CPSC 418 / MATH 318 — Introduction to Cryptography
ASSIGNMENT 3

Name: Harjee Johal
Student ID: 30000668

Problem 1 — Flawed MAC designs, 13 marks

(a) The message M_2 is of the form $M_2 = M_1||X$, where X is an arbitrary n-bit block. From the question description we also know that $M_1 = P_1||P_2||\ldots||P_L$, where $P_1, P_2, \ldots, P_L$ are each n-bit blocks.

(b)

Problem 2 — Fast RSA decryption using Chinese remaindering, 8 marks)

We are told that $d_p \equiv d \mod p-1$. This means that d_p can be written in the form: $d_p = d + j(p-1)$, where j is an integer. We are also told that $d_q \equiv d \mod q-1$. This means that d_q can be written in the form: $d_q = d + k(q-1)$, where k is an integer.

Next, we are told that $M_p \equiv C^{d_p} \mod p$. Since we know that $d_p = d + j(p-1)$, that means that we can re-write this as: $M_p \equiv C^{d+j(p-1)} \mod p$. We can manipulate this using power rules to obtain:

$$\begin{aligned} & C^{d+j(p-1)} && \mod p \\ \equiv & C^d C^{j(p-1)} && \mod p \\ \equiv & C^d (C^{p-1})^j && \mod p \end{aligned}$$

Since p is a prime, that means that $\phi(p) = p-1$. Furthermore, since we're told that $gcd(n, C) = 1$, that means that C and n share no prime factors. Since n's prime factors are p and q, that means that $gcd(p, C)$ and $gcd(q, C)$ must also be 1. Since $\phi(p) = p-1$ and $gcd(p, C) = 1$, we can apply Euler's theorem on C^{p-1}, meaning that $C^{p-1} \equiv 1 \mod p$. Using this, we can further simplify M_p:

$$\begin{aligned} & C^d (C^{p-1})^j && \mod p \\ \equiv & C^d (1)^j && \mod p \\ \equiv & C^d (1) && \mod p \\ \equiv & C^d && \mod p \end{aligned}$$

Thus, we can see that $M_p \equiv C^d \mod p$. That means that $M_p = C^d + sp$, where s is an integer.

Furthermore, we are told that $M_q \equiv C^{d_q} \mod q$. Since we know that $d_q = d + k(q-1)$, that means that we can re-write this as: $M_q \equiv C^{d+k(q-1)} \mod q$. We can manipulate this using power rules to obtain:

$$\begin{aligned} & C^{d+k(q-1)} && \mod q \\ \equiv & C^d C^{k(q-1)} && \mod q \\ \equiv & C^d (C^{q-1})^k && \mod q \end{aligned}$$

Since q is a prime, that means that $\phi(q) = q-1$. Earlier, we demonstrated that since $gcd(n, C) = 1$, then $gcd(q, C)$ must also equal 1. Since $\phi(q) = q-1$ and $gcd(q, C) = 1$, we can apply Euler's theorem on C^{q-1}, meaning that $C^{q-1} \equiv 1 \mod q$. Using this, we can further simplify M_q:

$$
\begin{aligned}
& C^d(C^{q-1})^k \mod q \\
\equiv & C^d(1)^k \mod q \\
\equiv & C^d(1) \mod q \\
\equiv & C^d \mod q
\end{aligned}
$$

Thus, we can see that $M_q \equiv C^d \mod q$. That means that $M_q = C^d + tq$, where t is an integer.

Lastly, we are told that $M \equiv pxM_q + qyM_p \mod n$. We can substitute M_p with $C^d + sp$ and M_q with $C^d + tq$ to obtain:

$$
\begin{aligned}
M &\equiv pxM_q + qyM_p \mod n \\
&\equiv px(C^d + tq) + qy(C^d + sp) \mod n \\
&\equiv pxC^d + pqtx + qyC^d + pqsy \mod n \\
&\equiv C^d(px + qy) + pq(tx + sy) \mod n
\end{aligned}
$$

Where $tx + sy$ is an integer. We know that $n = pq$, and from step 3 of the algorithm we know that $px + qy = 1$. Using this information, we obtain:

$$
\begin{aligned}
M &\equiv C^d(px + qy) + pq(tx + sy) \mod n \\
&\equiv C^d + n(tx + sy) \mod n \\
&\equiv C^d \mod n
\end{aligned}
$$

