CPSC 418 / MATH 318 — Introduction to Cryptography
ASSIGNMENT 3

Name: Aifaz Dhuka
Student ID: 30069823

Problem 1 — Flawed MAC designs (11 marks)

a. Suppose an attacker know PHMAC$_k(M_1)$. Since-
PHMAC$_k(M_1) = I_T Hash(K||M_1)$, we know that the attacker also knows $I_T Hash(K||M_1) = I_T Hash(K||P_1||P_2||...||P_L)$. This further implies that the attacker has knowledge about the following:

$$\text{PHMAC}_k(M_1) = I_T Hash(K||M_1) = f(...(f(f(f(0_n, k), P_1), P_2), P_3)..., P_L)$$

Let $M_2 = M_1||X$, where X be an arbitrary n-bit block. Since k is not known to the attack and since f is public, the attacker can compute PHMAC of M_2 without the knowledge of k and just by knowing the f, M_1 and PHMAC$_k(M_1)$. Now by looking at the algorithm, we know that PHMAC$_k(M_2)$ =PHMAC$_k(M_1||X) = f(f(...(f(f(f(0_n, k), P_1), P_2), P_3)..., P_L), X) = f(\text{PHMAC}_k(M_1), X)$. Since f is public, the attacker is able to compute $f(\text{PHMAC}_k(M_1), X)$ and thus he is able to compute PHMAC$_k(M_2)$ without knowing k. Since he is able to get that, the PHMAC is not computational resistant.

b. Suppose an attacker know AHMAC$_k(M_1)$. Suppose $I_T Hash$ is not weakly collision resistant. Since AHMAC$_k(M_1) = I_T Hash(M_1||K)$. So this implies the following:

$$\text{AHMAC}_k(M_1 =) I_T Hash(M_1||K) = f(...(f(f(f(0_n, P_1), P_2), P_3), P_4), ..., k)$$

$$= f(I_T Hash(M_1), k)$$

Since we know $I_T Hash$ is not weakly collision resistant, it means given X, there exists another (and is feasible to find) Y such that $X \neq Y$ and $I_T Hash(X) = I_T Hash(Y)$. Let M_2 be the colliding message with M_1 for the $I_T Hash$ function. So $I_T Hash(M_1) = I_T Hash(M_2)$. Since we know how AHMAC$_k(M_1) = f(I_T Hash(M_1), k)$ And since we know $I_T Hash(M_1) = I_T Hash(M_2)$, then we could do the following:

$$AHMAC_k(M_2) = f(I_T Hash(M_2), k) = f(I_T Hash(M_1), k) = AHMAC_k(M_1)$$

So we see that in this case AHMAC$_k(M_2)$ =AHMAC$_k(M_1)$. Since we can calculate AHMAC of M_2 without knowing k, we know it is not computationally resistant.

Problem 2 — Fast RSA decryption using Chinese remaindering (7 marks)

Suppose M is the message that is encrypted using the normal RSA way that is $C = M^e \bmod n$. We know p and q and also that $n = pq$. We would show that the alternative way to decrypt the message does get the correct message. Let M' be the message decrypted using the alternative method. We will show that $M' = M = C^d$. We know that $M = C^d \mod n$ which could be written as $C^d \mod pq$ since $pq = n$. Since we know p and q are relatively prime, we can use the Chinese remainder theorem and get the following:

$$M = C^d \mod p$$

$$M = C^d \mod q$$

Further from the procedure, we know that $d_p = d \mod (p-1)$ which implies that $d = k(p-1)+d_p$ where $k \in \mathbb{Z}$. Similarly $d_q = d \mod (q-1)$ which implies that $d = j(q-1) + d_q$ where $j \in \mathbb{Z}$. So

$$M = C^d \mod p = C^{k(p-1)+d_p} \mod p = (C^{p-1})^k * C^{d_p}$$

. Since we know for prime p, $a^{p-1} \mod p = 1$, we get

$$(C^{p-1})^k * C^{d_p} \mod p = 1^k * C^{d_p} \mod p = C^{d_p} \mod p = M_p \mod p$$

