Mike Simister - 10095107
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. (Security of RSA, 15 marks)

(a)

$$\begin{aligned}
\text{We have that: } n = pq,\ \phi(n) &= \phi(p)\phi(q) = (p-1)(q-1) \\
\text{so, } \phi(n) &= pq + 1 - p - q \\
&= n + 1 - p - q \qquad \textbf{(b/c pq = n)} \\
p + q &= n - \phi(n) + 1 \\
q &= n - \phi(n) - p + 1 \\
\text{since } n &= pq \\
n &= p(n - \phi(n) - p + 1) \\
&= p^2 - p(\phi(n) + 1) \\
\text{which means } p^2 - p(\phi(n) + 1) - n &= 0
\end{aligned}$$

because we know n and $\phi(n)$ we can solve this using the well known quadratic formula where,

$$\begin{aligned}
a &= 1 \\
b &= (n - \phi(n) + 1) \\
c &= n \\
\text{making } p &= \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}
\end{aligned}$$

(b)

We know that: $GCD(e_1, e_2) = 1$ so, $\exists\ x, y$ such that $x * e_1 + y * e_2 = 1 \pmod{n}$

Using the Extended Euclidean Algorithm, we can compute x, y

At which time we have $C_1 * C_2 = (M^{e_1})^x * (M^{e_2})^y = M^{e_1 * x + e_2 * y} = M^1 = M$

(c)

Given that this message is encrypted for all of the key owners.
Also given that $M < n_i$ for each i
Also given that $1 \leq i \leq k$
According to the Chinese Remainder Theorem there is a unique $x < n_1 n_2 ... n_k$ such that for each i we have $x = C_i \pmod{n)_i}$ The CTR describes how we can compute x
$M^k < n_1 n_2 ... n_k$, and also satisfies these equations. So, $x = Mk$

(d)

Problem 2. (Fast RSA decryption using Chinese remaindering, 6 marks)

Given that:

$$C \equiv M^e \pmod{n}$$
$$d_p \equiv d(\pmod{p-1})$$
$$d_q \equiv d(\pmod{p-1})$$
$$M_p \equiv C^{d_p} \pmod{p}$$
$$M_q \equiv C^{d_q} \pmod{q}$$

We can say that:

$$C \equiv M^e \pmod{p}$$

because:

$$C \equiv M^e \pmod{n} \textbf{ so,}$$
$$C = M^e + n(k) \textbf{ for some } k$$
$$= M^e + p(qk) \textbf{ for some } k$$

we can use similar logic to say that:

$$C \equiv M^e \pmod{q}$$

so because,

$$d_p \equiv d \pmod{p-1}$$

we can say that: $d_p = d + (p-1)(t)$ **for some** t

so for, $M_p \pmod{p}$

$$M_p \equiv C^{d_p} \equiv C^{d+(p-1)(t)} \equiv C^d * (C^{(p-1)})^t \equiv C^d \equiv M^{ed} \equiv M \pmod{p}$$

The same can be said for $M_q \pmod{q}$

since $M_p \equiv M \pmod{p}$ **we can say that**

$$M_p = M + p(k) \textbf{ for some } k$$

and since $M_q \equiv M \pmod{q}$ **we can say that**

$$M_q = M + p(t) \textbf{ for some } t$$

so, setting $M' \equiv pxM_q + qyM_p \pmod{n}$

and subbing for M_q **and** M_p

$$M' \equiv px(M + q(t)) + qy(M + p(k)) \pmod{pq}$$
$$M' \equiv M(px) + \cancel{pxq(t)} + M(qy) + \cancel{pqy(k)} \pmod{pq}$$
$$M' \equiv M(px + qy) \pmod{pq}$$
$$M' \equiv M \pmod{pq} \quad \square$$

Problem 3. (An IND-CPA, but not IND-CCA secure version of RSA, 8 marks)

Given that:

$$r < n$$
$$s = r^e \pmod{n}$$
$$t = H(r) \oplus M$$

and given that:

$$\textbf{Encryption} \rightarrow C = s||t = r^e \pmod{n}||H(r) \oplus M$$
$$\begin{aligned}\textbf{Decryption} \rightarrow M &= H(s^d \pmod{n}) \oplus t \\ &= H(r^{ed} \pmod{n}) \oplus H(r) \oplus M \\ &= H(r \pmod{n}) \oplus H(r) \oplus M\end{aligned}$$

