1. You have a long ciphertext from the XVII. century. How can you decide whether it was produced with a monoalphabetic or polyalphabetic cipher? **(5p)** If it would be a polyalphabetic cipher, give a method to determine the key size! **(5p)**

2. You have a long ciphertext from the XVII. century and you would like to check whether it is produced with a monoalphabetic or polyalphabetic cipher. How can you check that? **(5p)** Construct your own polyalphabetic cipher! You can reuse tabula recta or the Alberti disc. Describe the method of encryption and decryption! **(5p)**

3. You perform frequency analysis on a ciphertext. As a result you have two letters which frequencies are significantly different than the others, but the others seem to be uniform. What would you assume about the cipher? **(5p)** Describe a polyalphabetic cipher that cannot be cracked by guessing the key size and performing frequency analysis! **(5p)**

4. There is a long ciphertext that was generated by some polyalphabetic cipher. How could you find out the length of the secret key? Describe 2 different methods! **(2x4p)** Once you have found out the length of the key, how could you proceed with the cryptanalysis? **(2p)**

5. You are a cryptanalyst and you get a ciphered message, which consist of just random characters at the first sight. The text is from the XVI. century and supposed to be English. What would you do if you would like to decrypt the message? Describe methods and decisions that you can make, just like a flow chart! **(10p)**

6. Describe the Feistel architecture! What is the advantage of the architecture? **(4p)** Using the DES cipher as a building block, depict the 3DES cipher! **(3p)** How large is the key at 3DES and why is it so? **(3p)**

7. What are the weak and semi-weak keys in the case of block ciphers? Why should we disable them? **(3p)** Are the any weak keys in AES? Why? **(2p)** You have a electronic device and its DES chip goes out. Unfortunately, there is no DES chip on the market anymore. Could you replace that chip using a 3DES chip, if you wish not to change other elements? (The 3DES chip is a 3DES-EDE and has two lines for the two keys.) How? **(3p)** Can you build a more secure device with this solution? **(2p)**

8. Build a product cipher and sketch it (it can be DES or AES as well)! **(5p)** What is the reason we use 3DES and how does 3DES-EDE look like? **(3p)** How large is the key at 3DES and why is it so? **(2p)**

9. Draw the sketch of the Feistel architecture. **(5p)** Draw in the input, output, keys and the functions. Based on the sketch give the formula of R_i and L_i using K_i, f. (You can use other indexes of course). **(3p)** How do the Feistel architecture works when the ciphertext is decrypted? **(2p)**

10. What is the CTR operation mode in the case of block ciphers? **(5p)** Why is this recommended in the case of random access? **(2p)**? Let assume that you have 8 blocks to decrypt. The 5th byte of the second block gets wrong during the transmission. What blocks and bytes do remain readable at the receiver side? **(3p)**

11. Sketch the detailed CFB and OFB operation modes of block ciphers (encryption and decryption)! **(6p)** Is it possible to use an asymmetric block cipher with CFB or OFB? **(2p)** What are the benefits of the CTR operation mode? **(2p)**

12. You have a message that is exactly 1000 characters long. You want to transfer this message securely to somebody you know. Use the AES cipher and choose an operation mode, which is secure and efficient! Describe the method and all related tasks you have chosen (e.g. padding if you use it) and reason your decision! **(6p)** The radio channel that you use to transmit the message is lossy. How would you extend your previous procedure in order to provide a solution, where your message cannot be misunderstood? **(4p)**

13. Sketch the blocks of the CFB and OFB operation modes of a block cipher! Show the difference between the two block diagrams! **(5p)** What is the role of the IV and how we get its value? **(2p)** Assume that we have 5 blocks to transmit and the 3th block is erased silently (so the decoder cannot notice it). What blocks can be decoded correctly using the CFB and OFB operation modes? **(3p)**

14. You have linear feedback shift registers (LFSR). Please give two different architectures that combine them into a stream cipher and strengthen the output compared to a single LFSR! **(6p)** How do you use a key in such architectures? **(2p)** Why you should avoid ciphering two different plaintext stream with the same keystream? **(2p)**

