Information security: an Overview on Cryptography
MSc spring 2017

István Vassányi PhD
vassanyi@irt.vein.hu

Sample test questions

1. What are the three most important aspects of data security? Give an example for each.
2. What is a mono-alphabetic cryptosystem, and what is the traditional method of attack against it?
3. Draw a sketch model of modern secret key based cryptographic communication with a short explanation of its components (like ciphertext, key etc)
4. Which are the four basic types of attacking a secret key cryptosystem? Explain them briefly.
5. What are the steps of a brute force ciphertext attack?
6. What are the technical requirements for a perfect cryptosystem? Can these requirements be met in practice? If yes, give an example. If not, why not?
7. Can the brute force attack be successfully applied against a perfect cryptosystem? If yes, how? If not, why not?
8. What is the hardest problem in the application of secret key cryptosystems? How this problem can be circumvented?
9. How can you assess the quality (i.e. randomness) of a pseudo random bit stream?
10. What are the practical, real-life application areas of perfect cryptosystems? Why?
11. State the principle of computational secrecy.
12. How can you assess whether the key size of a secret key system is large enough to withstand a brute force attack?
13. State the principle of thermodynamic limitations.
14. Why is it important to eliminate any direct connection between fragments of the key, fragments of the plain text and fragments of the ciphertext in a secret key system? What is the problem in this respect with the classic mono-alphabetic cryptosystem?
15. What is the role of language entropy and language redundancy in cracking simple cryptosystems?
16. Describe the structure of a block product cipher (like DES, AES etc).
17. What is called an avalanche effect?
18. Specify and describe the basic operational modes of block ciphers. Hint: the first one is ECB.
19. What are the advantages and disadvantages of stream ciphers over block ciphers?
20. Draw a sketch of a cryptosystem with stream ciphers showing the secret key.
21. How and why an initialization vector is used in secret key systems?
22. What are the three most important requirements for a stream cipher algorithm?
23. How can a LFSR be used to implement a stream cipher?
24. Define the meaning of trap function and give two examples most relevant in cryptography.
25. What are the trap functions on which the RSA and the Diffie-Hellman methods are based?

26. Why public key cryptosystems are inherently less safe than secret key systems?
27. Compare the relative speed of secret key, public key and stream ciphers and message digest algorithms.
28. Compare the key size of secret key, RSA and ECC ciphers that is needed to implement the same level of security.
29. What are the components of a hybrid cryptosystems? Give at least one example for a widely used hybrid system.
30. Describe the principle of the Diffie-Hellman cryptosystem.
31. How a digital signature is generated using RSA?
32. How a digital signature generated by RSA can be verified?
33. What does the term non-repudiation mean in relation to digital signatures? How non-repudiation is ensured?
34. Why a hash function is often used in digital signature algorithms?
35. Describe the steps of a man-in-the-middle attack against a public key system.
36. How a man-in-the-middle attack against a public key system can be prevented?
37. What are the main parts of a digital certificate? How a certificate is generated?
38. Describe the hierarchical certification scheme and compare it to the web of trust scheme for authentication.
39. What is the role of a trust anchor in a hierarchical chain of trust? How the certificate of a trust anchor is verified?
40. How the Diffie-Hellman key sharing protocol can be implemented with Elliptic Curve Cryptography?
41. Why certificates are to be checked before use at a trusted Online Certificate Status Protocol (OCSP) server?
42. Describe the main attack types against message digest algorithms.
43. Describe the rainbow table attack against a password hash algorithm.
44. Describe the birthday attack against a message digest algorithm.
45. What are the approximate recommended sufficient minimum key sizes for AES and RSA and what is the recommended sufficient minimum hash size for SHA-2?
46. What is the basic incentive of applying ECC instead of RSA for key establishment?
47. Describe the Babbage-Golic attack against stream ciphers.
48. How (by which physical means) a problem to be solved by a Quantum Computer is formulated?
49. What is the fundamental advantage of Quantum Key Distribution over public key cryptosystems?
50. Describe the main steps of the BB84 protocol.