Introduction to cryptography

Examples of assessment questions

- Describe in details the RSA digital signature scheme with appendix.
- On which principle is based the security of the RSA digital signature scheme and where this principle appears to be used in the scheme?
- What RSA key owners must avoid having together in their key and why?
- What is the difference between MDC (manipulation detection code) and MAC (message authentication code)?
- What are the properties that MDCs have to respect to be considered secure?
- What are the properties that MACs have to respect to be considered secure?
- What is the Merkle-Damgard construction?
- What is a sponge function?
- How do we ensure integrity during transmission of information over a public channel?
- What are the two transformations that are at the basis of the security of symmetric ciphers?
- Is it still secure to use DES today (motivate your answer)?
- Which efficient cryptographic primitive(s) Alice and Bob can use (and how) if Alice wants to send a public message m to Bob in a way that Bob can be sure that the message he receives is well the one sent by Alice?
- Is El Gamal signature scheme a signature scheme with appendix or with recovery? Why?
- On what principle is based the security of the El Gamal encryption scheme and where this principle appears in the scheme [the formulas of the scheme are given]?
- What may happen if, after an El Gamal signature is computed, the value of *k* used to generate the signature is revealed?
- Describe in details the RSA encryption scheme.
- Where is stored the plaintext and in fine the ciphertext in AES?
- Describe clearly and precisely what is realized by KeyExpansion, AddRoundKey, ShiftRow, MixColumn and ByteSub
- What are the properties that have to be respected by an authentication protocol to be a zero-knowledge protocol (explain clearly the meaning of those properties)?
- Define and explain what is the Jacobi symbol.
- Compute (with all the details) $\phi(77)$

- Compute (with all the details) the square roots of 78 modulo 91
- Compute (with all the details) the square roots of 3 modulo 143
- Compute (with all the details) $\left(\frac{9}{13}\right)$
- Compute (with all the details) $\left(\frac{21}{77}\right)$
- What is the one time pad? How to use it?
- What is a mode of operation (or an encryption mode) of a symmetric encryption scheme?
- …

This list of examples of questions is **not** an exhaustive list of possible questions.

Different other questions and different other types of questions may be asked.