. We get M_q similarly to the above part. So now we have the following:

$$M = C^{d_p} \mod p = M_p \mod p$$

$$M = C^{d_q} \mod p = M_q \mod q$$

Further, this implies that M_p and M_q can be written as:

$$M_p = M + pk$$
$$M_q = M + qm$$

where m and k are integers.
We know that since $gcd(p,q) = 1$, there exist x and y such that $px + qy = 1$. Now, since we know $M' = pxM_q + qyM_p \mod n$, we can do the following using the M_p and M_q values:

$$\begin{aligned}
M' &= pxM_q + qyM_p \mod n \\
&= px(M+qm) + qy(M+pk) \mod n \\
&= pxM + pxqm + qyM + pkqy \mod n \\
&= ((pxM + qyM) \mod n + (pq)xm \mod n + (pq)ky \mod n) \mod n \\
&= ((pxM + qyM) \mod n + 0 + 0) \mod n \\
&= M(px+qy) \mod n \\
&= M(1) \mod n \\
&= M \mod n
\end{aligned}$$

We get $M' = M \mod n$. Thus this alternative way of decryption works correctly.

Problem 3 — RSA primes too close together (21 marks)

a. Since we know $n = pq$ and we also know that p and q are primes. So the factors of n are 1, n, p and q. Suppose x and y are integers and $x > y > 0$. Let $n = x^2 - y^2 = (x + y)(x - y)$. So, since we know $n = pq$ and $p > q$ and $x > y > 0$, which implies $x + y > x - y > 0$. So We can substitute as follows, $p = x + y$ and $q = x - y$. Now, the following is trivial (using simultaneous equations): $p + q = 2x$ and $p - q = 2y$. This leads us to our first solution that $x = \frac{p+q}{2}$ and $y = \frac{p-q}{2}$.
Similarly we could write $n = n * 1$ and it is obvious that $n > 1 > 0$ as n is a product of two primes and (just a random prime, not related to pq) even if both the primes were the smallest prime that is 2, n would be 4. So we can substitute as follows, $n = x + y$ and $1 = x - y$ as we know $x + y > x - y$. So, using simultaneous equations, we get $n + 1 = 2x$ and $n - 1 = 2y$ which leads us to another solution that is $x = \frac{n+1}{2}$ and $y = \frac{n-1}{2}$.
Since n could be written as products of 1,n, p and q only, these are the only solutions.

b. We know $n = pq$ and we also know that $p > q$ and since p and q are odd primes, $p > q > 2$. Since $n = pq$, this implies that $n + 1 > pq$ and since $q > 2$, $n + 1 > pq > 2p = p + p$ and since $p > q$, this follows that $p + p > p + q$. Thus we reached a conclusion that $n + 1 > p + q$.

c. First I will show that the second half of the inequality is true, that is $\frac{p+q}{2} < p$. This could also be written as $p + q < 2p = p + p$. Since we know $p > q$, this implies that $p + q < p + p = 2p$. And thus the second half of the inequality is true.
Now I will show the first half of the inequality, that is $\sqrt{n} < \frac{p+q}{2}$. This could be simlified as $n < (\frac{p+q}{2})^2 = \frac{(p+q)^2}{4}$. This could be further simplified as

$$4n < (p + q)^2 = p^2 + 2pq + q^2 = p^2 + 2n + q^2$$

Now we could subtract $2n$ from both sides and get $2n < p^2 + q^2$ which could be written as $0 < p^2 + q^2 - 2n = p^2 + q^2 - 2pq = (p - q)^2$. So we have the inequality rewritten as $0 < (p - q)^2$ and since we know $p > q$, then $(p - q) > 0$ and so is $(p - q)^2 > 0$ thus the first half of the inequality is correct.
Thus $\sqrt{n} < \frac{p+q}{2} < p$ is true(correct).

