First part of the exam of Criptografia Aplicada

January 11, 2024 **14h00m – 15h30m/17h00m**

1.0 **1:** Explain the fundamental operating principle of a stream cipher.

1.0 **2:** Digest algorithms, such as MD5, SHA-1, SHA2, etc., are hash functions that have 3 properties that distinguish them from other hash functions. Describe each of these properties in detail.

1.0 **3:** Imagine that you communicate secretly with a group of interlocutors using the public keys of the recipients. However, public key encryption is typically much less efficient than a symmetric cipher, so it is normally replaced by a mixed or hybrid cipher. Explain how this type of cipher works.

1.0 **4:** HMAC (Hashed-based Message Authentication Code) is a parameterizable way of calculating a MAC (Message Authentication Code). Explain:

a) What is a MAC?

b) What is a MAC for?

c) How does HMAC work?

1.0 **5:** Imagine that you have a set of files to which you want to apply, individually, a cipher with the same key (that is, each file is encrypted individually, but the same key is used in all) and you decide to use the AES algorithm (*Advanced Encrypton Standard*) in Counter mode (CTR) for each of these files.

a) Indicate two characteristics of this cipher method that are potentially advantageous.

b) Indicate what special care you should take regarding the encryption of these files using the same key.

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

1.0 **7:** What is the Chinese remainder theorem used for? What operations of the RSA cryptosystem can be speed up by using this theorem?

1.0 **8:** 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 **9:** 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 **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"?

Second part of the exam of Criptografia Aplicada

January 11, 2024 **14h00m – 15h30m/17h00m**

1.0 $\boxed{\textbf{11:}}$ The distribution of public keys is currently done mainly through public X.509 certificates. Explain:

a) What is the main function of a public key certificate?

b) Why does a certificate have to be digitally signed?

1.0 $\boxed{\textbf{12:}}$ Consider the concept of revoking an X.509 public key certificate. Explain:

a) What does it consist of?

b) Who is responsible for communicating it?

c) How can this communication be carried out?

1.0 $\boxed{\textbf{13:}}$ An X.509 public key certificate can be a root of a certification chain. Explain:

a) What is a certification chain?

b) What makes a certificate the root of a certification chain?

1.0 $\boxed{\textbf{14:}}$ Long Term Validation (LTV) is an expression that is used to refer to the ability of a digital signature to be verifiable reliably many years after it was produced. What is the main problem that the passage of time creates in validating signatures, and which led to the creation of mechanisms that allow LTV (don't describe them!)?

1.0 $\boxed{\textbf{15:}}$ Non-repudiation is a characteristic that is normally desirable regarding digital signatures of documents. Explain:

a) What does non-repudiation consist of?

b) What relevance do smartcard devices, such as the Portuguese eID (Citizen Card), have in ensuring this feature?

1.0 $\boxed{\textbf{16:}}$ Explain how two points on an elliptic curve are added.

1.0 $\boxed{\textbf{17:}}$ Explain how you can efficiently multiply a point on an elliptic curve by a negative integer.

1.0 $\boxed{\textbf{18:}}$ Explain how to share a secret among n entities, $n \geq n$, in such a way that only t entities, $2 \leq t \leq n$, are needed to reveal the secret. Consider the cases $t < n$ and $t = n$.

1.0 $\boxed{\textbf{19:}}$ The one-of-two oblivious transfer protocol allows one entity to extract an item of information (from a set of two items) from another entity is such a way that this other entity cannot infer which item was extracted. Explain how this protocol can be adapted to extract one of n items, with $n > 2$. Does your solution scale well, i.e., can it be used in a practical way when n is large?

1.0 $\boxed{\textbf{20:}}$ Quadratic residue properties are indirectly used in zero-knowledge proofs. What is the mathematical problem that makes them useful in this context?