Name: Joshua Dow

Student ID: 10150588

Problem 1 — A modified man-in-the-middle attack on Diffie-Hellman, 12 marks

(a) Alice selects a, Bob selects b
Alice computes $y_a \equiv g^a \mod p$, Bob computes $y_b \equiv g^b \mod p$
Alice sends y_a, Bob sends y_b
Mallory intercepts and sends y_a^q to Bob, y_b^q to Alice
Alice,Bob calculate $K \equiv y_b^{qa} \equiv g^{bqa} (\mod p) \equiv g^{aqb} (\mod p) \equiv y_a^{qb} \equiv K$
So the key calculated is the same

(b) Since g is a primitive root of p, then $\{g^1, g^2, ..., g^{p-1}\}$ is the set of all non zero congruence classes modulo p. By Fermats Little Theorem we know $g^{p-1} \equiv 1 (\mod p)$ since g is a primitive root of p. The set above $\{g^1, g^2, ..., g^{p-1}\}$ contains only m elements since p-1 = mq and any g^{mq} is already in $\{g^1, g^2, ..., g^{p-1}\}$ since it is a cyclic group. So we need only show all of the elements are distinct as follows:
Proof:
Clearly $\{g^1, g^2, ..., g^{p-1}\} \subseteq < g >$ since $< g >$ is set set of all powers generated by g (mod p). Let $x \in < g >$, and say $x = g^k$, then $k = ql + r$ where $0 \leq r \leq p - 1$. Then $x = g^k = (g^l)^q g^r = 1^q g^r = g^r \in \{g^1, g^2, ..., g^{p-1}\}$ so $< g > \subseteq \{g^1, g^2, ..., g^{p-1}\}$. Given this then $< g > = \{g^1, g^2, ..., g^{p-1}\}$.
Next suppose $g^k = g^l$, where $0 \leq k \leq l \leq p - 1$, then $g^{l-k} = 1$ and $0 \leq m - k \leq p - 1$. Then $l - k = 0$, so $g^m = g^k$. So $\{g^1, g^2, ..., g^{p-1}\}$ are all distinct. So there are m values for k.
Note that when g is a primitive root of p $|K| = m$ if not, then $|K|$ is at most m.

(c) The advantage is Mallory only needs one key instead of two. This allows her to read,spoof, and alter messages without having to use/calculate separate keys.

Problem 2 — RSA and binary exponentiation, 24 marks

(a) $(e, n) = (11, 77)$

i. M = 17, $C \equiv M^e \equiv 17^{11} (\mod 77)$
$e = 11, 11 = 8 + 2 + 1 = 1011$
$b_0 = 1, b_1 = 0, b_2 = 1, b_3 = 1$
$r_0 \equiv 17^{b_0} \equiv 17 (\mod 77)$
$r_1 \equiv (r_0^2) \equiv 17^2 (\mod 77) \equiv 58 (\mod 77)$
$r_2 \equiv (58^2)(17) (\mod 77) \equiv 57188 (\mod 77) \equiv 54 (\mod 77)$
$r_3 \equiv (54^2)(17) (\mod 77) \equiv 49572 (\mod 77) \equiv 61 (\mod 77)$
So $17^{11} \equiv 61 (\mod 77)$, C = 61

ii. To find p,q we factor n = 77 = 7 x 11, $\phi(n) = (p-1)(q-1) = 60$, then we have the congruence $11d \equiv 1 (\mod 60)$
By Extended Euclidean Algorithm:
$11d + 60l = 1$
$11 = 0 * 60 + 1 * 11, q_0 = 0$
$60 = 5 * 11 + 5, q_1 = 5$
$11 = 2 * 5 + 1, q_2 = 2$
$5 = 2 * 2 + 1, q_3 = 2$
$2 = 2 * 1 + 0, q_4 = 2$
So = 4 and:
$d = (-1)^{n-1} B_{n-1}$ where $B_{-2} = 1, B_{-1} = 0$
$B_0 = 0 * 0 + 1 = 1$
$B_1 = 5 * 1 + 0 = 5$
$B_2 = 2 * 5 + 1 = 11$
$B_3 = 2 * 11 + 5 = 27$
$d \equiv (-1)^3 * 27 \equiv -27 (\mod 60) \equiv 33 (\mod 60)$

iii. C = 32, $M \equiv C^d \equiv 32^{33} (\mod 77)$
$d = 33, 33 = 32 + 1 = 100001$
$r_0 \equiv 32 (\mod 77)$
$r_1 \equiv 32^2 \equiv 23 (\mod 77)$
$r_2 \equiv 23^2 \equiv 67 (\mod 77)$
$r_3 \equiv 67^2 \equiv 23 (\mod 77)$
$r_4 \equiv 23^2 \equiv 67 (\mod 77)$
$r_5 \equiv 67^2 * 33 \equiv 23 * 33 (\mod 77) \equiv 66 (\mod 77)$
So $32^{33} \equiv 66 (\mod 77), M = 66$