We can remove $n(tx + sy)$ from the expression since it's a multiple of n, and the modular arithmetic is being done modulus n. Therefore, we obtain $M \equiv C^d \mod n \equiv M^{ed} \mod n$. In RSA, integers e and d are determined so that $ed \equiv 1 \mod n$. Therefore, that means that $M \equiv M^{ed} \mod n \equiv M^1 \mod n \equiv M \mod n$. Therefore, the M obtained using this method of decryption is the same as the M determined during "normal" RSA decryption.

Problem 3 — RSA primes too close together, 18 marks)

(a) We are told that $y > 0$. We are also told that $x + y = p$. This means that $y = p - x$. Since $y > 0$, then that means that $p - x > 0$ as well. Since $p - x > 0$, then $p > x$.

We are told that $n = x^2 - y^2$. This means that $y^2 = x^2 - n$. Since $y > 0$, that means that $y^2 > 0$. Since $y^2 = x^2 - n$, and $y^2 > 0$, then that means $x^2 - n > 0$ as well. If $x^2 - n > 0$, then $x^2 > n$, which means that $x > \sqrt{n}$.

From this, we can see that $p > x$ and that $x > \sqrt{n}$. Thus, we can see that $p > x > \sqrt{n}$.

(b) We're told that in the Fermat factorization algorithm there is a *while* loop that computes both $a = a + 1$ and $b = \sqrt{a^2 - n}$. This loop continues while the computed value of b isn't an integer.

We know that $n = x^2 - y^2$. Therefore, we can re-write this equation as: $b = \sqrt{a^2 - (x^2 - y^2)}$. When $a = x$, then we get:

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

Thus, when $a = x$, then $b = y$. Since by definition y is an integer, that means that the *while* loop will terminate when $a = x$.

We're also told that the algorithm outputs $a - b$ once it's completed. Since the *while* loop terminates when $a = x$, and $b = y$ when $a = x$, then that means $a - b = x - y$. By definition, $q = x - y$, meaning that when this algorithm terminates, it outputs q.

We can also show that the *while* loop won't terminate for a value of a less than x using a proof by contradiction. Suppose that the loop does terminate for some integer $a < x$. Then that means that for that value of a, we get $b = \sqrt{a^2 - n}$, where b is an integer. We can re-arrange the equation $b = \sqrt{a^2 - n}$ to obtain:

$$\begin{aligned} b &= \sqrt{a^2 - n} \\ b^2 &= a^2 - n \\ n &= a^2 - b^2 \\ n &= (a + b)(a - b) \end{aligned}$$

From this, we can see that $n = (a + b)(a - b)$. Since $n = pq$ and $n > p > q > 0$, then that means $p = a + b$ and $q = a - b$. From these two equations, we can see that $a = \frac{p+q}{2}$. By definition, $x = \frac{p+q}{2}$. Therefore, that would mean that $a = x$. However, we defined a such that $a < x$. This is a contradiction. Therefore, this shows that the loop does not terminate for any value of $a < x$.

(c) The value of a is initialized as $a = \lceil\sqrt{n}\rceil$. During the first iteration of the loop, the algorithm first performs $a = a + 1$, and then computes $b = \sqrt{a^2 - n}$. It continues to do this until it finally reaches $a = x$. This means that the first iteration of the loop is performed with $a = \lceil\sqrt{n}\rceil + 1$, and the last iteration of the loop is done with $a = x$. The number of iterations between the first and last values of a is thus $x - \lceil\sqrt{n}\rceil$. The last iteration of the loop is after $a = x$. The condition at the top of the *while* loop is checked one last time. Since b is an integer when $a = x$, that means that the condition at the top of the *while* loop will not be satisfied on the last iteration, meaning that the *while* loop will be skipped. However, this iteration is still counted. Therefore, there are $x - \lceil\sqrt{n}\rceil$ iterations where the loop is entered, and 1 iteration where the loop is not entered. Therefore, there are $x - \lceil\sqrt{n}\rceil + 1$ iterations overall.

