Auto-Evaluation Questions
(Symmetric Cryptography)

1. What is symmetric encryption

2. Given the tables from X.800 Framework Security Services and Attack Types – Class 1, try to understand and to figure out the place (cells) where symmetric encryption fits.

3. From the question 2, summarize the various types of attacks against communication channels that we can protect with symmetric cryptopgraphy.

4. Do you believe that symmetric encryption can be used to completely protect from traffic-flow confidentiality? Present your arguments.

5. What are the generic security properties of symmetric encryption methods and what are the main considerations to have symmetric encryption for greater security?

6. Discuss the requirements that must be satisfied for the correct and secure use of symmetric encryption.

7. In symmetric encryption methods we need in general encryption and decryption functions (symmetric) and a shared secret key. However, this is not sufficient and depending on the requirements we have, we need other security association parameters.

8. Present the differences between block ciphers and stream ciphers.

9. Name at least five block ciphers (indicating their keysizes and blocksizes) and five stream ciphers Try to find this with the symmetric algorithms you have in your java installation (JCA-JCE crypto-providers)

10. Describe the main components, parameters and concerns of the Feistel Structure as a base design structure for Symmetric Block-Encryption Algorithms.

11. Consulting the bibliography, try to explain how the DES algorithm works (internally).

12. Why an algorithm such as DES uses different rounds of the core-encryption function (or step) and a key-scheduling algorithm to generate different sub-keys for each round ?

13. What are the advantages and disadvantages of using 3DES. Discuss the disadvantages, comparatively to AES, for example.

14. List the important design criteria for a stream cipher.

15. What is cryptanalysis ? Summarize the types of cryptanalysis attacks (or cryptanalysis studies) to evaluate the security or robustness of a symmetric encryption algorithm

16. Present some cryptanalysis criteria in the study of security of a symmetric-encryption algorithm

17. Explain why using the considerations of computation evolution (for example using the Moore Law), we can expect to break by Brute Force the AES w/ a 128 bit key somewhere in the years 2082-2090, and not in 10E+17 years as wecan project with the current computational power.

18. Explain the differences between unconditional security and computational security in the security study of cryptographic algorithms.

19. Try to develop a feeling on the performance of different symmetric encryption algorithms. Using a tool (such as openssl) try to find a performance factor between the use of DES, TripleDES and AES.

20. Explain how Triple-DES works when we use a 112 bit key and a 168 bit key.

21. What is Onion-Encryption ? What are the advantages and disadvantages of using such scheme ?

22. Explain whet is the *whitening* technique in improving the security in the use of symmetric encryption methods.

23. Try to present other possible alternative methods to improve the security in using symmetric encryption methods with a similar objective as targeted by the whitening technique.

24. The AES design didn't follow the classic Feistel Structure, focusing more on specific algebraic constructions. Present the main computation steps in the internal structure of the AES algorithm.

25. Try to find the criteria imposed by NIST to select the AES algorithm as a standard (decision on the Rijndael Algorithm), in the initial launched contest (where other proposals were considered).

26. Name different modes of operation for block ciphers for message-confidentiality

27. Name modes of operation for block ciphers that include authentication-codes.

28. What are the advantages and disadvantages of the ECB mode? Present these advantages in terms of security, performance, transmission-faults and message recovery

29. Idem (question 28) for CBC.

30. Idem (question 28, 29) for CTR.

31. One advantage in OFB, CFB and CTR modes, is that a receiver don't need to have a decryption function to decrypt the ciphertext messages received from a sender, so the implementation for such modes only require the encryption function. Why?

32. Do you believe that the Initialization Vector used for CBC encryption can be sent in cleartext (so, known by a possible adversary) between a sender and a receiver exchanging encrypted messages? Present your argumentation in answering this question.

33. Using CBC mode used in block-ciphers, the ciphertext is necessarily bigger that the plaintext. True or False? Justify.

34. What cipher modes of block-encryption operation can be used to avoid that ciphertext will be bigger than the plaintext. Give an example of how this is avoided in a specific mode.

35. Try to give examples of applications (according to their requirements) that can use ECB, CBC, CFB, CTR or OFB.

36. What is the padding computation in a symmetric block encryption algorithm? Why we need to use padding?

37. Explain the differences between a Zero-Padding and a PKCS$5 and PKCS#7 Padding processing. In your explanation include the security concern.

38. Suppose you want to create your own padding function for high security in using a block cipher in CBC mode (not using a standard scheme). Present a design proposal and explain the security of your proposal.

