NTNU Department of Information Security and Communication Technology

TTM4135 Applied Cryptography and Network Security
Semester Spring, 2023

Worksheet 5: RSA

QUESTION 1

Review the definitions of the following concepts. They are things that you would be expected to know in the exam.

(a) trapdoor oneway function;

(b) RSA equations;

(c) RSA padding;

(d) prime number theorem;

(e) square-and-multiply algorithm;

(f) Håstad's attack;

(g) Miller's theorem.

QUESTION 2

Suppose that an RSA public key is chosen with primes $p = 13$ and $q = 17$. Suppose that the public key $e = 5$ is used.

(a) Find the value of d.

(b) Find the ciphertext value for $M = 4$ and $M = 13$.

(c) Decrypt the ciphertext and verify that the correct value is recovered.

QUESTION 3 Challenge Question

In this question we show that $f(x) = x^2 \bmod n$ is a trapdoor one-way function, when $n = pq$ and $p \bmod 4 = q \bmod 4 = 3$ and p and q are different primes. We do this in three steps.

(a) Suppose that $x \equiv y^2 \bmod p$ for some y. Then show that $x^{(p+1)/4} \bmod p$ is a square root of x in $\mathbb{Z}_p^*$.

(b) Use the part above to show that if p and q are known, then a square root modulo n can be efficiently computed (assume we have an efficient exponentiation function). Thus p and q are a trapdoor to invert f.

(c) Now suppose that there exists an algorithm A to find square roots modulo n. Show that if you know y so that $x \equiv y^2 \bmod n$ and A finds a different square root z with $z \neq x \bmod n$ and $z \neq -x \bmod n$, then this can be used to factorise n. Hence deduce that inverting f is as hard as factorising n so that f is one-way.

QUESTION 4

Suppose that RSA encryption uses a modulus n of 3000 bits. Assuming that the square-and-multiply method is used for exponentiation, compare the computational cost of encryption, measured in the number of squarings and the numbers of multiplications, in the following cases:

(a) $e = 3$

(b) $e = 2^{16} + 1$

(c) e is chosen randomly between 0 and n.

How much computation is required for decryption in each case?

QUESTION 5

Suppose that the same message m has been encrypted for three recipients with different RSA moduli: 205, 319 and 391. Each recipient uses public exponent $e = 3$. Suppose also that no random padding has been added. The three ciphertexts found are: 180, 43 and 218 respectively.

Demonstrate Håstad's attack by finding the value of m without making use of the factorisation of the moduli.

QUESTION 6

Consider RSA with values $p = 23$, $q = 31$, $n = 713$ and $d = 233$. Suppose the received ciphertext is $C = 266$.

Examine the faster decryption method using the Chinese Remainder Theorem, using these values:

(a) Compute $M_p = C^{d \bmod p-1} \bmod p$.

(b) Similarly compute M_q.

(c) Combine these results using the Chinese Remainder Theorem and show that the result is correct.

QUESTION 7

Suppose that an attacker obtains an RSA private key $d = 233$ and also has the public key $e = 17$ and $n = 713$. Apply Miller's algorithm to factorise n.

QUESTION 8

Suppose that you know that two RSA moduli $n_1 = 1517$ and $n_2 = 1591$ share one factor. Use this knowledge to efficiently factorise both numbers. (Do not try to factorise both directly.)

QUESTION 9

Slide 38 of Lecture 9

Use the diagram on ~~Slide 34 of Lecture 10~~ to write down two equations for outputs t and s when computing the OAEP padding algorithm from a message m. Hence show that the OAEP padding can be inverted by anyone (without using any secret) to recover m.