Solution to Problem Set 4

Due on Monday, November 3, 2008.

In the problems below, "textbook" refers to Douglas R. Stinson, *Cryptography: Theory and Practice, Third Edition*, Chapman & Hall/CRC, 2006.

Problem 1: Homomorpohic Mapping χ

Textbook, problem 5.5.

Solution:

According to Chinese remainder theorem, define the function $\chi^{-1} : \mathbf{Z}_3 \times \mathbf{Z}_5 \times \mathbf{Z}_7 \to \mathbf{Z}_{105}$ as follows:

$$\chi^{-1}(a_1, a_2, a_3) = \left(\sum_{i=1}^{3} a_i M_i N_i \right) \bmod 105, \tag{1}$$

where $\{n_i\} = \{3, 5, 7\}$, $N_i = 105/n_i$ and $M_i = N_i^{-1} \bmod n_i$. Therefore, we compute $\chi^{-1}(a_1, a_2, a_3)$ as follows:

$$\left.\begin{array}{l} n_1 = 3, N_1 = 35, M_1 = 35^{-1} \bmod 3 = 2 \\ n_2 = 5, N_2 = 21, M_2 = 21^{-1} \bmod 5 = 1 \\ n_3 = 7, N_3 = 15, M_3 = 15^{-1} \bmod 7 = 1 \end{array}\right\}$$

$$\Rightarrow \chi^{-1}(a_1, a_2, a_3) = (70a_1 + 21a_2 + 15a_3) \bmod 105 \tag{2}$$

Thus we can compute $\chi^{-1}(2, 2, 3) = (70 \times 2 + 21 \times 2 + 15 \times 3) \bmod 105 = 17$.

Problem 2: Chinese Remainder Theorem

Textbook, problem 5.6.

Solution:

According to Chinese remainder theorem, define x as follows:

$$x = \chi^{-1}(a_1, a_2, a_3) = \left(\sum_{i=1}^{3} a_i M_i N_i \right) \bmod (25 \times 26 \times 27), \tag{3}$$

Therefore, we compute $\chi^{-1}(a_1, a_2, a_3)$ as follows:

$n_1 = 25$, $N_1 = 702$, $M_1 = 702^{-1} \bmod 25 = (-12) \bmod 25 = 13$.

i	r_i	u_i	v_i	q_i
1	702	1	0	
2	25	0	1	28
3	2	1	-28	12
4	1	-12	337	

$n_2 = 26$, $N_2 = 675$, $M_2 = 675^{-1} \bmod 26 = (-1) \bmod 26 = 25$.

i	r_i	u_i	v_i	q_i
1	675	1	0	
2	26	0	1	25
3	25	1	-25	1
4	1	-1	26	

$n_3 = 27$, $N_3 = 650$, $M_3 = 650^{-1} \bmod 27 = (-13) \bmod 27 = 14$.

i	r_i	u_i	v_i	q_i
1	650	1	0	
2	27	0	1	24
3	2	1	-24	13
4	1	-13	313	

$$\begin{aligned} x &= \chi^{-1}(12, 9, 23) \\ &= (702 \times 13 \times 12 + 675 \times 25 \times 9 + 650 \times 14 \times 23) \bmod (25 \times 26 \times 27) \\ &= 14387 \end{aligned}$$

Problem 3: Primitive Root

Textbook, problem 5.9.

Solution:

Lucas test says, g is a primitive root of p if and only if $g^{(p-1)/q} \not\equiv 1 \pmod{p}$ for all $q > 1$ such that $q \mid (p-1)$. Now because p and q are odd primes such that $p = 2q + 1$, there are only two integers that we need to test with, 2 and q. We know that $\alpha \not\equiv \pm 1 \pmod{p}$. Then $\alpha^2 \not\equiv 1 \pmod{p}$ since if it were, α would be a square root of $1 \pmod{p}$, and the only square roots of 1 modulo a prime are ± 1.

Now let us look at α^q. Since p is a prime and $\alpha \in \mathbf{Z}_p^*$, then $\phi(p) = p - 1 = 2q$, so by Euler's theorem, $\alpha^{2q} \equiv 1 \pmod{p}$. Then α^q is a square root of $1 \pmod{p}$, so

$$\alpha^q \equiv \pm 1 \pmod{p}. \tag{4}$$

According to Lucas test, α is a primitive root of p if and only if $\alpha^q \not\equiv 1 \pmod{p}$. Combining this with (4), we conclude that α is a primitive root of p if and only if $\alpha^q \equiv -1 \pmod{p}$.