d. Since lines 1 and 2 are just assignment statments and some colculations, ther terminate.
Next we will show that that the while loop is satisfied when $x = (p + q)/2$. So when $x = (p + q)/2$ and since $y = \sqrt{x^2 - n}$, this follows:

$$\begin{aligned}
y &= \sqrt{x^2 - n} \\
&= \sqrt{(\frac{p+q}{2})^2 - n} \\
&= \sqrt{\frac{p^2 + q^2 + 2pq}{4} - n} \\
&= \sqrt{\frac{p^2 + q^2 + 2n - 4n}{4}} \\
&= \sqrt{\frac{p^2 + q^2 - 2n}{4}} \\
&= \sqrt{\frac{(p-q)^2}{4}} = \frac{(p-q)}{2}
\end{aligned}$$

Since p and q are both odd, their difference will be even and can be written as $2k$ where k is an integer and thus we would get $y = \frac{(p-q)}{2} = \frac{2k}{2} = k$. Thus we get y as an integer when $x = (p+q)/2$.

Now we want the show that $x = (p+q)/2$ is the first value that gives an integer y. We will prove this by contradiction. Suppose there exist $x = a$ such that $y = \sqrt{x^2 - n}$ is an integer, where $\lceil(\sqrt{n})\rceil = \lceil(\sqrt{pq})\rceil \leq a < (p+q)/2$. So $n = a^2 + y^2$ and from part a, we know that x values are $(n+1)/2$ and $(p+q)/2$ such that y is an integer. So a has to be $(n+1)/2$. Since we know $p + q < n + 1$, this implies that $(p+q)/2 < (n+1)/2$ which is a contradiction to the supposition that $a < (p+q)/2$. Thus $x = (p+q)/2$ is the first x value that satisfies the while condition. And thus the while loop terminates as well.

Then algorithm outputs x-y. So $x - y = \frac{p+q}{2} - \frac{p-q}{2} = \frac{0+2q}{2} = q$. Thus the output is q and will thus terminate.

e. We know that the range of values x, that is when $\lceil(\sqrt{n})\rceil \leq x < (p+q)/2$, then the while loop fails and when $x = (p+q)/2$, this is the last time the while loop test is run. So we know that that the while loop failed $(p+q)/2 - \lceil(\sqrt{n})\rceil$ times and succeeded once. so total= $(p+q)/2 - \lceil(\sqrt{n})\rceil + 1$

f. We know $(x+\sqrt{n})(x-\sqrt{n}) = x^2 - n = y^2$. We akso know that $\sqrt{n} \leq \lceil(\sqrt{n})\rceil$. We also know from part c that $\sqrt{n} < \frac{p+q}{2} = x$, which implies that $1/\sqrt{n} > 1/x$. So we get the following:

$$(x - \lceil(\sqrt{n})\rceil) \leq (x - \sqrt{n}) = \frac{y^2}{(x+\sqrt{n})} < \frac{y^2}{(\sqrt{n}+\sqrt{n})} = \frac{y^2}{(2\sqrt{n})}$$

. Thus $(x - \lceil(\sqrt{n})\rceil) < \frac{y^2}{(2\sqrt{n})}$ is true

g. Suppose $p - q < 2Bn^{1/4}$ where B is an integer that is very small relative to n. We want to show that $x - \lceil(\sqrt{n})\rceil + 1 < \frac{B^2}{2} + 1$. Subtracting 1 from both sides we get $x - \lceil(\sqrt{n})\rceil < \frac{B^2}{2}$. From part f we know $(x - \lceil(\sqrt{n})\rceil) < \frac{y^2}{(2\sqrt{n})}$. So

$$\begin{aligned}
(x - \lceil(\sqrt{n})\rceil) &< \frac{y^2}{(2\sqrt{n})} \\
&= \frac{((p-q)/2)^2}{(2\sqrt{n})} \\
&= \frac{((p-q)^2/4)}{(2\sqrt{n})} \\
&= \frac{(p-q)^2}{4(2\sqrt{n})} \\
&< \frac{(2Bn^{1/4})^2}{4(2\sqrt{n})} \\
&= \frac{4B^2\sqrt{n}}{4 * 2 * \sqrt{n}} \\
&= \frac{B^2}{2}
\end{aligned}$$

Thus this upper bound is true that is $x - \lceil(\sqrt{n})\rceil + 1 < \frac{B^2}{2} + 1$.

