Université Libre de Bruxelles
Faculté des Sciences

January 23, 2019

INFO-F-405 Introduction to cryptography

This assessment has to be realized without the use of personal notes, books or any other support. You may use a calculator (but it is not required). You have to justify and detail each of your answers. Indicate your name, first name and year of study on every answer sheets. The answers to the questions should be on different answers sheets (on sheet per question).

Question 1: 2-DES and 3-DES

Explain and give the complexity of the exhaustive search of the keys for the 2-DES construction $E_{k_2}(E_{k_1}(x))$ and for the 3-DES construction $E_{k_3}(E_{k_2}(E_{k_1}(x)))$.

Question 2: Rabin cryptosystem

Key generation: p and q are two prime numbers, $n = pq$, the public key is n, the private key is (p, q)

Encryption: $E(x) = x^2 \bmod n$

Decryption: $D(y)$ is one of the four square roots of y modulo n

In the two following subquestions, the given numbers are artificially small, therefore exhaustive searches of the solutions will of course not be accepted.

Question 2.1

Let F be a blackbox such that given a ciphertext encrypted for Alice with Rabin (without redundancy), F outputs efficiently one of the corresponding plaintexts.

If $F(36) = 28$, and if the public key of Alice is $n = 187$, compute (in details) what are the elements of the private key of Alice.

Question 2.2

Let (11,13) be the private key of Bob, let $y = 53$ be a ciphertext intended for Bob, compute (in details) what are the possible corresponding plaintexts.

Question 3: Key management

Explain in details what are the differences and particularities of the keys management in symmetric cryptography and in asymmetric cryptography.

Question 4

Let f be an idealized collision resistant hash function. Discuss whether the following functions h_i are also collision resistant:

1. $h_1(x) = f(x^2)$
2. $h_2(x, y) = f(x) \oplus y$
3. $h_3(x, y) = f(f(x) \oplus y)$
4. $h_4(x) = f(\mathsf{AES}_k(x))$ for $k = \mathbf{0}$
5. $h_5(x) = f(3x + 1)$
6. $h_6(x) = \sin(f(x))^2 + \cos(f(x))^2$
7. $h_7(x, k) = f(k)||\mathsf{AES}_k(x)$
8. $h_8(x, k) = f(k^2)||\mathsf{AES}_k(x)$

A yes/no answer is worthless, you have to show that either you can find a collision, or that it is not possible following collision resistance of f.

Question 5

The Innovative Autonomous Car Renter (IACR) is a company proposing a rental service of self-driving cars communicating over the internet. Any user registered possess a smartcard with a secret key associated to a public key corresponding to the identity of the costumer. Once in a car, the user willing to drive to a place $\mathcal{P}$ will first insert their card into the car and enter their PIN code to unlock the secret key. Then, the car will communicate with the central authority to ask whether this user is authorized to go to $\mathcal{P}$. Once the journey is finished, the car will send a report to the central authority to process billing information. The IACR focuses on privacy and does not want to reveal where its costumers are traveling. Obviously, it also wants its system to be fair, meaning that only an authorized costumer can use the service and that billing information are not modified by a third party.

We ask you to explain what cryptographic algorithms can be use the ensure the security of such a system and to sketch the communications (from the smartcard to the car and from the car to the authorization server). For each type of crypto algorithm you use (hash, encryption, key exchange, ...), you will give an example of a suitable real-life algorithm.