(b) i. Proof by induction on i:

Base case: Let $s_0 = b_0$ and $s_{i+1} = 2s_i + b_{i+1}$ for $0 \leq i \leq k-1$

Let i = 1 then $s_1 = 2s_0 + b_1 = 2b_0 + b_1 = \sum_{j=0}^{i} b_j 2^{i-j} = b_0 * 2^{1-0} + b_1 * 2^0 = 2b_0 + b_1$

Inductive Hypothesis:

Suppose $0 \leq i \leq k$ such that $s_i = \sum_{j=0}^{i}$, we wish to show this for i+1

Inductive Step:

Let l = i+1, $0 \leq l \leq k-1$ such that:

$s_l = s_{i+1} = 2s_i + b_{i+1}$

$= 2\sum_{j=0}^{i} + b_{i+1}$

$= 2(b_0 2^i + b_1 2^{i-1} + ... + b_i) + b_{i+1}$

$= b_0 2^{i+1} + b_1 2^i + ... + b_i 2 + b_{i+1}$

$= 2s_i + b_l$

$= 2(2(s_{i-1} + b_i)) + b_{i+1}$

$= 2(...(2s_0 + b_1)...) + b_{i+1}$ as required. This concludes our induction on i

ii. Proof by induction on i:

Base case: Let i = 0 then,

$r_0 \equiv a^{s_0}(\mod m) \equiv a^{b_0}(\mod m) \equiv a(\mod m)$

Inductive Hypothesis:

Suppose for $0 \leq i \leq k$ such that $r_i \equiv a^{s_i}(\mod m)$ we wish to show this for i+1

Inductive Step:

$r_{i+1} \equiv a^{s_{i+1}}(\mod m)$

$\equiv a^{2s_i + b_{i+1}}(\mod m)$

$\equiv a^{2s_i} a^{b_{i+1}}(\mod m)$

$\equiv r_i^2 a^{b_{i+1}}(\mod m)$ By IH

If $b_{i+1} = 0$:

$r_{i+1} \equiv r_i^2 a^0(\mod m) \equiv r_i^2$

If $b_{i+1} = 1$:

$r_{i+1} \equiv r_i^2 a(\mod m)$ As required, and we conclude our induction on i

iii. Proof that $a^n \equiv r_k(\mod m)$

Suppose a^n, then $r_0 = a$

Let K be the number of binary digits required to represent n, then $b_0 = 1, b1, ..., b_{k-1}$

Using the proof from part ii, we have the following:

$r_{k-1} \equiv r_{k-2} a^{b_{k-1}}(\mod m)$

$\equiv (r_{k-3}) a^{b_{k-2}} a^{b_{k-1}}(\mod m)$

...

$\equiv (r_{k-k}) * a^{b_1} * a^{b_2} * ... * a^{b_{k-1}}(\mod m)$

$\equiv r_0 * a^{b_1} * a^{b_2} * ... * a^{b_{k-1}}(\mod m)$

$\equiv a * a^{b_1} * a^{b_2} * ... * a^{b_{k-1}}(\mod m)$

$\equiv a^{1 + b_1 + b_2 + ... + b_{k-1}}(\mod m)$

$\equiv a^n(\mod m)$ So $a^n \equiv r_k(\mod m)$ as required

Problem 3 — Fast RSA decryption using Chinese remaindering, 8 marks
Given $d_p \equiv d(\mod p-1) \equiv e^{-1}(\mod p-1), d_q \equiv (\mod q-1) \equiv e^{-1}(\mod q-1)$ and $M_p \equiv C^{d_p}(\mod p), M_q \equiv C^{d_q}(\mod q)$. Then $M' \equiv pxM_q + qyM_p$
$M' \equiv M_q + q((q^{-1}(\mod p))(M_p - M_q))(\mod p)$
So $M_q \equiv M'(\mod q)$
and $M_p \equiv M_p(\mod p)$
$\equiv ((M_p - M_q) + M_q)(\mod p)$
$\equiv M'(\mod p)$
Then M' = M since M'. The CRT version of RSA allows for significantly faster computation of M_p and M_q rather than C^d because of the fact d is very large.