Problem 4 — El Gamal is not semantically secure (12 marks)

Let M_1 and M_2 are plain texts such that $M_1 \in QR_p$ and $M-2 \in QN_p$. Let $C = (C_1, C_2)$ be an encryption of M_1 or M_2. We would prove that the attack correctly identifies the encrypted plain text. So we know that $M_1^{(p-1)/2} = 1 \mod p$ and $M_2^{(p-1)/2} = -1 \mod p$. Now we would prove all the assertions individually.
Note: Since $k \in \mathbb{Z}_{p-1}$, we know that k is odd.

Case 1: in this case- $\left(\frac{y}{p}\right) = 1$ and $\left(\frac{C_2}{p}\right) = 1$. So this follows that $y^{(p-1)/2} = 1$ and $C_2^{(p-1)/2} = 1$. So we can do the following:

$$\begin{aligned} y &= g^x \mod p \\ y^{(p-1)/2} &= (g^x)^{(p-1)/2} \mod p \\ &= 1 \mod p \end{aligned}$$

Similarly we can calculate for C_2:

$$\begin{aligned} C_2 &= My^k \mod p \\ C_2^{(p-1)/2} &= (My^k)^{(p-1)/2} \mod p \\ &= (M)^{(p-1)/2} * (y^k)^{(p-1)/2} \mod p \\ &= (M)^{(p-1)/2} * (g^{xk})^{(p-1)/2} \mod p \\ &= (M)^{(p-1)/2} * (g^{x(p-1)/2})^k \mod p \\ &= 1 * (g^{x(p-1)/2})^k \mod p \\ &= 1 * y^{(p-1)/2} \mod P \\ &= 1 \mod p \end{aligned}$$

Thus the attacker can correctly identify in this case as $(M)^{(p-1)/2}$ has to be 1 so the attacker can say $M = M_1$ as $M_1 \in QR_p$.

Case 2: in this case- $\left(\frac{y}{p}\right) = 1$ and $\left(\frac{C_2}{p}\right) = -1$. So this follows that $y^{(p-1)/2} = 1$ and $C_2^{(p-1)/2} = -1$. So we can do the following:

$$\begin{aligned} y &= g^x \mod p \\ y^{(p-1)/2} &= (g^x)^{(p-1)/2} \mod p \\ &= 1 \mod p \end{aligned}$$

Similarly we can calculate for C_2:

$$\begin{aligned}
C_2 &= My^k \mod p \\
C_2^{(p-1)/2} &= (My^k)^{(p-1)/2} \mod p \\
&= (M)^{(p-1)/2} * (y^k)^{(p-1)/2} \mod p \\
&= (M)^{(p-1)/2} * (g^{xk})^{(p-1)/2} \mod p \\
&= (M^{(p-1)/2}) * (g^{x(p-1)/2})^k \mod p \\
&= -1 * (g^{x(p-1)/2})^k \mod p \\
&= -1 * y^{(p-1)/2k} \mod P \\
&= -1 * 1^k \mod p = -1 \mod p
\end{aligned}$$

Thus the attacker can correctly identify in this case as $(M)^{(p-1)/2}$ has to be -1 so the attacker can say $M = M_2$ as $M_2 \in QN_p$.

