Collection of questions (June 2020)

In the following collection are gathered some questions from the (available) past exams, and teaching material provided by Prof. Zseby (in bold), integrated with some questions added from the slides' content (in regular thickness).

A. Attack types

1. **What is the difference between viruses and worms?**
2. **Explain SYN floods**
3. **What is a horizontal scan?** A vertical scan?
4. **Explain the DDoS reflection attack.**
5. What is meant by backscatter?
6. What are the phases of worm propagation?
7. **What is a monomorphic worm?** Polymorphic? Metamorphic?
8. **Name 2 different topologies for a Botnet Command&Control structure. What are their advantages and disadvantages?**
9. In hybrid Command&Control structures, what are servent and client bots?
10. List and explain the different evasion methods that are used to conceal the C&C.
11. What are the most common obfuscation methods for botnet control traffic?

B. Ciphers

1. What are the basic building blocks of cryptography? And In modern ciphers?
2. **Decrypt a message with the Caesar cipher, k=3**
3. What is Letter Frequencies analysis?
4. How does Vignère cipher work? How can it be broken? Calculate the ciphertext given a message and a key.
5. **How does a One-Time-Pad work? Calculate the ciphertext for a message and a key.**
6. **What distinguishes a good and a bad key for OTP? Name 4 properties for a good key.**
7. **Why is it a bad idea to use a OTP key twice?**
8. What it is meant with perfect security (or perfect secrecy)? And with computational security?
9. What is the main Kerchoff's principle?
10. Explain, with a simple drawing, how do rotor machines for encryption work.
11. What is the difference between a substitution cipher and a transposition cipher?
12. Encrypt a message using a Rail-Fence cipher with 3 rails.
13. **Can you use only Letter Frequencies analysis on a transposition cipher to get info about plaintext?**
14. **Explain the ciphertext-only, known-plaintext, chosen plaintext, and chosen ciphertext attacks.**
15. What is a related key attack?
16. **Explain what is the difference between stream and block ciphers.**
17. **Calculate the advantage given P(A(R) = 1) = 0.9 and P(A(G(s)) = 1) = 0.2. Can G be considered a good PRG?**

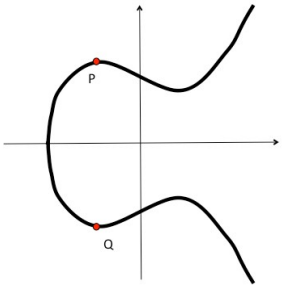
C. Symmetric cryptography

1. Draw the scheme of a SP (substitution-permutation) network
2. A5/1: How is the encryption built?
3. RC4: How is the algorithm initialized?
4. **RC4: How is the new value S[t] calculated based on S[i] and S[j] in the RC4 stream cipher (after initialization is completed)**
5. What is an improper implementation of RC4, that lead to a known vulnerability in networks?
6. **Draw the functional blocks and the structure of a Feistel cipher**
7. DES: Which building blocks does DES use?
8. **2DES: If E(m,kA) is the encryption function for Single-DES: How does the encryption function for Double DES look like?**
9. **3DES: Why isn't 3DES's encryption function E(E(E(m,k1),k2),k3)?**
10. AES: What are the 4 operations/steps of the AES cipher? How many rounds are performed?
11. **How does Electronic Code Book (ECB) mode work?**
12. **What can be used in an attack of ECB-encrypted messages?**
13. Name and draw the five most common block cipher modes named in the lecture.
14. What are the options for authenticated encryption?
15. Why isn't a CRC a good Message Authentication Code?
16. What is meant with CBC-MAC? What is the problem associated with it?
17. How is an HMAC built?
18. **Name 5 properties that should be fulfilled by a cryptographic hash function.**

