ECAM
BRUSSELS ENGINEERING SCHOOL

Fall 2019
Sébastien Combéfis

I5020 Computer Security

Quizz 2: Cryptography

This assessment evaluates the following competencies:

- *CS104 – Encrypt and decrypt messages with "historical" ciphers*
- *CS101 – Make connections between cryptographic tools and the CIA triad*
- *CS102 – Compare symmetric and asymmetric encryption schemes*
- *CS401 – Identify vulnerabilities in a system and propose countermeasures for them*
- *CS005 – Identify residual risks that come from a countermeasure*
- *CS107 – Understand how RSA can be used as an encryption and as a signature scheme*

Three affirmations are given for the five last assessed competencies. 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.

CS101	**True**	**False**
Message authentication codes (MAC) may be used to satisfy the C of the CIA triad.	☐	☐
It is impossible to work on the C of the CIA triad with cryptographic tools.	☐	☐
Symmetric encryption is way more efficient than asymmetric encryption when it is to ensure the C of the CIA triad in a system.	☐	☐

CS102	**True**	**False**
Asymmetric encryption is faster than symmetric encryption.	☐	☐
Symmetric encryption may need to have a secure channel before starting to communicate.	☐	☐
More keys are needed by symmetric encryption compared to asymmetric encryption.	☐	☐

CS401	**True**	**False**
The data that are stored in my database have been stolen several times. To better protect their confidentiality, I can use encryption.	☐	☐
Each time that my customers are downloading files on my application, they are corrupted. To be able to detect such a situation on the application, I can use a signature scheme.	☐	☐
For now, when customers want to securely connect to my application, they have to come to my office for me to install a key on their computer. To avoid this process, I can use a symmetric encryption.	☐	☐

CS005	**True**	**False**
One of the main drawbacks of introducing encryption is that I will have to think about key management.	☐	☐
Encrypting the content of a hard drive, to protect it from thefts, does not have any side effects nor residual risk.	☐	☐
Using encryption does not have any effects on the performance or on the speed of the communication process.	☐	☐

CS107	**True**	**False**
The RSA cryptosystem can be used as a signature scheme.	☐	☐
When using RSA as a signature scheme, the private key corresponds to the $sig_K(\cdot)$ function and the public key to the $ver_K(\cdot)$ function.	☐	☐
The trapdoor of the RSA cryptosystem is the fact that $d_K(\cdot)$ has a very large time complexity.	☐	☐

For the first assessed competency (CS104), you have to encrypt a plaintext $x_1 =$"`ASSESS`" and decrypt a ciphertext $y_2 =$"`PNQFJL`" using the Vigenère cipher with the following parameters: $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{26})^6$ and $K =$"`SECRET`". Give some details about your reasoning and write down the e_K and d_K functions.