Case 3: Suppose $\left(\frac{y}{p}\right) = -1$, $\left(\frac{C_1}{p}\right) = 1$ and $\left(\frac{C_2}{p}\right) = 1$. this follows that $y^{(p-1)/2} = -1$, $C_1^{(p-1)/2} = 1$ and $C_2^{(p-1)/2} = 1$. So we can do the following:

$$\begin{aligned}
y &= g^x \mod p \\
y^{(p-1)/2} &= (g^x)^{(p-1)/2} \mod p \\
&= -1 \mod p
\end{aligned}$$

$$\begin{aligned}
C_1 &= g^k \mod p \\
C_1^{(p-1)/2} &= (g^k)^{(p-1)/2} \mod p \\
&= 1 \mod p
\end{aligned}$$

$$\begin{aligned}
C_2 &= My^k \mod p \\
C_2^{(p-1)/2} &= (My^k)^{(p-1)/2} \mod p \\
&= (M)^{(p-1)/2} * (y^k)^{(p-1)/2} \mod p \\
&= (M)^{(p-1)/2} * (g^{xk})^{(p-1)/2} \mod p \\
&= (M^{(p-1)/2}) * (g^{x(p-1)/2})^k \mod p \\
&= 1 * (g^{k(p-1)/2})^x \mod p \\
&= 1 * C_1^{(p-1)/2k} \mod P \\
&= 1 * 1^k \mod p = 1 \mod p
\end{aligned}$$

Thus the attacker can correctly identify in this case as $(M)^{(p-1)/2}$ has to be 1. So the attacker can say $M = M_1$ as $M_1 \in QR_p$.

Case 4: Suppose $\left(\frac{y}{p}\right) = -1$, $\left(\frac{C_1}{p}\right) = 1$ and $\left(\frac{C_2}{p}\right) = -1$. this follows that $y^{(p-1)/2} = -1$, $C_1^{(p-1)/2} = 1$ and $C_2^{(p-1)/2} = -1$. So we can do the following:

$$\begin{aligned}
y &= g^x \mod p \\
y^{(p-1)/2} &= (g^x)^{(p-1)/2} \mod p \\
&= -1 \mod p
\end{aligned}$$

$$
\begin{aligned}
C_1 &= g^k \mod p \\
C_1^{(p-1)/2} &= (g^k)^{(p-1)/2} \mod p \\
&= 1 \mod p
\end{aligned}
$$

$$
\begin{aligned}
C_2 &= My^k \mod p \\
C_2^{(p-1)/2} &= (My^k)^{(p-1)/2} \mod p \\
&= (M)^{(p-1)/2} * (y^k)^{(p-1)/2} \mod p \\
&= (M)^{(p-1)/2} * (g^{xk})^{(p-1)/2} \mod p \\
&= (M^{(p-1)/2}) * (g^{x(p-1)/2})^k \mod p \\
&= -1 * (g^{k(p-1)/2})^x \mod p \\
&= -1 * C_1^{(p-1)/2k} \mod P \\
&= -1 * 1^k \mod p = -1 \mod p
\end{aligned}
$$

Thus the attacker can correctly identify in this case as $(M)^{(p-1)/2}$ has to be -1. So the attacker can say $M = M_2$ as $M_2 \in QN_p$.

Case 5: Suppose $\left(\frac{y}{p}\right) = -1$, $\left(\frac{C_1}{p}\right) = -1$ and $\left(\frac{C_2}{p}\right) = 1$. this follows that $y^{(p-1)/2} = -1$, $C_1^{(p-1)/2} = -1$ and $C_2^{(p-1)/2} = 1$. So we can do the following:

$$
\begin{aligned}
y &= g^x \mod p \\
y^{(p-1)/2} &= (g^x)^{(p-1)/2} \mod p \\
&= -1 \mod p
\end{aligned}
$$

$$
\begin{aligned}
C_1 &= g^k \mod p \\
C_1^{(p-1)/2} &= (g^k)^{(p-1)/2} \mod p \\
&= -1 \mod p
\end{aligned}
$$

$$
\begin{aligned}
C_2 &= My^k \mod p \\
C_2^{(p-1)/2} &= (My^k)^{(p-1)/2} \mod p \\
&= (M)^{(p-1)/2} * (y^k)^{(p-1)/2} \mod p \\
&= (M)^{(p-1)/2} * (g^{xk})^{(p-1)/2} \mod p \\
&= (M^{(p-1)/2}) * (g^{x(p-1)/2})^k \mod p \\
&= -1 * (g^{k(p-1)/2})^x \mod p \\
&= -1 * C_1^{(p-1)/2k} \mod P \\
&= -1 * (-1)^k \mod p = 1 \mod p
\end{aligned}
$$

