Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Sergio Pastrana Portillo
UC3M | GRUPO COMPUTER SECURITY LAB (COSEC)

Introduction to cryptosystems

Self-assessment test

Select the correct answer.

1. Choose the correct answer:
   - The classic definition of cryptography includes methods and techniques to prevent the unauthorized modification of information.
   - The classic definition of cryptography is concerned about information availability.
   - **The modern definition of cryptography includes ways to avoid data repudiation.**
   - Definitions of cryptography (classic and modern) point out the need of protecting data, not transforming it.

2. In a cryptosystem …
   - Keys do not exit.
   - There are a pair of keys necessarily different.
   - There is a key, that is shared between both parties, sender and receiver.
   - **There are a pair of keys, that may be the same.**

3. Cryptographic systems are classified by…
   - The type of operations: contractions and expansions.
   - The number of keys: basic and extended.
   - **The way of processing data to be encrypted: by blocks or streams.**
   - Its reversibility: reversible or irreversible.

4. According to Kerchkoff's principle,
   - **The security of a cryptosystem should be based, exclusively, on keeping the key secret.**
   - The security of a cryptosystem should be based on the secret of its design.
   - The security of a cryptosystem should depend on the randomness of cleartext messages.
   - The security of a cryptosystem should be based on the complexity of its operations.

5. The goal of cryptanalysis is:
    - Decrypt a given text.
    - Impersonate a legitimate sender.
    - **Recover the decryption key**.
    - Gain fame and obtain recognition, exclusively.

6. Regarding cryptanalysis attacks to the algorithm:
    - The easiest one is the chosen plaintext.
    - **In the chosen plaintext attack messages are encrypted with the same key.**
    - The cyphertext-only is the easiest one, because it is the only one in which the attacker knows the algorithm.
    - In the known-plaintext attack, the attacker chooses one or more cryptograms and encrypts them with different keys.

7. Vernam cipher:
    - **Is unconditionally secure if, among other issues, the encryption key is random.**
    - Is computationally secure, but not unconditionally secure.
    - Is unbreakable if the encryption key is random and it is used only once.
    - It is impractical because it encrypts bit by bit and it will be extremely slow.

8. A brute-force attack:
    - **Half of possible keys should be tested, on average, to succeed.**
    - If the key length is of 128 bits, the attack can be performed in less than an hour with a conventional computer.
    - Breaking a 26 characters key is feasible in just a few years using parallel processing.
    - Even if the key is of 32bits, a brute-force attack is impossible.

9. Regarding information theory:
    - **An unconditionally secure cipher does not filter information to the cryptanalyst, even if the cryptogram is too long.**
    - A mathematical vulnerable cipher always filters the same information to the cryptanalyst.
    - It measures how much a message is of the interest of the cryptanalyst.
    - It measures the amount of information that a cipher can process in the same cryptographic operations assuming a standard computer.

10. Concerning entropy:
    - If the source generates four messages, the maximum entropy is 4.
    - It is nil if all messages generated by the same source are equiprobable.
    - It can be positive or negative.
    - **It measures the uncertainty that an observer has when a message m appears.**

11. M is a source of messages that generates four messages (m1, m2, m3 y m4), and the probability of each of them is: p(m1) =p(m3)= 40%, p(m2)=15%, p(m4)=5%. Then, the entropy of M is:
    - 0
    - **2,73**
    - -0,51
    - 0,51

12. Concerning the randomness of a sequence…
    - It can be confirmed using a set of tests.
    - If there is a very long sequence of consecutive values, it can be confirmed that the sequence is not random.
    - **It prevents the inference of a subsequence at the light of others.**
    - A random sequence can be generated using a computer algorithm.

13. Computational problems can be classified into…
    - Tractable and intractable, whether exist or not an algorithm to solve the problem.
    - Decidable or undecidable, depending on the time needed to solve the problem.
    - Deterministic or random, whether the solution is always the same or if it varies over time.
    - **P or NP class, whether the time to solve them grows polynomially or not, respectively, based on the problem size.**