ECAM
BRUSSELS ENGINEERING SCHOOL

Winter 2020
Sébastien Combéfis

SE507μ Hacking Password Hashes with Rainbow Tables

Quizz 1: Secure password storage

This assessment evaluates the following competencies:

- *CS007 – Understand why it is important to store passwords carefully*
- *CS210 – Understand how passwords can be stored securely in databases*
- *CS109 – Understand what is a cryptographic hash function*

Three affirmations are given for each assessed competency. For each of them, you have to decide whether it is true or false. To get a star for the competency, you must have the correct answer for the three affirmations.

CS007	**True**	**False**
A password stored in a file or in a database can never be found by anyone.	☐	☐
A password is only used to identify a user on a system.	☐	☐
A password can never be shoulder sniffed, it is always safe regarding this kind of attack.	☐	☐

CS210	**True**	**False**
It is a bad practice to store a password in clear (that is, not encrypted) in a database.	☐	☐
It is important to use a very fast hash function to store securely passwords in a database.	☐	☐
It is always easy to reverse a hashed password stored in a database, that is, finding the corresponding clear password.	☐	☐

CS109	**True**	**False**
A hash function can be used to check for data integrity.	☐	☐
Given a hash function $h_K(\cdot)$ and a fingerprint $y = h_K(x)$, it is easy to find x.	☐	☐
It is never possible that two different values x_1 and x_2 result in the same fingerprint, that is, $h_K(x_1) = h_K(x_2)$.	☐	☐