Institut for Matematik og Datalogi
Syddansk Universitet

October 11, 2019
JFB

Cryptology – 2019 – Lecture 9

Announcements

1. All lectures on Thursdays will start at 16:10, instead of 16:15.
2. Lectures on Thursday, October 24, and Thursday, November 21, are cancelled.
3. There will be a Cyber Security Challenge which you can sign up for until October 16: https://challenges.dk/da/challenge/cyber-security-challenge-2019. This is not part of the course.

Lecture, October 1

We began on chapter 14, covering up through section 14.4.2.

Lecture, October 7

We will finish chapter 14, including section 11.7.3 for security of MACs, and cover section 11.4.

Lecture, October 10

We will review RSA, cover Rabin's encryption scheme (subsection 15.1.1), and cover subsections 2.2. We may also cover sections 1.3.5, 1.3.6 and 1.3.9 from chapter 1.

Problem session October 21

1. Suppose you as a cryptanalyst intercept the ciphertext $C = 10$ which was encrypted using RSA with public key $(n = 35, e = 5)$. What is the plaintext M? How can you calculate it?

2. In an RSA system, the public key of a given user is $(n = 3599, e = 31)$. What is this user's private key?

3. With RSA, there have been recommendations to use a public exponent $e = 3$.

   (a) What would the advantage to this be?

   (b) If $e = 3$, the two prime factors dividing the modulus, p and q, must be such that $p \equiv q \equiv 2 \pmod 3$. Why is it impossible to have one or both of p and q congruent to 0 or 1 modulo 3?

   (c) Suppose that $e = 3$, $p = 3r + 2$ and $q = 3s + 2$. What would the decryption exponent d be?

   (d) Check the calculations in the example in section 15.3.4 of the textbook.

4. Suppose the modulus used in RSA has 1024 bits. What is the unicity distance of this RSA cryptosystem? Why?

5. The proof of correctness (that decrypting gives the original message as the result) that I presented on my slides only held for messages in $\mathbb{Z}_n^*$. What happens with messages not in $\mathbb{Z}_n^*$ and why?

6. Section 15.3.3 shows an attack on the use of a shared modulus. Suppose the shared modulus is 1763 and some user has sent the same message to two users, using public exponents $e_1 = 511$ and $e_2 = 1021$.

   Case 1: Let $c_1 = 165$ and $c_2 = 196$. What do you get? Is this correct? What happened?

   Case 2: Let $c_1 = 952$ and $c_2 = 196$. What do you get? Is this correct? Think about what t_2 is.

7. In the proof of Lemma 15.4, the adversary creates a ciphertext $c = 2^e \cdot c^*$ to be decrypted. For an random $m \in \mathbb{Z}_N^*$, it can choose $c = m^e \cdot c^*$ instead, giving a random ciphertext. What would it do then?

8. Suppose $n = 11,820,859$ is an RSA modulus. Suppose you know $\phi(n) = 11,813,904$. Find the factors of n. Show your work. (You may use Maple to solve the quadratic equation, but explain how you used it.) See section 15.3.2.

9. Suppose that $p = 2q+1$, where p and q are odd primes. Suppose futher that $\alpha \in \mathbb{Z}_p^*$, $\alpha \not\equiv \pm 1 \pmod{p}$. Prove that α is a primitive element modulo p (generator) if and only if $\alpha^q \equiv -1 \pmod{p}$. (Problem 5.9 in CTP.)

10. We may do a midway course evaluation at the end.