39. Considering the internal structure of the RC4 stream cipher, describe some strengths in the practical use of the algorithm.

Alternative/Complementary Challenging Questions: If you find correct answers you will be a "crypto-winner"

40. In the sequence of the question 39, try to understand the vulnerability of using RC4 in the WEP protocol (for 802.11 WLANs protection), particularly when using a short key (ex, 40 bit)

    Sources for your investigation: WEP Protocol:
    https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

    Initial tracks for your investigation:
    https://www.dummies.com/programming/networking/understanding-wep-weaknesses/

41. From what you learned in question 40 try to argument if the vulnerability in the WEP case-study is die to RC4 internal vulnerabilities (as strenghthed in question 39) or is a problem of use in the WEP protocol.

42. (Q2.2) Consider a very simple symmetric block encryption algorithm in which 32-bits blocks of plaintext are encrypted using a 64-bit key.

    Encryption is defined as $C = (P \text{ xor } K_0) \text{ n+ } K_1$ where
    C = ciphertext,
    K = secret key,
    K_0 = leftmost 64 bits of K, K_1 = rightmost 64 bits of K,
    xor = bitwise exclusive OR,
    n+ is addition mod 2^{64}.

    a) Show the decryption equation. That is, show the equation for P as a function of C, K_0, and K_1.

    b) Suppose and adversary has access to two sets of plaintexts and their correspond- ing ciphertexts and wishes to determine K. We have the two equations:

    $$C = (P \text{ xor } K_0) \text{ n+ } K_1; \qquad C' = (P' \text{xor } K_0) \text{ n+ } K_1 ;$$

    First, derive an equation in one unknown (e.g., K_0). Is it possible to proceed further to solve for K_0?

43. (Q2.5) Consider a Feistel cipher composed of 16 rounds with block length 128 bits and key length 128 bits. Suppose that, for a given k, the key scheduling algorithm determines values for the first eight round keys,
    $k_1, k_2, \ldots, k_8$, and then sets $k_9 = k_8, k_{10} = k_7, k_{11} = k_6, \ldots, k_{16} = k_1$

    Suppose you have a ciphertext c. Explain how, with access to an encryption oracle, you can decrypt c and determine m using just a single oracle query. This shows that such a cipher is vulnerable to a chosen plaintext attack. (An encryption oracle can be thought of as a device that, when given a plaintext, returns the corresponding ciphertext. The internal details of the device are not known to you, and you cannot break open the device. You can only gain information from the oracle by making queries to it and observing its responses.)

44. For any block cipher, the fact that it is a nonlinear function is crucial to its security. To see this, suppose that we have a linear block cipher EL that encrypts 128-bit blocks of plaintext into 128-bit blocks of ciphertext. Let EL(k, m) denote the encryption of a 128-bit message m under a key k (the actual bit length of k is irrelevant).

    Thus, EL(k, [m_1 xor m_2])= EL(k, m_1) xor EL(k, m_2) for all 128-bit patterns m_1, m_2

Describe how, with 128 chosen ciphertexts, an adversary can decrypt any ciphertext without knowledge of the secret key *k*. (A "chosen ciphertext" means that an adversary has the ability to choose a ciphertext and then obtain its decryption. Here, you have 128 plaintext–ciphertext pairs to work with, and you have the ability to chose the value of the ciphertexts.)

45. (Q2.9) What RC4 key value will leave S unchanged during initialization? That is, after the initial permutation of S, the entries of S will be equal to the values from 0 through 255 in ascending order.
46. (Q2.13) Is it possible to perform encryption operations in parallel on multiple blocks of plaintext in CBC mode? How about decryption?
47. (Q2.14) Suppose an error occurs in a block of ciphertext on transmission using CBC. What effect is produced on the recovered plaintext blocks?
48. (Q2.17) Explain how the CTS mode works and why it maintains the ciphertext block size with the same size of the plaintext blocksize.

49. (Q2.18) If a bit error occurs in the transmission of a ciphertext character in 8-bit CFB mode, how far does the error propagate?

50. Try to train for the following questions: I give you the formal representation (formula) of a certain mode of operation and the work scheme (picture) of the mode. Can you write the formula for decryption.

    Ex: for CBC Encryption: $C_i = E_K$ (Pi XOR Ci-1) with $C_0 = E_K$ (Pi XOR IV)

    Can you rite the formulas for Decryption: P_i = …. and P_i = ……

    Try to do the same for other modes: CTR, OFB, CFB, CTS