Problem 4 – The ElGamal public key cryptosystem is not semantically secure, 10 marks

(a) If $\left(\frac{y}{p}\right) = 1, \left(\frac{C_2}{p}\right) = 1$ Then $C = E(M_1)$
Proof:
Since $\left(\frac{y}{p}\right) = 1, \left(\frac{C_2}{p}\right), \exists_{X_1, X_2} \in Z$ such that: $X_1^2 \equiv y(\mod p)$ and $X_2^2 \equiv C_2(\mod p)$ and
$C_2 C_1^{p-1-x} \equiv M(\mod p)$
$x_2^2 * g^{k(p-1-x)} \equiv M(\mod p)$
$(x_2 * g^{k(p-1-x)})^2 \equiv M(\mod p)$
and $x_2 * g^{k(p-1-x)} \in Z$ so $\left(\frac{M}{p}\right) = 1$ and $C = E(M_1)$

(b) If $\left(\frac{y}{p}\right) = 1, \left(\frac{C_2}{p}\right) = -1$ Then $C = E(M_2)$
Proof:
Since $\left(\frac{y}{p}\right) = 1, \exists_{X_1} \in Z$ such that: $X_1^2 \equiv y(\mod p)$
$C_2 C_1^{p-1-x} \equiv M(\mod p)$
$M y^k C_1^{p-1-x} \equiv M(\mod p)$
$M(X_1^2)^k C_1^{p-1-x} \equiv M(\mod p)$
$M(X_1^2)^k g^{k(p-1-x)} \equiv M(\mod p)$
$M(X_1^2)^k (g^{p-1})^{k-x} \equiv M(\mod p)$
$M(X_1^2)^k 1^{k-x} \equiv M(\mod p)$
$M(X_1^2)^k \equiv M(\mod p)$
$M(X_1^2)^k$ So M is not a quadratic residue mod p, then $M \notin QN_p$. So $C = E(M_2)$

(c) If $\left(\frac{y}{p}\right) = -1, \left(\frac{C_1}{p}\right) = 1, \left(\frac{C_2}{p}\right) = 1$ then $X_2^2 \equiv C_1(\mod p), X_3^2 \equiv (\mod p)$
$C_2 C_1^{p-1-x} \equiv M(\mod p)$
$X_3^2 X_2^{2(p-1-x)} \equiv M(\mod p)$
$(X_3 X_2^{p-1-x})^2 \equiv M(\mod p)$
Then $\left(\frac{M}{p}\right) = 1$ so $C = E(M_1)$

(d) If $\left(\frac{y}{p}\right) = -1, \left(\frac{C_1}{p}\right) = 1, \left(\frac{C_2}{p}\right) = -1$ then $X_2^2 \equiv C_1(\mod p)$
$C_2 C_1^{p-1-x} \equiv M(\mod p)$
$C_2 X_2^{2(p-1-x)} \equiv M(\mod p)$
$M g^{kx} X_2^{2(p-1-x)} \equiv M(\mod p)$
Then $\left(\frac{M}{p}\right) = -1$ so $C = E(M_2)$

(e) If $\left(\frac{y}{p}\right) = -1, \left(\frac{C_1}{p}\right) = -1, \left(\frac{C_2}{p}\right) = 1$ then $X_3^2 \equiv (\mod p)$
$C_2 C_1^{p-1-x} \equiv M(\mod p)$
$X_3^2 C_1^{p-1-x} \equiv M(\mod p)$
$X_3^2 g^{k(p-1-x)} \equiv M(\mod p)$ Then $\left(\frac{M}{p}\right) = -1$ so $C = E(M_2)$

(f) If $\left(\frac{y}{p}\right) = -1, \left(\frac{C_1}{p}\right) = -1, \left(\frac{C_2}{p}\right) = -1$
$C_2 C_1^{p-1-x} \equiv M(\mod p)$
$M(g^{p-1})^k \equiv M(\mod p)$
$M \equiv M(\mod p)$
Then $M \in QR_p$ so $C = E(M_1)$

Problem 5 — An IND-CPA, but not IND-CCA secure version of RSA, 10 marks
Let $C' = (s||t \oplus M_1)$
$C' = (r^e(\mod n)||H(r) \oplus M_i \oplus M_1)$
$M' \equiv H(r^{ed}(\mod n)) \oplus (H(r) \oplus M_i \oplus M_1)$
If $i = 1$, $M' \equiv H(r^{ed}(\mod n)) \oplus (H(r) \oplus M_1 \oplus M_1)$
$M' \equiv H(r^{ed}(\mod n)) \oplus (H(r))$
$M' \equiv 0$
Otherwise $M' \not\equiv 0$
Either M' is 0, in which case we know for certain $M_i = M_1$