(d) We are asked to prove that $x - \lceil\sqrt{n}\rceil < \frac{y^2}{2\sqrt{n}}$. We know that $n = x^2 - y^2$. We can rearrange this to get $y^2 = x^2 - n = (x + \sqrt{n})(x - \sqrt{n})$. We can re-arrange this equation to get: $(x - \sqrt{n}) = \frac{y^2}{x+\sqrt{n}}$.

In part (a), we showed that $x > \sqrt{n}$. From this, we can see that $x + \sqrt{n} > 2\sqrt{n}$. Since $2\sqrt{n} < x + \sqrt{n}$, that means that $\frac{y^2}{2\sqrt{n}} > \frac{y^2}{x+\sqrt{n}}$. Since $(x - \sqrt{n}) = \frac{y^2}{x+\sqrt{n}}$, that means that $(x - \sqrt{n}) < \frac{y^2}{2\sqrt{n}}$.

By definition, $\lceil\sqrt{n}\rceil \geq \sqrt{n}$. Since $\lceil\sqrt{n}\rceil \geq \sqrt{n}$, then that means $x - \sqrt{n} \geq x - \lceil\sqrt{n}\rceil$. We can use this to show that since $(x - \sqrt{n}) < \frac{y^2}{2\sqrt{n}}$, that means $(x - \lceil\sqrt{n}\rceil) < \frac{y^2}{2\sqrt{n}}$. Thus, we have proven that $x - \lceil\sqrt{n}\rceil < \frac{y^2}{2\sqrt{n}}$.

(e) Suppose that $p - q < 2B\sqrt[4]{n}$. We can re-arrange this to obtain:

$$\begin{aligned}
\frac{p-q}{2} &< B\sqrt[4]{n} \\
y &< B\sqrt[4]{n} \qquad (y = \frac{p-q}{2}) \\
y^2 &< B^2\sqrt{n} \\
\frac{y^2}{\sqrt{n}} &< B^2 \\
\frac{y^2}{2\sqrt{n}} &< \frac{B^2}{2}
\end{aligned}$$

Thus, we can see that $\frac{y^2}{2\sqrt{n}} < \frac{B^2}{2}$. In part (d), we showed that $x - \lceil\sqrt{n}\rceil < \frac{y^2}{2\sqrt{n}}$. Using this statement, we can see that $x - \lceil\sqrt{n}\rceil < \frac{B^2}{2}$. Since $x - \lceil\sqrt{n}\rceil < \frac{B^2}{2}$, then that means that $x - \lceil\sqrt{n}\rceil + 1 < \frac{B^2}{2} + 1$. We showed in part (c) that the number of loops iterations performed by Fermat's Factorization algorithm to factor n is also $x - \lceil\sqrt{n}\rceil + 1$. Therefore, we can see that algorithm factors n after at most $\frac{B^2}{2} + 1$ iterations.

Problem 4 – The El Gamal public key cryptosystem is not semantically secure, 12 marks

We are asked to prove that El Gamal is not semantically secure. We do this by proving 6 assertions. The assertions are as follows:

Assertion 1: If $\left(\frac{y}{p}\right) = 1$ and $\left(\frac{C_2}{p}\right) = 1$, then $C = E(M_1)$:

Since $C_2 \equiv My^k \mod p$, this implies that $\left(\frac{C_2}{p}\right) = \left(\frac{My^k}{p}\right) = \left(\frac{M}{p}\right)\left(\frac{y}{p}\right)^k$. Since $\left(\frac{y}{p}\right) = 1$ and $\left(\frac{C_2}{p}\right) = 1$, we can substitute them into the equation to get: $1 = \left(\frac{M}{p}\right)(1)^k = \left(\frac{M}{p}\right)$. Since $\left(\frac{M}{p}\right) = 1$, then that means that M is a quadratic residue modulo p. We are told in the question that M_1 is a quadratic residue modulo p, and M_2 is not a quadratic residue modulo p. Therefore since the M in $C_2 \equiv My^k \mod p$ is a quadratic residue modulo p, it must be M_1, meaning that in this case $C = E(M_1)$. Thus the assertion is true.

