A Attack Tpyes

1) What is a vertical Scan?

2) Explain Side Channel Attacks.

3) What is the difference between a worm and a virus?

4) What is a methamorphic worm?

5) What is the purpose of an Reflection DoS Attack an how does it work?

6) Name and explain two Command & Control Communication Stuctures

B Ciphers

1) How does the Vigenere Cipher work and in which way is it possible to break it?

2) Explain the terms „Cryptology, Cryptography and Cryptoanalysis“.

3) What is the disadvantage of an One Time Pad?

4) Explain the difference between Perfect Security and Computational Security.

5) How works the Adaptively Chosen Ciphertext attack?

6) What purpose has the A5/1 Keystream Generator and how does it work in general?

7) Assume an Initialization Vector IV = (4,255,V). How does it look in the table S[i] after two Swap and Calculate operations?

8) What are the advantages of Stream ciphers?

9) On which cipher is DES based on, and how does it look like as block diagram?

10) Explain why the Triple DES look like this C = E(D(E(m,kA),kB),kC)
and not with C = E(D(E(m,kA),kB),kC).

11) Draw the principle of AES and explain the single components. Is AES a Stream or a Block cipher?

12) What are the differences between ECB and CBC? Draw both encryption modes.

13) What kind of cipher realizes CTR mode?

C Message Authentication Codes

1) Does CRC protect against Man in the Middle attacks?

2) Explain the Birthday Attack.

3) Sketch the authentication procedure via assymetric cryptography. And what is the solution for possible Man in the Middle attacks?

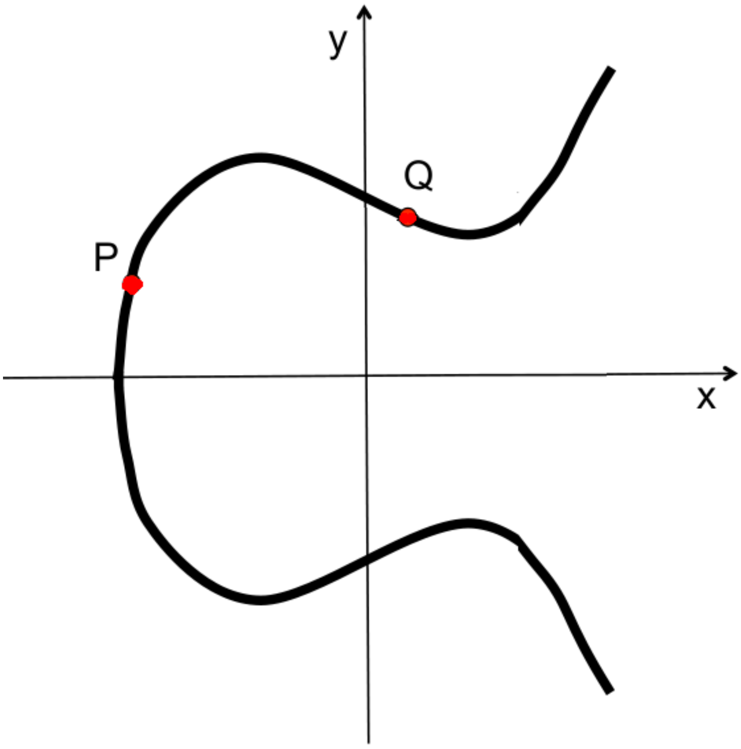
D Assymetric Cryptography

1) Is the trapdoor information in RSA a secret?

2) Give an short example to the RSA encryption procedure.

3) Assume and elliptic curve graph with $y^2 = x^3 + 4ax - b$ does it need an additional condition? And if yes, why? Give an example.

4) Calculate P+Q=R Graphically with the point ECC arithmetic. How do you calculate R if you only have P? Sketch an additional figure to show this.



5) Sketch an example for an Repeated point addition.

6) What is a possible side channel attack on ECC?

E Security Protocols

1) Name 6 IPsec services.

2) What does the IPsec standard say about supporting the cryptographic method AES-XCBC-MAC for Message authentication (ESP,AH)? (MUST,SHOULD(+),MAY or SHOULD NOT)

3) Is the Padding field in the ESP header variable or not?

4) What does RFC6434 say about IPsec (MUST,SHOULD(+),MAY or SHOULD NOT)?

5) On which level runs TLS and what are the 3 most important goals of it?

6) Sketch an key exchange of TLS.

F Anomaly Detection

1) Sketch an block diagram of an Intrusion Detection System and drop some words for every entity.

2) What are the pros and cons of a signature based detection?

3) Explain a Multi-class anomaly detection.

4) Name and explain two classification-based techniques. What are the pros and cons of them?