Brendan Petras - 10137098
Introduction to Cryptography   CPSC 418   Fall 2016
Department of Computer Science
University of Calgary

December 9, 2016

HOME WORK #[4]

Problem	Marks
1	
2	
3	
4	
5	
6	
7	
Total	

Problem 1.

(a) $\Phi(n) = (p-1)(q-1) = pq - p - q + 1$
$\Phi(n) = n - p - \frac{n}{p} + 1$
$\Phi(n)p = np - p^2 - n + p$
$0 = np - p^2 - n + p - \Phi(n)p$ - rearrange
$0 = p^2 + \Phi(n)p - np - p + n$ - group like terms
$0 = p^2 + (\Phi(n) - n - 1)p + n$
We can find the roots of this quadratic which will return p and q.
With, $a = 1, b = \Phi(n) - n - 1, c = n$
$x = \frac{-b\pm\sqrt{b^2-4ac}}{2a}$, x will return two solutions, namely p and q, assuming $\sqrt{b^2 - 4ac} \neq 0$.

(b) Start with $M = M^1$
Notice that $gcd(e_1, e_2) = 1$ means that $e_1x + e_2y = 1$
Notice that $M^1 = M^{e_1x+e_2y}$
$= M^{e_1x} * M^{e_2y}$
$= C_1^x * C_2^y$ - since $M^{e_1} = C_1$ and $M^{e_2} = C_2$
Since C_1, C_2, x, y are known we can find M.

(c) Given $(e, n_1), (e, n_2), ..., (e, n_i)$ and $gcd(n_i, n_j) = 1$, with $i \neq j$
In general, $C_i \equiv M^e \pmod{n_i}$, for all i. Assume $k \geq e$ where k is number of participants.
By The Chinese Remainder Theorem, we can efficiently compute C,
with $C \equiv C_i \pmod{n_i}$ for $1 \geq i \geq k$. So $C \equiv M^e \pmod{n}$ with $(n = \prod_1^i n_i)$.
Which is to say M^e is not modded by any n_i
Thus finding $C_i = (M^e)^{\frac{1}{e}}$ is a eth root calculation

(d) Given $e = 3$ Bob wants to send $M, M + r, M + s$ o Alice
M - unknown, r, s, C, C_r, C_s - known
$C \equiv M^3 \pmod{n}$
$C_r \equiv (M + r)^3 \pmod{n}$
$C_s \equiv (M + s)^3 \pmod{n}$

$C \equiv M^3 \pmod{n}$
$C_r \equiv (M + r)^3 \equiv M^3 + 3M^2r + 3Mr^2 + r^3 \pmod{n}$
$C_s \equiv (M + s)^3 \equiv M^3 + 3M^2s + 3Ms^2 + s^3 \pmod{n}$
$C_r \equiv C_r - C \equiv 3M^2r + 3Mr^2 + r^3 \pmod{n}$
$C_s \equiv C_s - C \equiv 3M^2s + 3Ms^2 + s^3 \pmod{n}$
$\equiv 3M^2r + 3Mr^2 \pmod{n}$ - remove r^3 since it is a known constant
$\equiv 3M^2s + 3Ms^2 \pmod{n}$ - remove s^3 since it is a known constant
$\equiv 3Mr(M + r) \pmod{n}$ - factor Mr
$\equiv 3Ms(M + s) \pmod{n}$ - factor Ms
$\equiv 3Mr\sqrt[3]{C_r} \pmod{n}$ - sub C_r
$\equiv 3Ms\sqrt[3]{C_s} \pmod{n}$ - sub C_s
$M \equiv 1(3r\sqrt[3]{C_r})^{-1} \pmod{n}$ - modular inverse C_r
$M \equiv 1(3s\sqrt[3]{C_s})^{-1} \pmod{n}$ - modular inverse C_s

Problem 2. Prove CRT decrypts like normal, prove $m' = m$

$m \equiv pxM_q + qyM_p \pmod{n}$
$m \equiv qyM_p \pmod{p}$
$m \equiv M_p \pmod{p}$ - since $gcd(px + qy) = 1 -> gy \equiv 1 \pmod{p}$
$m \equiv pxM_q \pmod{q}$
$m \equiv M_q \pmod{p}$ - since $gcd(px + qy) = 1 -> px \equiv 1 \pmod{q}$

$m' \equiv C^d \pmod{n}$
$m' \equiv C^{d_p + \cancel{(p-1)L}} \pmod{p}$ - by Fermat's LT
$m' \equiv M_p \pmod{p}$
$m' \equiv C^{d_q + \cancel{(q-1)T}} \pmod{q}$ - by Fermat's LT
$m' \equiv M_q \pmod{q}$

So, $gcd(p, q) = 1$
$px + qy = 1$
$M(px + qy) = M$
$Mpx + Mqy = M$
$M_q px + M_p qy \equiv M \pmod{n}$

Problem 3. Prove that the cryptosystem is NOT IND-CCA

A cryptosystem is not IND-CCA secure if some active attacker, with some decryption oracle can, in polynomial time, select two plaintexts M_1, M_2 and correctly distinguish between the encryptions of M_1 and M_2 with probability significantly greater than 1/2.

