CPSC 418 / MATH 318 — Introduction to Cryptography
ASSIGNMENT 3

Name: Daniel Heyns (Crypto Wizard)
Student ID: 30021292

Problem 1 — Flawed MAC designs (11 marks)

a.
$$PHMAC_K(M_2) := ITHash(K||M_2) = ITHash(K||M_1||X)$$

We know $ITHash(K||M_1)$ and because $ITHash$ is iterative, we can "pick-up" where we "left-off" in the hash algorithm. This is done by preforming $ITHash$, but in step 1... $H = PHMAC_K(M_1)$ and the Input is simply X. The function f is public so this can be done manually by the attacker.

b. So if we run through $ITHash$ with the message $M1$,

$$\begin{aligned} H_1 &= f(0^n, P_1) \\ H_2 &= f(H_1, P_2) \\ &... \\ H_L &= f(H_L, P_L) = ITHash(M_1) \\ H_{L+1} &= f(H_{L+1}, K) = AHMAC_K(M_1) \qquad (1) \end{aligned}$$

Because $ITHash$ is not weak collision resistant and because we know M_1, we can find an M_2 that results in $ITHash(M2) = ITHash(M_1)$ where $M_1 \neq M_2$. Because $ITHash(M2) = ITHash(M_1)$, H_{L+1} in (1) will be the same for both M_1 and M_2 and thus, $AHMAC_K(M_1) = AHMAC_K(M_2)$. So we have found a new message/$AHMAC$ pair.

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

Let

$$\begin{aligned} M_q &\equiv C^{d_q}(mod\, q) \\ &\equiv C^{d+t\phi(q)}(mod\, q) \quad \text{For some } t \,\epsilon\, \mathbb{Z} \\ &\equiv C^d(C^{\phi(q)})^t(mod\, q) \\ &\equiv C^d(1)^t(mod\, q) \quad \text{Euler's Theorem, gcd}(C,q) = 1 \\ &\equiv C^d(mod\, q) \end{aligned}$$

$$\begin{aligned} M_p &\equiv C^{d_p}(mod\, p) \\ &\equiv C^{d+t\phi(p)}(mod\, p) \quad \text{For some } t \,\epsilon\, \mathbb{Z} \\ &\equiv C^d(C^{\phi(p)})^t(mod\, p) \\ &\equiv C^d(1)^t(mod\, p) \quad \text{Euler's Theorem, gcd}(C,q) = 1 \\ &\equiv C^d(mod\, p) \end{aligned}$$

Now we take all modular equivalencies and transform them into regular equations by adding a multiple of the modulus'd number in the form $k_1, k_2, k_3 \,\epsilon\, \mathbb{Z}$,

$$\begin{aligned} M_p &= C^d + k_1 p \\ M_q &= C^d + k_2 q \\ M &= pxM_q + qyM_p + k_3 n \end{aligned}$$

So,

$$\begin{aligned} M^{'} &= pxM_q + qyM_p + k_3 n \\ M^{'} &= px(C^d + k_2 p) + qy(C^d + k_1 p) + k_3 n \\ &= pxC^d + pxk_2 q + qyC^d + qyk_1 p + k_3 n \\ &= pxC^d + qyC^d + pxk_2 q + qyk_1 p + k_3 n \\ &= C^d(px + qy) + pq(xk_2 + yk_1) + k_3 n \\ &= C^d + n(xk_2 + yk_1) + k_3 n \\ &= C^d + n(k_2 x + k_1 y + k_3) \equiv C^d \equiv M(mod\, n) \end{aligned}$$

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

a. Let $x, y \in \mathbb{Z}$ and $x > y > 0$.

And $n = x^2 - y^2$ and $n = pq$ where $p > q$.

So,

$$\begin{aligned} n &= x^2 - y^2 \\ &= (x+y)(x-y) \end{aligned}$$

We see n is a product of the two numbers, i.e. n's factors.
Factors of n are $\{1, q, p, n\}$, so we have two cases.