Problem 4: RSA Speedup

Textbook, problem 5.13.

Solution:

(a) We have the following equations:

$$\begin{aligned} d_p &= d \bmod (p-1) && (5) \\ d_q &= d \bmod (q-1) && (6) \\ x_p &= y^{d_p} \bmod p && (7) \\ x_q &= y^{d_q} \bmod q && (8) \\ x &= M_p q x_p + M_q p x_q \bmod n && (9) \end{aligned}$$

Combining (5) and (7) gives

$$x_p = y^{d \bmod (p-1)} \bmod p \tag{10}$$

Since p is prime, $\phi(p) = p - 1$. According to Euler's theorem, if $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod p$, which implies

$$y^d = y^{\lfloor d/(p-1) \rfloor (p-1) + d \bmod (p-1)} \equiv y^{d \bmod (p-1)} \pmod p \tag{11}$$

Combining (10) and (11) gives

$$y^d \bmod p \equiv x_p \pmod p \tag{12}$$

Similarly, from (6) and (8) we can derive

$$y^d \bmod p \equiv x_q \pmod q \tag{13}$$

Therefore, according to Chinese reminder theorem, there is a unique solution for $y^d \bmod p$, which is calculated exactly the same as (9) does. Thus we conclude that the value x returned by this algorithm is in fact $y^d \bmod p$.

(b)

$$\begin{aligned} d_p &= 1234577 \bmod (1511 - 1) = 907 \\ d_q &= 1234577 \bmod (2003 - 1) = 1345 \\ M_p &= 2003^{-1} \bmod 1511 = 777 \\ M_q &= 1511^{-1} \bmod 2003 = 973 \end{aligned}$$

(c)

$$\begin{aligned} x_p &= 152702^{907} \bmod 1511 = 242 \\ x_q &= 152702^{1345} \bmod 2003 = 1087 \\ x &= (777 \times 2003 \times 242 + 973 \times 1511 \times 1087) \bmod (1511 \times 2003) = 1443247 \end{aligned}$$

Problem 5: RSA Insecure Against Chosen Ciphertext Attack

Textbook, problem 5.14

Solution:

Let $y\hat{y} \equiv 1 \pmod n$. Then the multiplicative property implies

$$1 = y\hat{y} \bmod n = e_K(x)e_K(\hat{x}) \bmod n = e_k(x\hat{x} \bmod n) \tag{14}$$

Applying decryption function $D_{K'}(\cdot)$ to both sides of (14) and noting $D_{K'}(1) = 1$, we have

$$1 = x\hat{x} \bmod n \tag{15}$$

Given $\hat{x}$, we can easily compute x using extended Euclidean algorithm.

Problem 6: RSA Common Modulus Failure

Textbook, problem 5.16.

Solution:

(a) We have the following equations:

$$
\begin{aligned}
y_1 &= x^{b_1} \bmod n && (16)\\
y_2 &= x^{b_2} \bmod n && (17)\\
c_1 &= b_1^{-1} \bmod b_2 && (18)\\
c_2 &= (c_1 b_1 - 1)/b_2 && (19)\\
x_1 &= y_1^{c_1}(y_2^{c_2})^{-1} \bmod n && (20)
\end{aligned}
$$

Plugging (17-19) into (20) gives

$$
\begin{aligned}
x_1 &= (x^{b_1 c_1})(x^{b_2 c_2})^{-1} \bmod n\\
&= (x^{b_1 c_1})(x^{b_1 c_1 - 1})^{-1} \bmod n\\
&= x^{b1 c_1 + 1 - b_1 c_1} \bmod n\\
&= x \bmod n\\
&= x && (21)
\end{aligned}
$$

(b) Applying (18-20) gives

$$
\begin{aligned}
c_1 &= 43^{-1} \bmod 7717 = 2692\\
c_2 &= (2692 \times 43 - 1)/7717 = 15\\
x_1 &= (12677^{2692} \times 14702^{-15}) \bmod 18721\\
&= (13145 \times 3947^{-1}) \bmod 18721\\
&= (13145 \times 5668) \bmod 18721\\
&= 15001 && (22)
\end{aligned}
$$