Academic Year: Winter Semester 2021/22

6090: Security of Computer and Embedded Systems

Problem Sheet 7

Cryptographic Foundations Part 2

In this problem sheet, we will deepen our knowledge of asymmetric cryptographic schemes. In particular, we will have a closer look on RSA and also develop an understanding of crypto attacks.

1. Crypto Concepts

This section contains a couple of multiple-choice questions covering the basic concepts of cryptography. You might want to review the lecture slides and read Section 5.1 and Section 5.2 of Anderson [1] before working on these questions.

Exercise 1: *Crypto Concepts*

1. What makes a one-way function computationally feasible?
   - ☐ Key
   - ☐ Cipher
   - ☐ Trapdoor
   - ☐ Inversion
2. In asymmetric encryption, the public key is used for
   - ☐ Decrypting a message
   - ☐ Encryption and decryption
   - ☐ Encrypting a message
   - ☐ None of the mentioned
3. Which of the following are asymmetric encryption schemes?
   - ☐ DES
   - ☐ RSA
   - ☐ AES
   - ☐ ECC
   - ☐ ROT13
4. Which of the following are properties of public-key encryption schemes?
   - ☐ They are usually faster than symmetric encryption schemes
   - ☐ Participants need to agree on a pre-shared secret
   - ☐ A key is a pair of a public and a secret key
   - ☐ They are used as part of SSL/TLS (and, thus, https)

2. Cryptographic Hash Functions

In this section, we will deepen our understanding of cryptographic hash functions.

Exercise 2: *Hash Functions*

A hash function h maps an input x of an arbitrary bit length to an output $h(x)$ of fixed bit length n.

This process is called hashing in order to compress a message to generate a fingerprint.

$h(x)$ is a "cryptographic" function if it has certain additional properties.

Define these properties.

3. Asymmetric Encryption

In the following exercises, we will deepen our knowledge of public-key cryptography in general and RSA in particular. Thus, it is recommended to read Chapter 19 of Schneier [3] for an overview as well as the details in Chapter 8 of Menezes et al [2].

Exercise 3: *Extended Euclidean Algorithm*

To compute the key pair for RSA, we need to find a d (with $1 < d < \Phi$) such that

$$e \cdot d \bmod \Phi = 1$$

This is called the *multiplicative inverse*. It can be computed with the Extended Euclidean Algorithm. We will now develop this algorithm.

1. Let $\gcd(a, b)$ be the greatest common divisor of a and b. Convince yourself that

   $$\gcd(a, b) = \gcd(b, a \bmod b)$$

   holds for all non-negative integers a and b.

2. The Euclidean Algorithm for computing the greatest common divisor is based applying the equation $\gcd(a, b) = \gcd(b, a \bmod b)$ until b equals 0, e.g.,

   $$\gcd(30,21) = \gcd(21,9) = \gcd(9,3) = \gcd(3,0) = 3$$

   Define algorithm $\gcd(a, b)$ in pseudocode (or similar to a programming language that you know).

3. Modify the Euclidean Algorithm so that it returns a triple (d, x, y) that satisfies the equation

   $$d = \gcd(a, b) = ax + by$$

   Hints:

   - For $b = 0$, we need to return $(a, 1,0)$ to satisfy $a = a \cdot 1 + 0$
   - To compute x and y in the recursion, make use of the following fact:

     $$d = bx' + (a - \left\lfloor \frac{a}{b} \right\rfloor b)y' = ay' + b(x' - \left\lfloor \frac{a}{b} \right\rfloor y')$$

4. Use the Extended Euclidean Algorithm to find a d such that

   $$33 \cdot d \bmod 40 = 1$$

Exercise 4: *RSA – Generating Keys*

Bob wants to generate an RSA key-pair for himself. He starts by choosing the "large" prime numbers $p = 11$ and $q = 5$.

Continue the generation of the RSA key pair for Bob (Hint: you might want to reuse the results of the last exercise).

Exercise 5: ***RSA – Encryption/Decryption***

Recall the RSA algorithm discussed in the lecture. Furthermore,

- Alice's public key is $(n_a, e_a) = (55, 33)$, her private key is $d_a = 17$
- Bob's public key is $(n_b, e_b) = (39, 5)$, his private key is $d_b = 5$

Consider the following scenarios:

1. Bob wants to send the message "**`geheim`**" to Alice. Encode the letters by their position in the alphabet (e.g., the letter "**`a`**" is represented by the number 1) and compute the cipher text.
2. Alice sends the following encrypted message to Bob:

$$28, 5, 9, 18, 5, 11$$

Decrypt the message. Again, the numbers represent the letters by their position in the alphabet.

3. Did you observe anything strange or suspicious?

References

1. Ross J. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. John Wiley & Sons, Inc., New York, NY, USA, 1st edition, 2001. The complete book is available at: http://www.cl.cam.ac.uk/~rja14/book.html
2. Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. Handbook of Applied Cryptography. CRC Press, Inc., Boca Raton, FL, USA, 5th edition, 2001. The complete book is available at: http://cacr.uwaterloo.ca/hac/
3. Bruce Schneier. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.