<u>Case 1</u>
Let,

$$\begin{aligned} 1 &= x - y \\ x &= y + 1 \end{aligned}$$

Now,

$$\begin{aligned} n &= x^2 - y^2 \\ y^2 &= x^2 - n \\ y^2 &= (y+1)^2 - n \\ y^2 &= y^2 + 2y + 1 - n \\ y &= \frac{n-1}{2} \end{aligned}$$

Let,

$$\begin{aligned} n &= x + y \\ y &= n - x \end{aligned}$$

Now,

$$\begin{aligned} n &= x^2 - y^2 \\ x^2 &= n + y^2 \\ x^2 &= n + (n-x)^2 \\ x^2 &= n + n^2 - 2nx + x^2 \\ x &= \frac{n+1}{2} \end{aligned}$$

<u>Case 2</u>
Let,

$$\begin{aligned} q &= x - y \\ x &= q + y \end{aligned}$$

Now,

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

Let,

$$
\begin{aligned}
n &= x + y \\
y &= p - x
\end{aligned}
$$

Now,

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

Given the two cases we see that no matter what, the only outcomes we get are the given x and y values.

b. p, q are odd primes, therefore

$$p > q > 2$$

So,

$$
\begin{aligned}
pq &> 2p \\
n &> p + p \\
n + 1 &> p + p + 1 \quad (1)
\end{aligned}
$$

And,

$$
\begin{aligned}
p &> q \\
p + p &> p + q \\
p + p + 1 &> p + q \quad (2)
\end{aligned}
$$

Now we put (1) and (2) together...

$$n + 1 > p + p + 1 > p + q$$

So,

$$n + 1 > p + q$$

c. Let,

$$
\begin{aligned}
q &< p \\
p+q &< p+p \\
p+q &< 2p \\
dfracp+q2 &< p \qquad (3)
\end{aligned}
$$

And,

$$
\begin{aligned}
p &> q \\
p-q &> 0 \\
p^2-2pq+q^2 &> 0 \qquad \text{(square both sides)} \\
p^2+q^2 &> 2pq \\
p^2+q^2 &> 2n \\
p^2+q^2+2n &> 4n \\
p^2+2pq+q^2 &> 4n \\
p+q &> 2\sqrt{n} \qquad \text{(root both sides)} \\
\frac{p+q}{2} &> \sqrt{n} \qquad (4)
\end{aligned}
$$

Combine (3) and (4)

$$\sqrt{n} < \frac{p+q}{2} < p$$

d. Let,

$$x = \frac{p+q}{2}$$

then,

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

$p > q > 2$ and p and q are both odd.
Therefore,

$$
\begin{aligned}
p &= 2r+1 \\
q &= 2i+1 \qquad \text{where } r > i > 0 \text{ and } r, i \,\epsilon\, \mathbb{Z}
\end{aligned}
$$

Now,

$$y = \frac{2r+1-2i-1}{2} = \frac{2r-2i}{2} = r-i$$

Because $r > i$ and $r, i \in \mathbb{Z}$, $y \in \mathbb{Z}$.The "while" condition is satisfied.

Suppose there exists $a \in \mathbb{Z}$, $\lceil \sqrt{n} \rceil < a < \frac{p+q}{2}$ such that $y = \sqrt{a^2-n}$ is an integer.
So,

$$\begin{aligned} y &= \sqrt{a^2-n} \\ y^2 &= a^2-n \\ n &= a^2-y^2 \quad , \quad n = x^2-y^2 \\ a &= x = \frac{p+q}{2} \end{aligned}$$

But $a < \frac{p+q}{2}$ contradiction!

Finally,

$$x = \frac{p+q}{2} \text{ and } y = \frac{p-q}{2}$$

$$x-y = \frac{p+q}{2} - \frac{p-q}{2} = \frac{p+q-p+q}{2} = \frac{2q}{2} = q$$

e. While conditions ends when $x = \frac{p+q}{2}$ and the initial value of x, $x_0 = \lceil \sqrt{n} \rceil$ and x is incremented each loop by one. Therefore $\frac{p+q}{2} - x_0$ will give the number of cycles the loop runs before x reaches $\frac{p+q}{2}$, but the while condition will be checked an additional time when $x = \frac{p+q}{2}$ and will be rejected. Therefore the while loop condition will be tested $\frac{p+q}{2} - x_0 + 1 = x - \lceil \sqrt{n} \rceil + 1$

f. Start with,

$$x^2 - n = y^2$$

divide both sides by $x + \sqrt{n}$

$$x - \sqrt{n} = \frac{y^2}{x+\sqrt{n}} \qquad (5)$$

Now,

$$x = \frac{p+q}{2} \text{ and } \frac{p+q}{2} > \sqrt{n} \qquad \text{from (c)}$$