Assertion 2: If $\left(\frac{y}{p}\right) = 1$ and $\left(\frac{C_2}{p}\right) = -1$, then $C = E(M_2)$:

Since $C_2 \equiv My^k \mod p$, this implies that $\left(\frac{C_2}{p}\right) = \left(\frac{My^k}{p}\right) = \left(\frac{M}{p}\right)\left(\frac{y}{p}\right)^k$. Since $\left(\frac{y}{p}\right) = 1$ and $\left(\frac{C_2}{p}\right) = -1$, we can substitute them into the equation to get: $-1 = \left(\frac{M}{p}\right)(1)^k = \left(\frac{M}{p}\right)$. Since $\left(\frac{M}{p}\right) = -1$, then that means that M is not a quadratic residue modulo p. We are told in the question that M_1 is a quadratic residue modulo p, and M_2 is not a quadratic residue modulo p. Therefore since the M in $C_2 \equiv My^k \mod p$ is not a quadratic residue modulo p, it must be M_2, meaning that in this case $C = E(M_2)$. Thus the assertion is true.

Assertion 3: If $\left(\frac{y}{p}\right) = -1$ and $\left(\frac{C_1}{p}\right) = 1$ and $\left(\frac{C_2}{p}\right) = 1$, then $C = E(M_1)$:

Since $y \equiv g^x \mod p$, then that means that $\left(\frac{y}{p}\right) = \left(\frac{g}{p}\right)^x$. Since we know that $\left(\frac{y}{p}\right) = -1$, that means that $-1 = \left(\frac{g}{p}\right)^x$. From this, we can see that $\left(\frac{g}{p}\right) = -1$, and x must be an odd integer. Next, we see that $C_1 \equiv g^k \mod p$, meaning that $\left(\frac{C_1}{p}\right) = \left(\frac{g}{p}\right)^k$. We know that $\left(\frac{C_1}{p}\right) = 1$ and $\left(\frac{g}{p}\right) = -1$, meaning that $1 = (-1)^k$. Therefore, k must be an even number.

Next, we can see that since $C_2 \equiv My^k \mod p$, then $\left(\frac{C_2}{p}\right) = \left(\frac{M}{p}\right)\left(\frac{y}{p}\right)^k$. We know that $\left(\frac{C_2}{p}\right) = 1$ and that $\left(\frac{y}{p}\right) = -1$ and that k is an even number. Therefore, we can see that $1 = \left(\frac{M}{p}\right)(-1)^{even} = \left(\frac{M}{p}\right)$. Since $\left(\frac{M}{p}\right) = 1$, then that means that M is a quadratic residue modulo p. We know that M_1 is a quadratic residue modulo p, and M_2 is not a quadratic residue modulo p. Therefore since the M in $C_2 \equiv My^k \mod p$ is a quadratic residue modulo p, it must be M_1, meaning that in this case $C = E(M_1)$. Thus the assertion is true.

Assertion 4: If $\left(\frac{y}{p}\right) = -1$ and $\left(\frac{C_1}{p}\right) = 1$ and $\left(\frac{C_2}{p}\right) = -1$, then $C = E(M_2)$:

Since $y \equiv g^x \mod p$, then that means that $\left(\frac{y}{p}\right) = \left(\frac{g}{p}\right)^x$. Since we know that $\left(\frac{y}{p}\right) = -1$, that means that $-1 = \left(\frac{g}{p}\right)^x$. From this, we can see that $\left(\frac{g}{p}\right) = -1$, and x must be an odd integer. Next, we see that $C_1 \equiv g^k \mod p$, meaning that $\left(\frac{C_1}{p}\right) = \left(\frac{g}{p}\right)^k$. We know that $\left(\frac{C_1}{p}\right) = 1$ and

$\left(\frac{g}{p}\right) = -1$, meaning that $1 = (-1)^k$. Therefore, k must be an even number.

Next, we can see that since $C_2 \equiv My^k \mod p$, then $\left(\frac{C_2}{p}\right) = \left(\frac{M}{p}\right)\left(\frac{y}{p}\right)^k$. We know that $\left(\frac{C_2}{p}\right) = -1$ and that $\left(\frac{y}{p}\right) = -1$ and that k is an even number. Therefore, we can see that $-1 = \left(\frac{M}{p}\right)(-1)^{even} = \left(\frac{M}{p}\right)$. Since $\left(\frac{M}{p}\right) = -1$, then that means that M is not a quadratic residue modulo p. We know that M_1 is a quadratic residue modulo p, and M_2 is not a quadratic residue modulo p. Therefore since the M in $C_2 \equiv My^k \mod p$ is not a quadratic residue modulo p, it must be M_2, meaning that in this case $C = E(M_2)$. Thus the assertion is true.