Choosing a ciphertext of:

$$C = s||t \oplus M_1$$

gives a decryption of:

$$M_i = H(r \pmod{n}) \oplus H(r) \oplus M_i \oplus M_1$$
$$M_i = H(r) \oplus H(r) \oplus M_i \oplus M_1$$
$$M_i = M_i \oplus M_1$$

Which means that we can tell with 100 % certainty if the message is M_1 or M_2, i.e. If it decrypts to 0, then it is M_1 otherwise it is M_2

Problem 4. (Attacks on the ElGamal signature scheme, 23 marks)

(a)

(i)

We are given: $(r, s_1), (r, s_2)$
assuming that intercepting $(r, s_1), (r, s_2)$
means we also have also intercepted M_1, M_2 **then,**

$$\begin{aligned}s_1 - s_2 &\equiv [H(M_1||r) - xr]K^{-1} - [H(M_2||r) - xr]K^{-1} \pmod{p-1} \\ &\equiv [H(M_1||r) - H(M_2||r)]K^{-1} \pmod{p-1}\end{aligned}$$

so if we knew K

$$K(s_1 - s_2) \equiv [H(M_1||r) - H(M_2||r)] \pmod{p-1}$$

but we know that $\gcd((s_1 - s_2), p-1) = 1$

so we can find an inverse for $(s_1 - s_2)$

$$\begin{aligned}K(s_1 - s_2)(s_1 - s_2)^{-1} &\equiv [H(M_1||r) - H(M_2||r)](s_1 - s_2)^{-1} \pmod{p-1} \\ K &\equiv [H(M_1||r) - H(M_2||r)](s_1 - s_2)^{-1} \pmod{p-1}\end{aligned}$$

giving us K **in terms of things we know, mainly,**

$$H(M_1||r),\ H(M_2||r),\ (s_1 - s_2)^{-1}$$

(ii)

Given that we know K and that we can re-arrange the equation

$$xr = H(M,r) - ks \pmod{p-1}$$

Since we know r, k, s and $sH(M,r)$ and we know that $\gcd(r,(p-1)) = 1$

We can find an inverse for r giving,

$$xrr^{-1} \equiv r^{-1}(H(M,r) - ks \pmod{p-1})$$
$$x \equiv r^{-1}(H(M,r) - ks \pmod{p-1})$$

(b)

(i)

We want to show that $v_1 = v_2$ or

$$y^r r^s \equiv g^M \pmod{p}$$
$$y^r r^{-rv*} \equiv g^M \pmod{p}$$
$$y^r (g^u y^v)^{-rv*} \equiv g^M \pmod{p}$$
$$y^r y^{vv*-r} g^{u-rv*} \equiv g^M \pmod{p}$$
$$\cancel{y^r y^{-r}} g^{u-rv*} \equiv g^M \pmod{p}$$
$$g^{su} \equiv g^M \pmod{p}$$
$$g^M \equiv g^M \pmod{p}$$

(c)

(i)

Given

$R \equiv rup - r(p-1) \pmod{p(p-1)}$ **we can state that**

$R = rup - r(p-1) + p(p-1)(k)$ **for some** k

taking the entire statement above $\pmod{p-1}$ **we have**

$R \equiv rup - \cancel{r(p-1) + p(p-1)(k)} \pmod{p-1}$

We can re-write the equation as:

$R \equiv ru(p-1) + ru \pmod{p-1}$ **giving us:**

$R \equiv ru \pmod{p-1}$

So, we can again re-write the equation as:

$R = ru + (p-1)(t)$ **for some t, and thus we can conclude that:**

$y^R \equiv y^{ru+t(p-1)} \equiv y^{ru\cancel{(y^t)^{p-1}}} \pmod{p}$

(ii)

Given

$R \equiv rup - r(p-1) \pmod{p(p-1)}$ **we can state that**

$R = rup - r(p-1) + p(p-1)(k)$ **for some** k

taking the entire statement above $\pmod{p-1}$ **we have**

$R \equiv \cancel{rup} - r(p-1) + \cancel{p(p-1)(k)} \pmod{p}$

$R \equiv \cancel{-rp} + r \pmod{p}$

$R \equiv r \pmod{p}$

and given

$S \equiv su \pmod{p-1}$ **we can state that**

$S = su + (p-1)(t)$ **for some t**

giving us

$R^s \equiv R^{su+(k)(p-1)} \equiv R^{su} * \cancel{(R^k)^{(p-1)}} \pmod{p}$

and from the section above,

$R \equiv r \pmod{p}$ **so** $R^{su} \equiv r^{su} \pmod{p}$

Submitted by Mike Simister - 10095107 on December 9, 2016.