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)

uc3m | Universidad Carlos III de Madrid

CRYPTOGRAPHY AND COMPUTER SECURITY COURSE

Introduction to cryptosystems
Self-assessment test

Select the correct answer.

1. Choose the correct answer:

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

2. In a cryptosystem …

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

3. Cryptographic systems are classified by…

   o The type of operations: contractions and expansions.
   o The number of keys: basic and extended.
   o The way of processing data to be encrypted: by blocks or streams.
   o Its reversibility: reversible or irreversible.

4. According to Kerchkoff's principle,

   o The security of a cryptosystem should be based, exclusively, on keeping the key secret.
   o The security of a cryptosystem should be based on the secret of its design.
   o The security of a cryptosystem should depend on the randomness of cleartext messages.
   o The security of a cryptosystem should be based on the complexity of its operations.

5. The goal of cryptanalysis is:

   o Decrypt a given text.
   o Impersonate a legitimate sender.
   o Recover the decryption key.
   o Gain fame and obtain recognition, exclusively.

6. Regarding cryptanalysis attacks to the algorithm:

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

7. Vernam cipher:

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

8. A brute-force attack:

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

9. Regarding information theory:

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

10. Concerning entropy:

   o If the source generates four messages, the maximum entropy is 4.
   o It is nil if all messages generated by the same source are equiprobable.
   o It can be positive or negative.
   o 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:

   o 0
   o 2,73
   o -0,51
   o 0,51

12. Concerning the randomness of a sequence…

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

13. Computational problems can be classified into…

   o Tractable and intractable, whether exist or not an algorithm to solve the problem.
   o Decidable or undecidable, depending on the time needed to solve the problem.
   o Deterministic or random, whether the solution is always the same or if it varies over time.
   o P or NP class, whether the time to solve them grows polynomially or not, respectively, based on the problem size.