*C. Olivier-Anclin*

# Session 1 - Introduction

**Exercise 1 (False or false.)**
Explain why each of the following statements is wrong.

1. It is safe to store user passwords in plaintext if the server always uses HTTPS.
2. A block cipher with keys of 512 bits is always secure.
3. There will never be any technological reason to use block-cipher keys larger than 128 bits.
4. One should always use block-cipher keys larger than 128 bits.
5. One should always use the latest-published, most recent block cipher.

**Exercise 2 (Brute-force attack)**

1. How many different passwords having exactly 8 characters, knowing that only alphanumeric, - and _ characters are used, are there? Explain your computation and give the result in the form of a power of 2.
2. How many passwords of 8 characters are there, assuming that all 128 ASCII characters can be used? Explain your computation and give the result with power of 2.
3. We assume that we need 1 day to perform a brute-force attack on a password satisfying properties of question 1. How many days do we need to perform a brute-force attack on a password satisfying properties of question 2?
4. Assuming that the authentication process does not use salt in the computation of the hash, which method can be advised to break passwords more efficiently that the brute-force attack does?

**Exercise 3 (Does Double Encryption Increase Security?)**
Consider a symmetric encryption scheme $E_k^2(\cdot)$ with a key $k = k_1 \| k_2$. The double encryption of a message $m$ is defined as:

$$c = E_{k_2}(E_{k_1}(m))$$

where $k_1$ and $k_2$ are two independent keys.

Does encrypting a message twice with two different keys necessarily make the encryption more secure than a single encryption with $E$? Justify your answer.

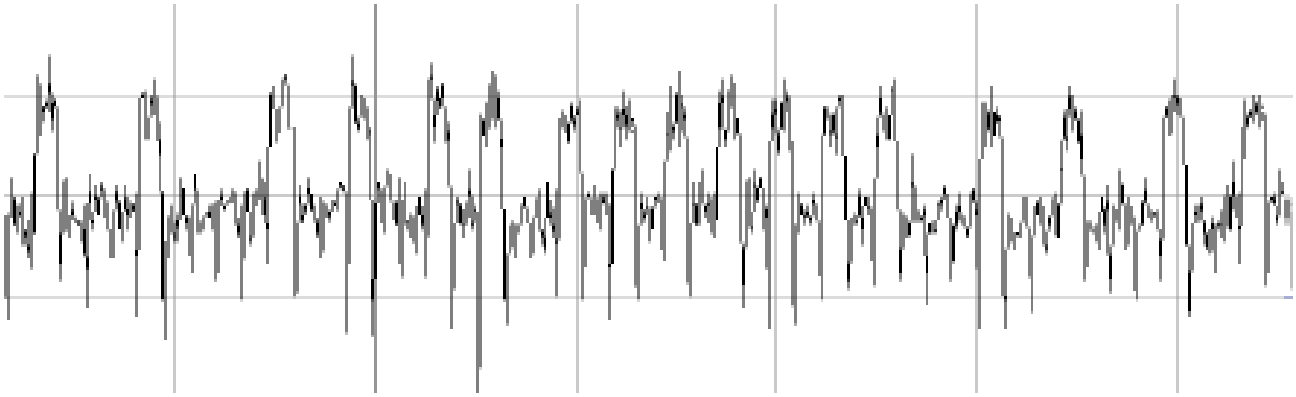
**Exercise 4 (Power Attack on RSA Signature)**
The *Square and Multiply* algorithm allows to compute $a^d \mod n$, for $d \in \mathbb{N}$, it works as follows.

**Input:** $a$, $d$, $n$
**Output:** $a^d \mod n$
Convert $d$ to binary $k_s k_{s-1} \dots k_1 k_0$
$b \leftarrow 1$
**for** $i = s, i >= 0, i$-- **do**
  $b \leftarrow b \cdot b \mod n$
  **if** $k_i = 1$ **then**
    $b \leftarrow b \cdot a \mod n$
**return** $b$.

1. Run manually the square and multiply algorithm to compute $a^d \mod n$ with $a = 2$, $d = 11$, and $n = 21$.

2. With the appropriate tool, we can measure the electricity consumption of a cheapset that performs a RSA signature using the private key $d$.

   Knowing that a modular multiplication consumes more than a modular square multiplication, give the binary value of the private key $d$ (32 bits) using the following trace of a signature.



3. Recover the private key in hexadecimal.

**Exercise 5 (Generation of OpenPGP keys)**
Before exchanging with other persons using PGP, the first step consists in the generation of the encryption and signature keys. Explain the following facts:

1. The encryption and signature keys generation process can take several seconds.
2. The key generation process can change very significantly (twice as long) between two executions.
3. PGP can ask to move computer's mouse and to randomly type on the keyboard.

**Exercise 6 (Threat analysis)**
A company observes that each year, they undergo 5 virus attacks and 3 website disfigurements. Each reconditioning needs 2 days of work by the administrator, at a cost of 2,000 euros. The website can be fixed in a few hours, for 500 euros. The maintenance of an antivirus product and a protection system would cost 30 000 euros by year.

1. Compute the yearly cost of both threats and compare it to the maintenance cost of an antivirus and protection system.
2. Criticize the computation of the threat cost and propose a better method.

**Exercise 7 (Social engineering)**
Assume that you want to take over a Twitter account. While you know the victim's email, you do not manage to break its password. After some engineering, you find your victim's Paypal account, his Facebook account, his website and his website hosting company.

Calling Paypal and pretending to be an employee, you retrieve the last 4 digits of the credit card. However, any action involving the website host requires at least the last 6 digits of the credit card to authenticate via the hotline.

Give a strategy allowing you to retrieve full possession of the Twitter account.