D. Asymmetric cryptography

1. What are private and public keys? What is the relation between them? **When are these used to sign, encrypt, decrypt and verify a signature?**
2. How can authentication be performed via asymmetric cryptography?
3. What is meant with discrete logarithm problem?
4. **What function can be used to find out how many numbers 1 <= x <= n are relatively prime to n? Calculate this function for a given n and for a product of two factors.**
5. How does the Rivest-Shamir-Adleman trapdoor function work?
6. **RSA: How are encryption and decryption functions for RSA?**
7. **RSA: How is a digital signature generated based on RSA?**
8. What is a Forward Search attack?
9. Why do we need to introduce a random padding in messages encrypted with public-key cryptography?
10. **Sketch the Diffie-Hellman key exchange.**
11. **What is perfect forward secrecy?**
12. **Can you prove that a message signed from Bob (RSA) is valid (e.g. at court)?**
13. **What is the difference between a message authentication code and a digital signature?**
14. ECC vs RSA, what is the advantages of using ECC in place of RSA?

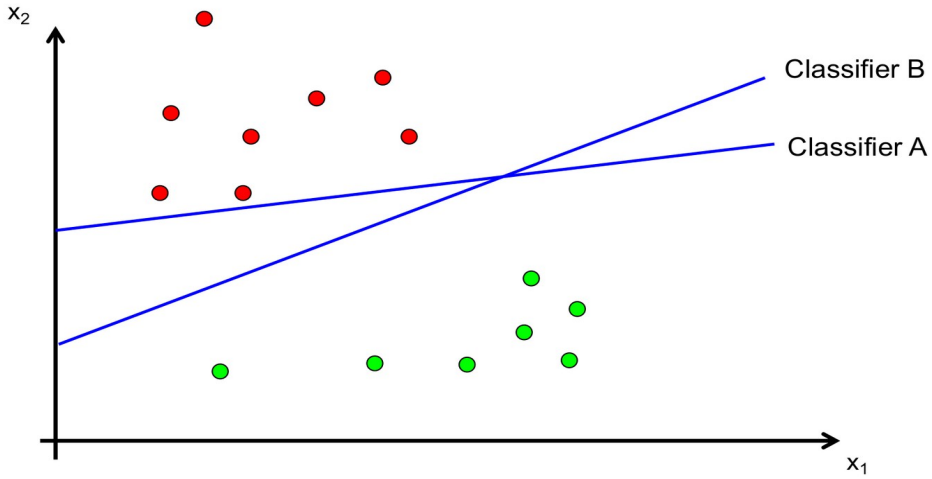
15. **ECC: What is the result of an addition of the points P and Q if elliptic curve arithmetic is used? What about P+P?**



16. ECC: What is used as generator in elliptic curve encryption?
17. ECC: What are public and private parameters of ECC?
18. **ECC: Sketch the Elliptic-Curves Diffie-Hellman key exchange.**

E. Anomaly Detection

1. **IPSec Authentication Header (AH) provides:**
   - ☐ **Confidentiality only**
   - ☐ **Integrity only**
   - ☐ **both Confidentiality and Integrity**
2. What are the three different modes of use of IPsec?
3. What is the Internet Key Exchange and what is its relation with IPsec?
4. **In TLS: (Multiple choice)**
   - ☐ **The TCP Port is not encrypted**
   - ☐ **Client auth is optional**
   - ☐ **DH can be used for key exchange**
5. What are the main differences between IPsec and TLS?
6. What is a traffic flow?
7. What are the four steps for traffic aggregation?
8. **What is the darkspace?**
9. **What is entropy? Distinguish between two samples, which one has higher entropy.**
10. **How can entropy values be used to detect attacks?**
11. What are the two detection techniques for attacks? What are their pros and cons?
12. **What is a point anomaly?** Contextual anomaly? Collective anomaly?
13. **What is the purpose of Support Vector Machines (SVMs)?**
14. **What can be done if you only have a technique to learn a linear classifier but the data is not linear separable?**
15. **Which classifier is better? How do we know? Which points are the support vectors?**



16. What is meant with Area under the ROC curve?