YALE UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

CPSC 467a: Cryptography and Computer Security *Handout #19 (rev. 2)*
Felipe Saint-Jean *November 17, 2005*

Solutions to Problem Set 5

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

Problem 22: Factoring RSA Modulus

Alice's public RSA key is $n = 3737, e = 77$. Eve discovers that $d = 3413$. Use the method of lecture notes 12, section 1.3, to factor n. You may use a calculator or computer if you wish, but you should show the steps of the algorithm in finding the factors.

Solution:

$ed - 1 = 262800$ that written in binary is 1000000001010010000. Using the notation in the lecture notes, we have $s = 4$ and $t = 16425$ so that $ed - 1 = t2^s$ with t odd. Now let's choose a random a, say $a = 978$. Therefore $b_0 \equiv a^t \equiv 1000 \pmod{n}$.

b_0	1000
b_1	2221
b_2	1

Thus we found a non-trivial square root of $1 \pmod{n}$ because $2221^2 \equiv 1 \pmod{n}$. Now $\gcd(2221 - 1, 3737) = 37$. Therefore, 37 is a factor of n.

Problem 23: Solving Diophantine Equations

Textbook, problem 3.14.2 (computer problem).

Solution:

part a

Using the extended Euclid's Algorithm, we get that $65537 \times (-1405) + 3511 \times 26226 = 1$.

part b

Multiplying the above result times 17, we get $65537 \times (-23885) + 3511 \times 445842 = 17$.

Problem 24: Finding Primitive Roots

Textbook, problem 3.13.21.

Solution:

part a

Any number r that divides 600 is the product of some subset of $S = (2, 2, 2, 3, 5, 5)$. If $r < 600$ then it is a subset of size at most 5. S has 3 unique subsets of size 5 that give the numbers 300, 200, and 120. Any subset of size 5 or less has to be a subset of one of those three therefore dividing one of 300, 200, or 120.

part b

We know, from Lagrange's Theorem, that $\mathrm{ord}(7) \mid \phi(601)$. If $\mathrm{ord}(7) < 600$ using part a it has to divide one of 300, 200 or 120.

part c

If $\mathrm{ord}(7) \,|\, k$ then $\mathrm{ord}(7) \cdot m = k$ for some m. Then

$$7^k \equiv 7^{\mathrm{ord}(7)\cdot m} \pmod{601}.$$

Since, by definition, $7^{\mathrm{ord}(7)} \equiv 1 \pmod{601}$ then $7^k \equiv 1 \pmod{601}$. So going back to the question, at least one of the values would be 1 and none is.

part d

Because $\mathrm{ord}(7) \,|\, 600$, by contradiction, if we assume that $\mathrm{ord}(7) < 600$, then it has to divide 300, 200 or 120. But in part c we showed that it is not true. Therefore, $\mathrm{ord}(7) = 600$ being that the definition of a primitive root.

part e

To test if a number a is a primitive root of n we have to verify that

$$a^{\frac{\phi(n)}{q_i}} \not\equiv 1 \pmod{n}$$

for all q_i distinct prime divisor of $\phi(n)$.

Problem 25: Legendre Symbol

Textbook, problem 3.13.29.

Solution:

part a

$\left(\frac{123}{401}\right) = 123^{\frac{401-1}{2}} \pmod{401} \equiv -1$. Therefore there is no solution.

part b

$\left(\frac{43}{179}\right) = 43^{\frac{179-1}{2}} \pmod{179} \equiv 1$. Therefore yes, there is a solution.

part c

$\left(\frac{1093}{65537}\right) = 1093^{\frac{65537-1}{2}} \pmod{65537} \equiv -1$. Therefore no, there is no solution.

Problem 26: Jacobi Symbol

Textbook, problem 3.13.30.

solution:

part a

If a has a a square root r then $r^2 \equiv a \pmod{n}$. Because $\gcd(r^2, n) = 1$, using rule 2 for Jacobi symbols,

$$\left(\frac{r^2}{n}\right) = \left(\frac{r}{n}\right)^2 \neq -1.$$

Therefore it can't be that a has a square root. This proof was submitted by Doug Swanson as part of his solution and I found it to be much more elegant than mine.

part b

$\left(\frac{3}{35}\right) = \left(\frac{3}{5}\right)\left(\frac{3}{7}\right)$. Also $\left(\frac{3}{5}\right) = -1$ and $\left(\frac{3}{7}\right) = -1$ thus $\left(\frac{3}{35}\right) = 1$.

part c

If $a^2 \equiv 3 \pmod{35}$ then, since $5 \mid 35$, $a^2 \equiv 3 \pmod{5}$ but we know that 3 has no square roots $\pmod{5}$ because $\left(\frac{3}{5}\right) = -1$.