Since k is odd, $(-1)^k = -1$. Thus the attacker can correctly identify in this case as $(M)^{(p-1)/2}$ has to be -1. So the attacker can say $M = M_2$ as $M_2 \in QN_p$.

Case 6: Suppose $\left(\frac{y}{p}\right) = -1$, $\left(\frac{C_1}{p}\right) = -1$ and $\left(\frac{C_2}{p}\right) = -1$. this follows that $y^{(p-1)/2} = -1$, $C_1^{(p-1)/2} = -1$ and $C_2^{(p-1)/2} = -1$. So we can do the following:

$$\begin{aligned} y &= g^x \mod p \\ y^{(p-1)/2} &= (g^x)^{(p-1)/2} \mod p \\ &= -1 \mod p \end{aligned}$$

$$\begin{aligned} C_1 &= g^k \mod p \\ C_1^{(p-1)/2} &= (g^k)^{(p-1)/2} \mod p \\ &= -1 \mod p \end{aligned}$$

$$\begin{aligned} C_2 &= My^k \mod p \\ C_2^{(p-1)/2} &= (My^k)^{(p-1)/2} \mod p \\ &= (M)^{(p-1)/2} * (y^k)^{(p-1)/2} \mod p \\ &= (M)^{(p-1)/2} * (g^{xk})^{(p-1)/2} \mod p \\ &= (M^{(p-1)/2}) * (g^{x(p-1)/2})^k \mod p \\ &= 1 * (g^{k(p-1)/2})^x \mod p \\ &= 1 * C_1^{(p-1)/2k} \mod P \\ &= 1 * (-1)^k \mod p = -1 \mod p \end{aligned}$$

Since k is odd, $(-1)^k = -1$. Thus the attacker can correctly identify in this case as $(M)^{(p-1)/2}$ has to be 1. So the attacker can say $M = M_1$ as $M_1 \in QR_p$.

Since in all the cases the assertions are correct, the El Gamal system is not semantically secure.

Problem 5 — An IND-CPA, but not IND-CCA secure version of RSA (12 marks)

Suppose M_1 and M_2 are plain texts. Mallory gets $C = (s||t) = (r^e \mod n||H(r) \oplus M_i)$ where i is 1 or 2.
She can trace through the decryption of C:
First it would separate s and t.
then the following would be done:

$$\begin{aligned} M &= H(s^d \mod n) \oplus t \\ &= H((r^e)^d \mod n) \oplus t \\ &= H((r^e)^d \mod n) \oplus H(r) \oplus M_i \end{aligned}$$

Since Mallory know m and since $|t| = m$, Mallory is able to separate s and t from C as they are just concatenations. So, Mallory can choose $C' = C \oplus 0^s||M_1 = s||t \oplus M_1$. So the decryption would give:

$$\begin{aligned} M &= C'^d \\ &= H((r^e)^d \mod n) \oplus H(r) \oplus M_i \oplus M_1 \\ &= H(r \mod n) \oplus H(r) \oplus M_i \oplus M_1 \\ &= H(r) \oplus H(r) \oplus M_i \oplus M_1 \\ &= M_i \oplus M_1 \end{aligned}$$

Now she can know whether $M_i = M_1$ or $M_i = M_2$. This is because when if $M_i = M_1$, $C'^d = 0$ otherwise it would result in something else. So if she sees 0, she can conclude it is M_1, otherwise M_2.