First written exam of Criptografia Aplicada

October 26, 2023 18h00m – 19h30m

1.0 **1:** Consider the Vernam cipher. Please indicate:

a) How does it work?

b) Why is it secure from the point of view of information theory (information-theoretic security)?

c) Why is it not normally used?

1.0 **2:** There are ciphers that use invertible SBoxes (they allow you to obtain the input value given the output), and others that use non-invertible SBoxes. AES is an example of the first case; DES (and E-DES, used in the first project) are examples of the second case. Explain:

a) What characteristics must invertible SBoxes have?;

b) Why is this inversion a requirement for AES but not for DES?

1.0 **3:** The CTR cipher mode allows to transform a monoalphabetic block cipher into a polyalphabetic cipher. Explain:

a) What are mono and polyalphabetic ciphers?

b) How does the encryption mode operates?

c) Why does it implements the aforementioned transformation?

1.0 **4:** Many operating systems store a transformation of passwords of its users with a digest function. When a password has to be verified, it is first used as input to said synthesis function and the result is compared with what was saved for the claiming user. Considering the 3 fundamental properties of digest functions indicate, justifying, which are vital to guarantee the secrecy of the passwords whose transformation is stored.

1.0 **5:** Consider that you have encrypted data stored on a disk, and that a single bit of this data undergoes a change due to external noise. That bit flip causes damage to the data recovered after decryption, and such damage depends on the way the data was encrypted and is decrypted. Considering the base cipher modes (ECB, CBC, OFB, CFB, CTR), indicate, justifying, which one would you choose to minimize the damage.

1.0 **6:** Modular arithmetic is used extensively in cryptographic applications. Why is it so useful?

1.0 **7:** The RSA cryptosystem can be used to cypher a message. Explain how. Explain also how that message can be decrypted. What is the mathematical problem that makes RSA “safe”?

1.0 **8:** The RSA cryptosystem can also be used to sign a message, i.e., to attest, if appropriate measures are taken, that the message was not forged by a third party. Explain how.

1.0 **9:** What is the Chinese remainder theorem used for? What operations of the RSA cryptosystem can be speed up by using this theorem?

1.0 **10:** Explain how to implement the Diffie-Hellman key exchange protocol, using modular arithmetic, to share a secret between three parties (instead of the two parties of the original protocol). What is the mathematical problem that makes RSA “safe”?