{G}$ and $(h \circ_{\mathcal{H}} h') \in \langle$. 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 inversed 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

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

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

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

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 $\mathcal{G} \times \mathcal{H}$.

$\square$

Problem 5): First, we will show that if $x \in \mathbb{Z}_N$, then $\forall x \in \mathbb{Z}_N^\star,\ f(x) = (x_p, x_q)$ where $x_p \in \mathbb{Z}_p$ & $x_q \in \mathbb{Z}_q$ and $x_p \in \mathbb{Z}_p^\star$ & $x_q \in \mathbb{Z}_q^\star$. To do this, we assume, to the contrary, that $x_p \notin \mathbb{Z}_p^\star$. This assumption implies that $\gcd([x \mod p], p) \neq 1$ 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 $z \notin \mathbb{Z}_N^\star$, violating the definition of $\mathbb{Z}_N^\star$ we started with. Therefore, $x_p \in \mathbb{Z}_p^\star$ *must* hold. To show that $x_q \in \mathbb{Z}_q^\star$ *must* also hold, we make the similar contrary assumption (that $x_q \notin \mathbb{Z}_q^\star$) and arrive at a similar contradiction, thereby requiring that $x_q \in \mathbb{Z}_q^\star$.

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

$$x = x_p = x' \mod p$$

and

$$x = x_q = x' \mod q$$

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 $x = x' \mod N$ and $x' = x \mod N$. Moreover, since $x, x' \in \mathbb{Z}_N$, we must have $x = x'$ so f *must* alsp 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 <u>onto</u> and, by extension, <u>bijective</u>.

Finally, we must show that

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

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

$$f\left((a+b) \mod N\right) = \left([[(a+b) \mod N] \mod p], [[(a+b) \mod N] \mod q]\right) \tag{5.2}$$

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

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

and

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

Therefore, the expression in 5.2 becomes

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

Separating this result according to a and b gives

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

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 $\left(x^e\right)^d$. This gives us

$$\begin{aligned} f\left(\left(x^{e}\right)^{d}\right) &= \left(\left[\left(x_{p}^{e}\right)^{d} \mod p\right], \left[\left(x_{q}^{e}\right)^{d} \mod q\right]\right) \\ &= \left(\left[\left(x_{p}^{e\,d}\right) \mod p\right], \left[\left(x_{q}^{e\,d}\right) \mod q\right]\right) \end{aligned}$$

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

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

Using the definition of $\phi(\cdots)$ 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

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

Using the relation $a^{\phi(N)} = 1 \mod N$, 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

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

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

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

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

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

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

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

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

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

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

$$N = p\,q \tag{7.2}$$

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

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

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.

<ins>**Problem 8):**</ins> For a public key encryption scheme $\prod = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$, we define **CPA** security according to the probability obtaining a secure result, as defined in the privacy experiment

$\mathsf{PubK}_{\mathcal{A},\prod}^{\text{LR-cpa}}$. This experiment goes as follows

The LR-orcale experiment $\mathsf{PubK}_{\mathcal{A},\prod}^{\text{LR-cpa}}(n)$

1. $\mathsf{Gen}(1^n)$ *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* $\mathsf{LR}_{pk,b}(\cdot,\cdot)$.
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* $\mathsf{PubK}_{\mathcal{A},\prod}^{\text{LR-cpa}}(n) = 1$, *we say that* $\mathcal{A}$ **succeeds**.

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

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

where $\mathsf{negl}\ (n)$ 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

$$\mathsf{Enc}_{pk}(m_1) \qquad \underline{\textbf{and}} \qquad \mathsf{Enc}_{pk}(m_2)$$

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

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

$$\mathcal{A}\left(pk, \mathsf{Enc}_{pk}\left(m_1\right), \mathsf{Enc}_{pk}\left(m_2\right)\right) \tag{8.2}$$

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

$$\mathcal{A}\left(pk, \mathsf{Enc}_{pk}\left(m_1\right), \mathsf{Enc}_{pk}\left(m_2\right)\right) = 1 \tag{8.3}$$

The expression in 8.2 yields

$$\mathcal{A}\left(pk, \mathsf{Enc}_{pk}\left(m_1\right), \mathsf{Enc}_{pk}\left(m_2\right)\right) = 0 \tag{8.4}$$

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* ph) to represent the attack by $\mathcal{A}$. This gives

$$\mathcal{A}\left(pk, \mathsf{Enc}_{pk}\left(m_{1,0}\right), \mathsf{Enc}_{pk}\left(m_{2,0}\right)\right), \tag{8.2 a}$$

for the first message pair; and

$$\mathcal{A}\left(pk, \mathsf{Enc}_{pk}\left(m_{1,1}\right), \mathsf{Enc}_{pk}\left(m_{2,1}\right)\right), \tag{8.2 b}$$

for the second message pair.

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

$$\mathsf{PubK}^{\mathsf{LR\text{-}cpa}}_{\mathcal{A},\prod}(n) = 1 \qquad \longleftrightarrow \qquad \mathcal{A}\left(pk, \mathsf{Enc}_{pk}\left(m_1\right), \mathsf{Enc}_{pk}\left(m_2\right)\right) = 1$$

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

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

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

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

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

$$\Big\{ \Pr\left[\mathcal{A}\left(pk, \mathsf{Enc}_{pk}\left(m_{1,0}\right), \mathsf{Enc}_{pk}\left(m_{2,0}\right)\right) = 1\right] - \\ - \Pr\left[\mathcal{A}\left(pk, \mathsf{Enc}_{pk}\left(m_{1,1}\right), \mathsf{Enc}_{pk}\left(m_{2,1}\right)\right) = 1\right]\Big\} \leq \left(\frac{1}{2} + \mathsf{negl}_0\left(n\right)\right) - \left(\frac{1}{2} + \mathsf{negl}_1 0\left(n\right)\right)$$

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

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

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

Considering the right-hand-side of 8.5, we see that $\Big|\mathsf{negl}_0\left(n\right) - \mathsf{negl}_1\left(n\right)\Big|$ also negligible itself. Therefore, we may define another negligible function, of order n, that satisfies the relation

$$\Big|\mathsf{negl}_0\left(n\right) - \mathsf{negl}_1\left(n\right)\Big| = \mathsf{negl}\left(n\right),$$

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

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

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 mathematical 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 probably, every possible message in the message space ($\mathcal{M}$) to encrypted into any cipher-text in the cipher-text space ($\mathcal{C}$).

We now

Problem 9):

Problem 10):

Problem 11):

Problem 12):

Problem 14):

Problem 15):

Problem 16):

Problem 17):

Problem 18):