YALE UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

CPSC 467a: Cryptography and Computer Security *Handout #17*
Felipe Saint-Jean *November 9, 2005*

Solutions to Problem Set 4

In the problems below, "textbook" refers to *Introduction to Cryptography with Coding Theory: Second Edition* by Trappe and Washington..

Problem 16: Chinese Remainder Theorem

Textbook, problem 3.13.10.

Solution:

Following the hint the problem can be written as

$$\begin{aligned} n &\equiv 1 \pmod 3 \\ n &\equiv 2 \pmod 4 \\ n &\equiv 3 \pmod 5 \end{aligned}$$

where n is the number of people in the parade. Defining $N_i = \frac{N}{n_i}$ where $N = n_1 n_2 n_3 = 3 \cdot 4 \cdot 5$ we get

$$\begin{aligned} N_1 &= 20 \\ N_2 &= 15 \\ N_3 &= 12 \end{aligned}$$

Now $M_i \equiv N_i^{-1} \pmod{n_i}$ so using the extended Euclid's algorithm to compute the inverses

$$\begin{aligned} M_1 &\equiv 2 \pmod{n_1} \\ M_2 &\equiv 3 \pmod{n_2} \\ M_3 &\equiv 3 \pmod{n_3} \end{aligned}$$

Now the solution is

$$n = \left(\sum_{i=1}^{3} a_i M_i N_i \right) \bmod n = (1 \cdot 20 \cdot 2 + 2 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3) \bmod 60 = 58$$

It is easy to see that 58 is a solution to the original set of equations. Now CRT gives a unique solution mod n so the next solution is $58 + 60 = 118$.

Problem 17: Modular Exponentiation

By making appropriate use of Euler's theorem, the following two problems are readily solved *without use of a computer or calculator*. Solve these problems by hand, and show your work.

(a) Textbook, problem 3.13.12.

(b) Textbook, problem 3.13.13.

Solution:

part 1:

$2^{10203} \pmod{101}$. First notice that $\phi(101) = 100$ so $2^{10203} \equiv 2^{10203 \pmod{100}} \equiv 2^3 \equiv 8 \pmod{101}$ therefore the reminder is 8.

part 2:

The last two digits are $123^{562} \pmod{100}$. $\phi(100) = \phi(2^2 \cdot 5^2) = 100 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{5}) = 40$. So $123^{562} \equiv 123^{562 \pmod{\phi(100)}} \equiv 123^2 \pmod{100} = 29$.

Problem 18: ElGamal Cryptosystem

Textbook, problem 7.6.11. In solving this problem, use the version of the ElGamal cryptosystem that is presented in the book, which differs slightly from the one presented in class.

Solution:

Decryption is done by computing $m \equiv tr^{-a} \pmod{p}$. In this case $t = 6$, $r = 7$, $a = 6$ and $p = 17$. First notice that $7^{-1} \equiv 5 \pmod{17}$ so $tr^{-a} \equiv 6 \cdot 7^{-6} \equiv 6 \cdot 5^6 \equiv 13 \pmod{17}$. Therefore $m = 12$.

Problem 19: Finding Square Roots

Textbook, problem 3.13.25.

Solution:

Part a:

First let's find the square roots mod the factors of $143 = 11 \cdot 13$. Notice that $133 \equiv 1 \pmod{11}$ so the square roots are trivially 1 and -1. Now $133 \equiv 3 \pmod{13}$. Using brute force we can get that $4^2 \equiv 3 \pmod{13}$ so -4 and 4 are square roots. Notice that there are efficient ways of computing square roots when $p \not\equiv 3 \pmod{n}$ but they were not covered in class and are not in the book. Combining the previous results using the CRT we get the four square roots. The first system

$$\begin{aligned} r_1 &\equiv 1 \pmod{11} \\ r_1 &\equiv 4 \pmod{13} \end{aligned}$$

gives that $r_1 \equiv 56$,

$$\begin{aligned} r_2 &\equiv -1 \pmod{11} \\ r_2 &\equiv 4 \pmod{13} \end{aligned}$$

gives that $r_2 \equiv 43$,

$$\begin{aligned} r_3 &\equiv 1 \pmod{11} \\ r_3 &\equiv -4 \pmod{13} \end{aligned}$$

gives that $r_3 \equiv 100$, and

$$\begin{aligned} r_4 &\equiv -1 \pmod{11} \\ r_4 &\equiv -4 \pmod{13} \end{aligned}$$

gives that $r_4 \equiv 87$.

Part b:

Now we want the square roots of $77 \pmod{143}$. We sill find only two square roots because $77 \equiv 0 \pmod{11}$ so 77 has only one square root $\pmod{11}$ and that is 0. Modulo 13, 77 has ± 5 as a square root. Using the CRT we can solve the systems and get the two square roots:

$$\begin{aligned} r_1 &\equiv 0 \pmod{11} \\ r_1 &\equiv 5 \pmod{13} \end{aligned}$$

gives that $r_1 \equiv 44$, and

$$\begin{aligned} r_2 &\equiv 0 \pmod{11} \\ r_2 &\equiv -5 \pmod{13} \end{aligned}$$

gives that $r_2 \equiv 99$.

Problem 20: Blum Primes

Show that -1 is a quadratic residue modulo an odd prime p iff $p \equiv 1 \pmod{4}$.
[Hint: Apply the Euler criterion.]

Solution:

($\Rightarrow$) If -1 is a quadratic residue modulo p, then

$$(-1)^{(p-1)/2} \equiv 1 \pmod{p}.$$

But $-1 \cdot -1 \equiv 1 \pmod{p}$ so $(p-1)/2$ has to be even. Thus $4 \,|\, (p-1)$ so $p \equiv 1 \pmod{4}$.

($\Leftarrow$) If $p \equiv 1 \pmod{4}$ then $(-1)^{(p-1)/2} \equiv 1$ because it is -1 raised to a even power. Therefore -1 is a quadratic residue modulo p.

Problem 21: Rabin Cryptosystem

Textbook, problem 3.13.27.

Solution:

part a:

There are at most 4 square roots to the ciphertext, so if the machine chooses one randomly we can expect the correct one after 4 attempts on average.

part b:

Factoring is equivalent to finding all square roots. Since factoring is believed to be hard, so is the problem of finding square roots.

part c:

Choosing 1 as the ciphertext, with probability $1/2$ we will get a non-trivial square root of 1. Using that square root we can factor n and from then on decrypt every message. Notice that that makes the Rabin Cryptosystem weak against chosen ciphertext attacks.