Start with M_1, M_2 with $M_1 \neq 0^n$
Apply the attack $C' = (s||t \oplus M_1)$, we can examine C' since we have a decryption oracle.

$C' = (s||t \oplus M_1)$
$C' = (s||H(r) \oplus M_1 \oplus M_i)$
if $i = 1$ then $C' = (s||H(r))$

Apply the decryption function D

$D(C') = H(s^d) \oplus H(r) \pmod n$
$D(C') = H(r^{ed}) \oplus H(r) \pmod n$
$D(C') = H(r) \oplus H(r) \pmod n$
$D(C') =^m$

Then we know with 100% probability which plaintext the ciphertext belongs to.
Thus it is not IND-CCA secure.

Problem 4. (a) i. Given $(r, s_1), (r, s_2), M_1, M_2, Hashfunction\ H$. Find k.

$ks_1 \equiv H(M_1, r) - xr \pmod{p-1}$
$ks_2 \equiv H(M_1, r) - xr \pmod{p-1}$
$ks_1 - ks_2 + H(M_1, r) - xr - H(M_2, r) + xr + (p-1)L - (p-1)T = 0$ converting from congruence to equality. With L,T real numbers.
$ks_1 - ks_2 + H(M_1, r) - xr - H(M_2, r) + xr + (p-1)L - (p-1)T = 0$
$k(s_1 - s_2) + H(M_1, r) - H(M_2, r) + \cancel{xr} - \cancel{xr} + (p-1)L - (p-1)T = 0$
$k(s_1 - s_2) \equiv H(M_2, r) - H(M_1, r) \pmod{p-1}$ - move back to congruence
$k \equiv [H(M_2, r) - H(M_1, r)](s_1 - s_2)^{-1} \pmod{p-1}$ - modular inverse since $gcd(s_1 - s_2, p-1) = 1$

ii. We now know k.

$ks_1 \equiv H(M_1, r) - xr \pmod{p-1}$
$xr \equiv H(M_1, r) - ks_1 \pmod{p-1}$
$x \equiv r^{-1}[H(M_1, r) - ks_1] \pmod{p-1}$ - since $gcd(r, p-1) = 1$

(b) i. Prove $y^r r^s \equiv g^m \pmod{p-1}$
$y^r r^s \equiv g^m \pmod{p-1}$
$y^r g^{su} y^{vs} \equiv g^{su} \pmod{p-1}$
$y^r y^{vs} g^{su} \equiv g^{su} \pmod{p-1}$ - now lets try getting $y^r y^{vs}$ to equal 1
$y^{r+vs} g^{su} \equiv g^{su} \pmod{p-1}$
$y^{r+-rv^*v} g^{su} \equiv g^{su} \pmod{p-1}$
$y^{(r+-r)1} g^{su} \equiv g^{su} \pmod{p-1}$ - since $vv^* \equiv 1 \pmod{p-1}$
$g^{su} \equiv g^{su} \pmod{p-1}$

ii. When we return the hash function H back into ElGamal, we no longer can find a m in $g^{H(M,r)}$ such that $m = H(M, r)$. This is the deffinition of pre-image resistance.

(c) i. Prove $R \equiv ru \pmod{p-1}$
$R = rup - r(p-1) + p(p-1)L$ - for some real L
$R \equiv rup + p^2 - p \pmod{p-1}$
$R \equiv p(ru + p - 1) \pmod{p-1}$
$R \equiv rup + \cancel{p(p-1)} \pmod{p-1}$
$R \equiv ru(p - 1 + 1) \pmod{p-1}$
$R \equiv \cancel{ru(p-1)} + ru) \pmod{p-1}$
$R \equiv ru \pmod{p-1}$

ii. Prove $R^S \equiv r^{su} \pmod{p}$
$R^S \equiv r^{su} \pmod{p}$
$R^{su} \equiv [rup - r(p-1)]^{su} \pmod{p}$
$R^{su} \equiv (\cancel{rup^{su}} - \cancel{rp^{su}} + r^{su}) \pmod{p}$
$R^{su} \equiv r^{su} \pmod{p}$
$R^S \equiv r^{su} \pmod{p}$

iii. Prove $y^R R^S \equiv g^{H(M')} \pmod{p}$ - This shows (R,S) is a valid signature to message M'
$y^R R^S \equiv g^{H(M')} \pmod{p}$
$y^{ru} r^{su} \equiv g^{H(M')} \pmod{p}$
$y^{ru} g^{ksu} \equiv g^{H(M')} \pmod{p}$
$g^{xru} g^{ksu} \equiv g^{H(M')} \pmod{p}$
$g^{xru} g^{[H(M)-xr]u} \equiv g^{H(M')} \pmod{p}$
$g^{xru} g^{H(M)u} g^{-xru} \equiv g^{H(M')} \pmod{p}$
$\cancel{g^{xru}} g^{H(M)u} \cancel{g^{-xru}} \equiv g^{H(M')} \pmod{p}$
$g^{H(M)u} \equiv g^{H(M')} \pmod{p}$
$g^{H(M')} \equiv g^{H(M')} \pmod{p}$ - via step 3 and the EEA.

Submitted by Brendan Petras - 10137098 on December 9, 2016.