Therefore,

$$\frac{p+q}{2} + \sqrt{n} > \sqrt{n} + \sqrt{n}$$

So from (5),

$$x - \sqrt{n} < \frac{y^2}{2\sqrt{n}}$$

The above can be inferred because the denominator on the right side is now less than it was when these two expressions were equal. We can also ceiling the $\sqrt{n}$ as the would only ever increase a negative number on the lesser side, thus this inequality will remain true.

$$x - \lceil \sqrt{n} \rceil < \frac{y^2}{2\sqrt{n}}$$

g. Let,

$$\begin{aligned}
p - q &< 2B\sqrt[4]{n} \\
p^2 - 2pq + q^2 &< 4B^2\sqrt{n} \\
p^2 + 2pq + q &< 4B^2\sqrt{n} + 4n \\
\frac{p^2 + 2pq + q}{4} &< B^2\sqrt{n} + n \\
x^2 &< B^2\sqrt{n} + n \\
x^2 - n &< B^2\sqrt{n} \\
y^2 &< B^2\sqrt{n} \\
\frac{y^2}{\sqrt{n}} &< B^2 \\
\frac{y^2}{2\sqrt{n}} &< \frac{B^2}{2\sqrt{n}} \\
\frac{y^2}{2\sqrt{n}} + 1 &< \frac{B^2}{2} + 1
\end{aligned}$$

From (f),

$$x - \lceil \sqrt{n} \rceil + 1 < \frac{y^2}{2\sqrt{n}} + 1 < \frac{B^2}{2} + 1$$

Therefore,

$$x - \lceil \sqrt{n} \rceil + 1 < \frac{B^2}{2} + 1$$

From (e),

$x - \lceil \sqrt{n} \rceil + 1$ is the number of steps before the algorithm factors n.

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

Let,

$$
\begin{aligned}
y &\equiv g^x (mod\, p), &(1)\\
C_1 &\equiv g^k (mod\, p) &(2)\\
C_2 &\equiv M y^k \; mod\, p) &(3)\\
g^{2i} &\,\epsilon\, QR_p &(4)\\
g^{2i+1} &\,\epsilon\, QN_p &(5)
\end{aligned}
$$

We now go through assertions in step 3.

<u>Assertion 1</u>
So,

$$\left(\frac{y}{p}\right) = 1, \qquad \left(\frac{C_2}{p}\right) = 1$$

From (3),

$$
\begin{aligned}
\left(\frac{C_2}{p}\right) &= \left(\frac{M}{p}\right)\left(\frac{y}{p}\right)^k \\
1 &= \left(\frac{M}{p}\right)(1)^k = \left(\frac{M}{p}\right)
\end{aligned}
$$

Therefore $M \,\epsilon\, QR_p$, i = 1.
<u>Assertion 2</u>
So,

$$\left(\frac{y}{p}\right) = 1, \qquad \left(\frac{C_2}{p}\right) = -1$$

From (3),

$$
\begin{aligned}
\left(\frac{C_2}{p}\right) &= \left(\frac{M}{p}\right)\left(\frac{y}{p}\right)^k \\
-1 &= \left(\frac{M}{p}\right)(1)^k = \left(\frac{M}{p}\right)
\end{aligned}
$$

Therefore $M \,\epsilon\, QN_p$, i = 2.
<u>Assertion 3</u>
So,

$$\left(\frac{y}{p}\right) = -1, \qquad \left(\frac{C_1}{p}\right) = 1, \qquad \left(\frac{C_2}{p}\right) = 1$$