Assertion 5: If $\left(\frac{y}{p}\right) = -1$ and $\left(\frac{C_1}{p}\right) = -1$ and $\left(\frac{C_2}{p}\right) = 1$, then $C = E(M_2)$:

Since $y \equiv g^x \mod p$, then that means that $\left(\frac{y}{p}\right) = \left(\frac{g}{p}\right)^x$. Since we know that $\left(\frac{y}{p}\right) = -1$, that means that $-1 = \left(\frac{g}{p}\right)^x$. From this, we can see that $\left(\frac{g}{p}\right) = -1$, and x must be an odd integer. Next, we see that $C_1 \equiv g^k \mod p$, meaning that $\left(\frac{C_1}{p}\right) = \left(\frac{g}{p}\right)^k$. We know that $\left(\frac{C_1}{p}\right) = -1$ and $\left(\frac{g}{p}\right) = -1$, meaning that $-1 = (-1)^k$. Therefore, k must be an odd number.

Next, we can see that since $C_2 \equiv My^k \mod p$, then $\left(\frac{C_2}{p}\right) = \left(\frac{M}{p}\right)\left(\frac{y}{p}\right)^k$. We know that $\left(\frac{C_2}{p}\right) = 1$ and that $\left(\frac{y}{p}\right) = -1$ and that k is an odd number. Therefore, we can see that $1 = \left(\frac{M}{p}\right)(-1)^{odd} = -\left(\frac{M}{p}\right)$, meaning that $\left(\frac{M}{p}\right) = -1$. Since $\left(\frac{M}{p}\right) = -1$, then that means that M is not a quadratic residue modulo p. We know that M_1 is a quadratic residue modulo p, and M_2 is not a quadratic residue modulo p. Therefore since the M in $C_2 \equiv My^k \mod p$ is not a quadratic residue modulo p, it must be M_2, meaning that in this case $C = E(M_2)$. Thus the assertion is true.

Assertion 6: If $\left(\frac{y}{p}\right) = -1$ and $\left(\frac{C_1}{p}\right) = -1$ and $\left(\frac{C_2}{p}\right) = -1$, then $C = E(M_1)$:

Since $y \equiv g^x \mod p$, then that means that $\left(\frac{y}{p}\right) = \left(\frac{g}{p}\right)^x$. Since we know that $\left(\frac{y}{p}\right) = -1$, that means that $-1 = \left(\frac{g}{p}\right)^x$. From this, we can see that $\left(\frac{g}{p}\right) = -1$, and x must be an odd integer. Next, we see that $C_1 \equiv g^k \mod p$, meaning that $\left(\frac{C_1}{p}\right) = \left(\frac{g}{p}\right)^k$. We know that $\left(\frac{C_1}{p}\right) = -1$ and $\left(\frac{g}{p}\right) = -1$, meaning that $-1 = (-1)^k$. Therefore, k must be an odd number.

Next, we can see that since $C_2 \equiv My^k \mod p$, then $\left(\frac{C_2}{p}\right) = \left(\frac{M}{p}\right)\left(\frac{y}{p}\right)^k$. We know that $\left(\frac{C_2}{p}\right) = -1$ and that $\left(\frac{y}{p}\right) = -1$ and that k is an odd number. Therefore, we can see that $-1 = \left(\frac{M}{p}\right)(-1)^{odd} = -\left(\frac{M}{p}\right)$, meaning that $\left(\frac{M}{p}\right) = 1$. Since $\left(\frac{M}{p}\right) = 1$, then that means that M is a quadratic residue modulo p. We know that M_1 is a quadratic residue modulo p, and M_2 is not a quadratic residue modulo p. Therefore since the M in $C_2 \equiv My^k \mod p$ is a quadratic residue modulo p, it must be M_1, meaning that in this case $C = E(M_1)$. Thus the assertion is true.

We've proved that all of Mallory's assertions are true. Therefore, El Gamal is not semantically secure.

