Xueyuan Su
April 4, 2010

Solutions to Problem Set 4

Due on Wednesday, March 24, 2010.

In the problems below, "textbook" refers to Wade Trapp and Lawrence C. Washington, *Introduction to Cryptography with Coding Theory, Second Edition*, Prentice-Hall, 2006.

Problem 1: Divides and mod

Textbook, exercise 3-7.

Solution: Let $\mathcal{P}(n)$ be the multi-set that includes all prime factors of n. For example, $\mathcal{P}(8) = \{2,2,2\}$ and $\mathcal{P}(12) = \{2,2,3\}$.

(a) $ab \equiv 0 \pmod{p}$ implies that $p \mid ab$. Because p is prime, we have either $p \in \mathcal{P}(a)$ or $p \in \mathcal{P}(b)$ (or both). In the first case, $p \mid a$ and thus $a \equiv 0 \pmod{p}$. In the second case, $p \mid b$ and thus $b \equiv 0 \pmod{p}$.

(b) $n \mid ab$ implies that $\mathcal{P}(n) \subseteq \mathcal{P}(ab)$. $\gcd(a,n) = 1$ implies that $\mathcal{P}(n) \not\subset \mathcal{P}(a)$. Therefore, it follows that $\mathcal{P}(n) \subseteq \mathcal{P}(b)$, and thus $n \mid b$.

Problem 2: Chinese Remainder theorem

Textbook, exercise 3-10.

Solution: Assume the smallest number is x. Then we set up the following formulas according to the available information.

$$x \equiv 1 \pmod{3}$$
$$x \equiv 2 \pmod{4}$$
$$x \equiv 3 \pmod{5}$$

Let $n = 3 \times 4 \times 5 = 60$. The above system has the same form as in Chinese remainder theorem and thus has a unique solution in $\mathbf{Z}_n$. Let $N_i = n/n_i$ and $M_i = N_i^{-1} \bmod n_i$, for $1 \le i \le 3$. Using extended Euclidean algorithm to compute M_i, we have

$$N_1 = 20, M_1 = 2$$
$$N_2 = 15, M_2 = 3$$
$$N_3 = 12, M_3 = 3$$

Then $x = \left(\sum_{i=1}^{3} a_i M_i N_i\right) \bmod n = 58$.

Let y be the next smallest number. We know that $y = 58 + 60 = 118$, because $x \equiv y \bmod 60$.

Problem 3: Euler theorem

Textbook, exercise 3-12.

Solution: Because 101 is prime, we have $\phi(101) = 100$. Since 2 is relatively prime to 101, $2 \in \mathbf{Z}^*_{101}$. By Euler's theorem,

$$2^{100} \bmod 101 = 1$$

Let x be the remainder of dividing 2^{10203} by 101. Then

$$x \equiv 2^{10203} \equiv (2^{100})^{102} \times 2^3 \equiv 8 \pmod{101}$$

Thus, $x = 8$.

Problem 4: Order

Textbook, exercise 3-20.

Solution:

(a) $\gcd(a, n) = 1$ implies that $a \in \mathbf{Z}^*_n$. By Euler's theorem, $a^{\phi(n)} \equiv 1 \pmod{n}$. Thus $r \leq \phi(n)$, because r is the smallest positive integer such that $a^r \equiv 1 \pmod{n}$.

(b) $a^m \equiv a^{rk} \equiv (a^r)^k \equiv 1^k \equiv 1 \pmod{n}$.

(c) $a^t \equiv a^{qr+s} \equiv (a^r)^q \times a^s = a^s \pmod{n}$. Because $a^t \equiv 1 \pmod{n}$, we have $a^s \equiv 1 \pmod{n}$.

(d) By definition, r is the smallest positive integer such that $a^r \equiv 1 \pmod{n}$. It follows that $s = 0$ because $a^s \equiv 1 \pmod{n}$ and $0 \leq s < r$. Therefore, $t = qr$ and thus $r \mid t$.