15. Sketch your own AES based iterative hash function! Detail the functionality of each box you draw! **(6p)** What is the output size of your function? How can you double the output size of the hash function? **(4p)**

16. You have a hash algorithm, which produces 128 bit hash output. The hash function is preimage and collision resistant. You would like to use this function in order to protect your messages from manipulations during the transit. How could you build such a secure and efficient protection mechanism using this hash function? Describe the protocol using figures, what would you do and how would you do that! **(6p)** It turns out that you have only 64 spare bits for the protection. What should you do in this case? **(4p)**

17. Describe the method, how can we calculate a CBC-MAC hash value for a given message using the AES cipher? **(4p)** Is it possible to use asymmetric ciphers in CBC-MAC? Why? **(2p)** You have a 100 byte message and you want to protect its

integrity during a transfer. Write down how should you prepare your message if you are using the hash algorithm that you described above (AES CBC-MAC)! **(4p)**

18. Describe a key exchange protocol, where you use public-private key pairs, both parties contributes to the session key, and needs maximum two messages. Suggest cryptographic algorithms to be used and also the size of their parameters! **(10p)**

19. Give a key exchange protocol, where: a) you don't need pre-negotiated long term keys, b) you don't need an online trusted third party, c) both parties contributes to the key, d) provides key confirmation. Suggest algorithms to be used and the size of the required parameters! **(10p)**

20. Describe a key exchange protocol using a trusted third party, and where each participant has a long term key with that third party! The key exchange should take no more than 3 messages! Describe the parameters and their role! Try to avoid any weakness in the protocol! **(7p)** In a key exchange protocol what is the pros/cons using a timestamp and using a nonce? **(3p)**

21. You have a friend, Bob, living in a far way country and you would like to exchange secret emails with him. All you have is a friend Cecil, whom you can trust and you know that Bob also trusts in him. You and Bob surely know Cecil's public key. You cannot be sure that nobody eavesdrops on your Internet connection. Construct a key exchange protocol that is efficient and can create a session key for you and Bob. **(8p)** Suggest cryptographic algorithms to be used in your protocol and define size for the key parameters! **(2p)**

22. There is Alice and Bob who want to chat on the Internet. They both know that NSA is watching their communication and they believe that their conversation should be private. They have never met before in real life, but on Facebook they found a common friend Cecil, whom they meet occasionally. They both trust in Cecil. Construct an algorithm, which can be used by Alice and Bob to generate a session key to cipher their chat sessions! In order to achieve high level security, they need new keys for each new sessions. They want to chat more frequently, than they meet with Cecil. Describe the algorithm formally and give the parameters precisely! **(10p)**

23. Alice and Bob already have a session key for their chat. Now Alice would like to send a 151 byte long private message to Bob. The chat application they use supports DES, 3DES, AES and RSA ciphers. Which one should be chosen? Explain your decision! **(3p)** If you would be the one, who writes the chat application, how would you use the cipher to encrypt the message? What kinds of padding and operation mode would you use? Describe the methods! Explain your decision! **(4p)** What would be the difference, if you could use an RC4 cipher? Explain it! **(3p)**

24. The NSA was smart enough to capture the messages between Alice and Bob. Sometimes they even change some bits in the messages during the transmission.

Let's suppose that the chat application uses CBC operation mode. Alice sends the 151 byte long chat message. NSA captures it and changes the 10th byte. What will Bob get, when he decrypts the message? Explain the result! **(3p)** Alice asks you to create an algorithm, which is able to filter out those messages that were modified during the transmission. You can rely on the ciphers the chat application supports. Describe your algorithm! Create a sketch showing the cipher block and the algorithm! The solution should be secure! **(4p)** How could you change your algorithm if the chat application would support SHA-512 as well? Describe it! **(3p)**

25. How would you change the algorithms in the chat application, if Alice and Bob could get a PKI certificate (containing their public key) from a trusted Certificate Authority? Describe the changes in the encryption and the integrity protection! **(2x5p)**