Institut for Matematik og Datalogi
Syddansk Universitet

November 14, 2016
JFB

Cryptology – E16 – Assignment 3

Assignment due Monday, November 28, 12:15

Note that this is part of your exam project, so it must be approved in order for you to take the exam in January, and you may not work with others not in your group. If it is late, it will not be accepted (though it could become an assignment you redo). You may work in groups of two (or three). Turn in the assignment through the SDU Assignment system in Blackboard, and remember to keep your receipt. Turn in one PDF file per group.

1. Even assuming that the primality test is executed several times, there is still a small probability of choosing a number which is not prime. Suppose the modulus N computed for RSA is the product of p and q, and the p chosen is prime, but q is not.

   (a) Suppose q is a Carmichael number. (Recall that a *Carmichael number* is a composite integer n such that for all $x \in \mathbb{Z}_n^*$, $x^{n-1} \equiv 1 \pmod{n}$.) Would encryption and decryption with N using RSA still work properly? Prove your answer. (Hint: try using the Chinese Remainder Theorem. Assume that the other parts of the keys are correctly calculated as defined by RSA from p and q.)

   (b) Suppose q is a not a Carmichael number. Would encryption and decryption with N still work properly using RSA? Prove your answer. (Hint: try using the Chinese Remainder Theorem.)

   (c) What other problem could exist if q is a composite number?

2. Show all steps in the calculations of the Jacobi symbol $\left(\frac{57}{99}\right)$, using the standard algorithm (using the four properties of the Legendre symbol given in the textbook).

3. Suppose the naive RSA algorithm is used to send the same message, m, to three different uses, with public keys $(15671917, 3)$, $(15484081, 3)$, and $(15672781, 3)$. Suppose the messages are 1767332, 2068137, and 331460, respectively. What is the message m? Use the technique in the textbook and show your work. (Assuming you use something like Maple for some of your calculations, you can just write the result and say that is what you used. Also for the next problem.)

4. Suppose the naive RSA algorithm is used to send the same message, m, to three different uses, with public keys $(15671917, 3)$, $(15484081, 3)$, and $(15460399, 3)$. Suppose the messages are 11467349, 1983665, and 6704277, respectively. What is the message m? Why should you use a different technique from that in the previous problem? Use a reasonable technique (not brute force) and show your work.

5. Run the Rabin-Miller primality test on 561, and show how you use the execution to actually factor 561.

6. Consider the following algorithm for finding square roots modulo a prime $p \equiv 5 \pmod 8$.

```
procedure SquareRoot($p, a$):
{ Input: A prime $p \equiv 5 \pmod 8$; a quadratic residue $a \pmod p$ }
{ Output: $x$ such that $a \equiv x^2 \pmod p$ }

    $q \leftarrow (p-1)/4$
    if ($a^q \equiv 1 \pmod p$) then return $a^{(q+1)/2} \pmod p$
    else return $a^{(q+1)/2} \cdot 2^q \pmod p$
```

   (a) Try this algorithm on $p = 29$ and $a = 22$.

   (b) Show why the algorithm behaves correctly when it executes the **then** part of the **if** statement.

   (c) Suppose $a = z^2 \pmod p$. Substitute this into the result computed in the **else** part of the **if** statement. Show that the result returned there is also correct.