(e) Combining parts (b) and (c) gives that $a^t \equiv 1 \pmod{n}$ iff $\mathrm{ord_n(a) \mid t}$. It follows that $\mathrm{ord_n(a) \mid \phi(n)}$ because $a^{\phi(n)} \equiv 1 \pmod{n}$.

Problem 5: Rabin cryptosystem

Textbook, exercise 3-27.

Solution:

(a)
- Assume $n \nmid m$. Then $m \in \mathbf{Z}^*_n$ and thus x has 4 square roots module n. Thus, each time the machine has a probability of $1/4$ returning the meaningful message m. The expected number of trials is thus 4.
- Assume $p \mid m$ and $q \nmid m$. Then x has 2 square roots module n. Thus, each time the machine has a probability of $1/2$ returning the meaningful message m. The expected number of trials is thus 2.
- Assume $q \mid m$ and $p \nmid m$. The analysis is similar to the previous case and thus the expected number of trails is 2.
- Assume $n \mid m$. Then $x = 0$. This is a special case and thus should be easily decrypted.

(b) A good message m is in $\mathbf{Z}^*_n$. It is hard for Oscar to determine m, because it is believed that there is no feasible algorithm to compute the square root of a number in $\mathbf{Z}^*_n$ without knowing the factorization of n.

(c) Eve chooses $m = 1$ and computes $x = m^2 \bmod n = 1$. Then Eve repeatedly feeds the machine with x until 2 different numbers $a, -a$ are obtained, such that a and $-a$ are not equal to 1 or -1 module n. This is possible because $x \in \mathbf{Z}_n^*$ and thus has 4 different square roots module n. Therefore, $a+1$ and $a-1$ are both non-zero. Since

$$0 \equiv a^2 - 1 \equiv (a+1)(a-1) \pmod{pq},$$

we have either $p \mid (a+1)$ or $q \mid (a+1)$. Without loss of generality, assume $p \mid (a+1)$. Then Eve computes $p = \gcd(a+1, n)$ and $q = n/p$.

Problem 6: Adaptive chosen ciphertext attack against RSA

Textbook, exercise 6-7.

Solution: We know that 2 is relatively prime to n because n is a product of two odd primes. Therefore, $2 \in \mathbf{Z}_n^*$. By Euler's theorem, $2^{\phi(n)} \equiv 1 \pmod{n}$. By the definition of RSA algorithm, $ed \equiv 1 \pmod{\phi(n)}$. Thus, we have

$$(2^e c)^d \equiv (2^e m^e)^d \equiv 2^{ed} m^{ed} \equiv 2m \pmod{n}$$

Let $x = D_d(2^e c \bmod n)$, where D is the decryption function used by Nelson. After obtaining x from Nelson, Eve computes the inverse of 2 module n by the extended Euclidean algorithm. Then Eve computes $m = (2^{-1}x) \bmod n$.

Problem 7: Same modulus attack on RSA

Textbook, exercise 6-16.

Solution: Since e_A and e_B are relatively prime, $\gcd(e_A, e_B) = 1$ and thus $xe_A + ye_B = 1$ for some integers x and y. Using extended Euclidean algorithm to solve this linear Diophantine equation, Eve gets a working pair (x, y). Then we have

$$(c_A)^x (c_B)^y \equiv (m^{e_A})^x (m^{e_B})^y \equiv m^{xe_A + ye_B} \equiv m \pmod{n}$$

Thus, after intercepting c_A and c_B, Eve computes $m = [(c_A)^x (c_B)^y] \bmod n$.

Problem 8: RSA puzzle

Textbook, exercise 6-23.

Solution: Since $\gcd(e, 12345) = 1$, $ex + 12345y = 1$ for some integers x and y. Using extended Euclidean algorithm to solve this linear Diophantine equation, we get a working pair (x, y). Since $m^{12345} \equiv 1 \pmod{n}$, we have

$$c^x \equiv (m^e)^x \equiv (m^e)^x (m^{12345})^y \equiv m^{ex+12345y} \equiv m \pmod{n}$$

Thus, we decrypt m by computing $c^x \bmod n$.