From (3),

$$
\begin{aligned}
\left(\frac{C_2}{p}\right) &= \left(\frac{M}{p}\right)\left(\frac{y}{p}\right)^k \\
1 &= \left(\frac{M}{p}\right)(-1)^k \qquad \text{from (4) and (5)}, \frac{g^k}{p} = 1, \quad k = 2i \\
1 &= \left(\frac{M}{p}\right)\left((-1)^2\right)^i = \left(\frac{M}{p}\right)(1)^i = \left(\frac{M}{p}\right)
\end{aligned}
$$

Therefore $M \epsilon QR_p$, i = 1.
<u>Assertion 4</u>
So,

$$\left(\frac{y}{p}\right) = -1, \qquad \left(\frac{C_1}{p}\right) = 1, \qquad \left(\frac{C_2}{p}\right) = -1$$

From (3),

$$\begin{aligned} \left(\frac{C_2}{p}\right) &= \left(\frac{M}{p}\right)\left(\frac{y}{p}\right)^k \\ -1 &= \left(\frac{M}{p}\right)(-1)^k \qquad \text{from (4) and (5), } \frac{g^k}{p} = 1, \quad k = 2i \\ -1 &= \left(\frac{M}{p}\right)\left((-1)^2\right)^i = \left(\frac{M}{p}\right)(1)^i = \left(\frac{M}{p}\right) \end{aligned}$$

Therefore $M \epsilon QN_p$, i = 2.
<u>Assertion 5</u>
So,

$$\left(\frac{y}{p}\right) = -1, \qquad \left(\frac{C_1}{p}\right) = -1, \qquad \left(\frac{C_2}{p}\right) = 1$$

From (3),

$$\begin{aligned} \left(\frac{C_2}{p}\right) &= \left(\frac{M}{p}\right)\left(\frac{y}{p}\right)^k \\ 1 &= \left(\frac{M}{p}\right)(-1)^k \qquad \text{from (4) and (5), } \frac{g^k}{p} = -1, \quad k = 2i+1 \\ 1 &= \left(\frac{M}{p}\right)\left((-1)^2\right)^i(-1) = \left(\frac{M}{p}\right)(1)^i(-1) = -\left(\frac{M}{p}\right) \end{aligned}$$

Therefore $M \epsilon QN_p$, i = 2.
<u>Assertion 6</u>
So,

$$\left(\frac{y}{p}\right) = -1, \qquad \left(\frac{C_1}{p}\right) = -1, \qquad \left(\frac{C_2}{p}\right) = -1$$

From (3),

$$\begin{aligned} \left(\frac{C_2}{p}\right) &= \left(\frac{M}{p}\right)\left(\frac{y}{p}\right)^k \\ -1 &= \left(\frac{M}{p}\right)(-1)^k \qquad \text{from (4) and (5), } \frac{g^k}{p} = -1, \quad k = 2i+1 \\ -1 &= \left(\frac{M}{p}\right)\left((-1)^2\right)^i(-1) = \left(\frac{M}{p}\right)(1)^i(-1) = -\left(\frac{M}{p}\right) \end{aligned}$$

Therefore $M \epsilon QR_p$, i = 1.

We see that all of Mallory's assertions are correct. Therefore, with cyphertext, information can be found that could not be found without. Not semantically secure.

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

Let,

$$C = (s||t) = (r^e(mod\, n)||H(r) \oplus M_i) \text{ where } i = 1 \text{ or } 2$$

Mallory chooses M_1 and M_2 where $M_1, M_2 \neq 0$.

$$\begin{aligned} C^{'} &= (s||t \oplus M_1) \\ &= (s||H(r) \oplus M_i \oplus M_1) \end{aligned}$$

Now,

$$H(r) \oplus M_i \oplus M_1 \neq H(r) \oplus M_i \qquad \text{As } M_1 \neq 0$$

So,

$$C^{'} = (s||t \oplus M_1)$$

Now we decrypt:

$$\begin{aligned} s_0 &= s \\ t_0 &= t \oplus M_1 \\ M^{'} &= H(s^d(mod\, n)) \oplus H(r) \oplus M_i \oplus M_1 \\ M_i &= H(s^d(mod\, n)) \oplus H(r) \oplus M_i \end{aligned}$$

Therefore we can do,

$$M^{'} \oplus M_1 = M_i$$

We obtain M_i to be compared to M_1 and M_2, giving us what i is.