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

We are asked to show that the version of RSA specified in this question is not IND-CCA secure. We start by choosing two different plaintexts, M_1 and M_2, and receive a ciphertext C that is an encryption of one of them. The ciphertext can be represented as:

$$C = (s||t) = (r^e (mod \quad n)||H(r) \oplus M_i)$$

where i = 1 or i = 2. The value r is a random k-bit value such that $r < n$. In this case, n also has k-bits. H is a public random function that maps $\{0,1\}^k$ to $\{0,1\}^m$, where m is the bit-length of the message being encrypted.

We then compute a new ciphertext, C' from C, such that:

$$C' = (s||t')$$

where $t' = t \oplus M_1$. From here, we have two cases:

Case 1: C is an encryption of M_1.

In the question, we are told that decryption is done via $M \equiv H(s^d (mod \quad n)) \oplus t$. The decryption of C' would therefore be: $M \equiv H(s^d (mod \quad n)) \oplus t'$. Since $t' = t \oplus M_1$, and in this case we know that $t = H(r) \oplus M_1$, that means that $t' = H(r) \oplus M_1 \oplus M_1$. A number XOR'd with itself equals zero, meaning that $t' = H(r) \oplus 0 = H(r)$. Therefore, the decryption of C' can be simplified to:

$$\begin{aligned} M &\equiv H(s^d (mod \quad n)) \oplus t' \\ &\equiv H(s^d (mod \quad n)) \oplus H(r) \end{aligned}$$

We know that $s = r^e$, meaning $s^d = r^{ed}$. By the definition of e and d, we know that $ed = 1 + k\phi(n)$, meaning that $r^{ed} = r^{1+k\phi(n)} = r(r^{\phi(n)})$. We can use Euler's theorem to show that $r^{\phi(n)} \equiv 1 \mod n$ (the probability of $gcd(r, n) \neq 1$ is very low). Thus, we can see that $r^{ed} \equiv r \mod n$. Therefore, $H(s^d (mod \quad n)) = H(r)$. Thus, we can once again modify the decryption process to see that:

$$\begin{aligned} M &\equiv H(s^d (mod \quad n)) \oplus H(r) \\ &= H(r) \oplus H(r) \\ &= 0 \end{aligned}$$

Therefore, when C is an encryption of M_1, then the decryption of C' is 0.

Case 2: C is an encryption of M_2.

In the question, we are told that decryption is done via $M \equiv H(s^d(mod \quad n)) \oplus t$. The decryption of C' would therefore be: $M \equiv H(s^d(mod \quad n)) \oplus t'$. Since $t' = t \oplus M_1$, and in this case we know that $t = H(r) \oplus M_2$, that means that $t' = H(r) \oplus M_1 \oplus M_2$. Therefore, the decryption of C' can be re-written as:

$$\begin{aligned} M &\equiv H(s^d(mod \quad n)) \oplus t' \\ &\equiv H(s^d(mod \quad n)) \oplus H(r) \oplus M_1 \oplus M_2 \end{aligned}$$

From the previous case, we showed that $H(s^d(mod \quad n)) = H(r)$. Thus, we can once again modify the decryption process to see that:

$$\begin{aligned} M &\equiv H(s^d(mod \quad n)) \oplus H(r) \oplus M_1 \oplus M_2 \\ &= H(r) \oplus H(r) \oplus M_1 \oplus M_2 \\ &= M_1 \oplus M_2 \end{aligned}$$

Therefore, when C is an encryption of M_2, then the decryption of C' is $M_1 \oplus M_2$. Mallory can easily compute this value, since she selects both M_1 and M_2.

From this, we can see that Mallory has a method to easily identify whether C is the ciphertext of M_1 or M_2 based on the decryption of C'. If the decryption of C' is 0, then C is an encryption of M_1. Otherwise, if the decryption of C' is $M_1 \oplus M_2$, then C is an encryption of M_2.

Problem 6 — An attack on RSA with small decryption exponent, 25 marks

(a)

(b)

(c)

(d)

(e)

(f)

Problem 7 — Universal forgery attack on the El Gamal signature scheme, 12 marks)

(a)

(b)

(c)

Problem 9 — Columnar transposition cryptanalysis, 10 marks