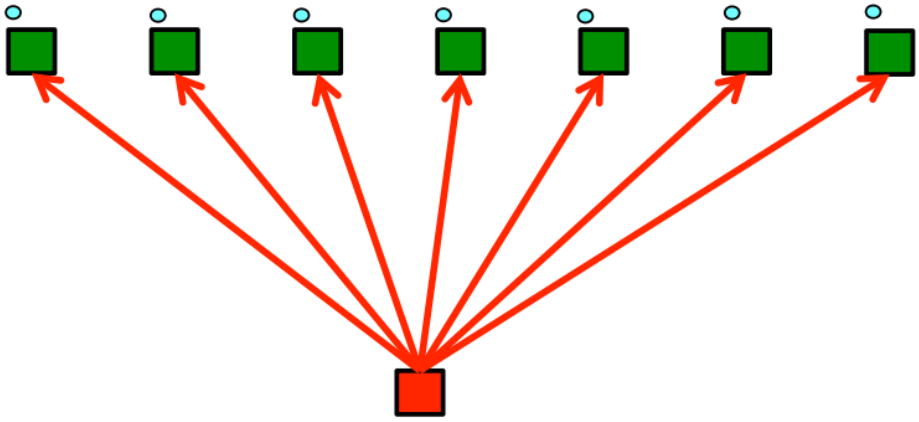
A Attack Types

1) What is a horizontal Scan?



- Search if a specific port is open on multiple hosts
- Packets to a single destination port on multiple destination IP addresses

2) Which protocol is often used for command&control structures in botnets?

IRC (Internet Relay Chat)

3) What is a monomorphic worm?

The Payload does not change and it may be fragmented in different ways .
Signature-based detection possible.
(Payload does not change and behaivour does not change)

B Ciphers

1) How does a One-Time Pad work?

The key is as long as (or longer) than the plaintext. The plaintext is encrypted bit by bit or letter by letter with the key and this key is only used once.
It´s a kind of polyalphabetic encryption.

2) What is a Chosen Plaintext Attack?

The attacker is able to choose a plaintext out of a set. This text will be encrypted and he is able to obtain the ciphertexts in relation to the plaintexts to analyze the encryption.

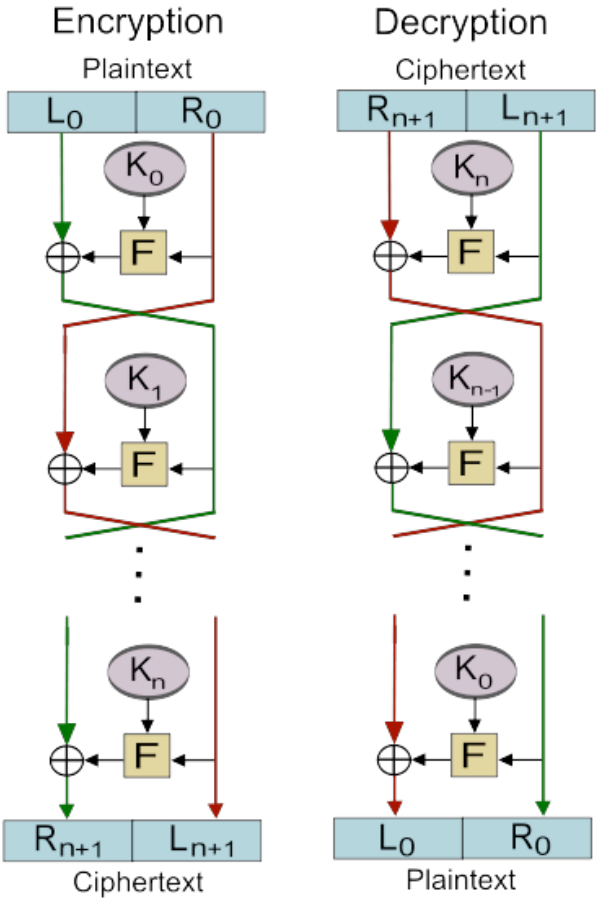
3) Explain the difference between stream and block ciphers.

Stream ciphers work like an one time pad, each bit is encrypted with XOR operation using an key.
Block ciphers work like an Codebook, there are blocks with equal lenght.

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)

S[t]=S[i]+S[j]

5) Draw the functional blocks and the structure of a Feistel ciper.

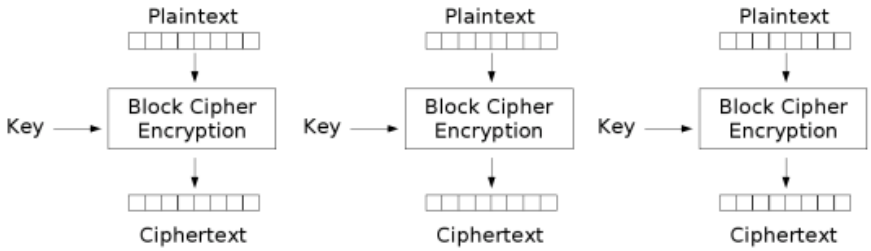


6) If E(m,kA) is the encryption function for Single-DES: How does the encryption function for Double DES look like?

E(E(m,kA),kB)

7) How does Electronic Code Book (ECB) mode work?

The message is split into blocks of equal size and it gets padding if needed.
Each block is encrypted independently .



Electronic Codebook (ECB) mode encryption

C Message Authentication Codes (MACs)

1) What is the difference between a message authentication code and a digital signature?

MAC s verify that message was not altered .
Generation and Verification of MAC works with same secret key (symmetric cryptography) so everyone who knows secret key can generate a valid MAC .
Digital Signatures prove that message was sent by a specific sender (non-repudiation) . Only the originator of the message should be able to provide correct signature . This is possible with asymmetric cryptography .

2) Name 5 properties that should be fulfilled by a cryptographic hash function.

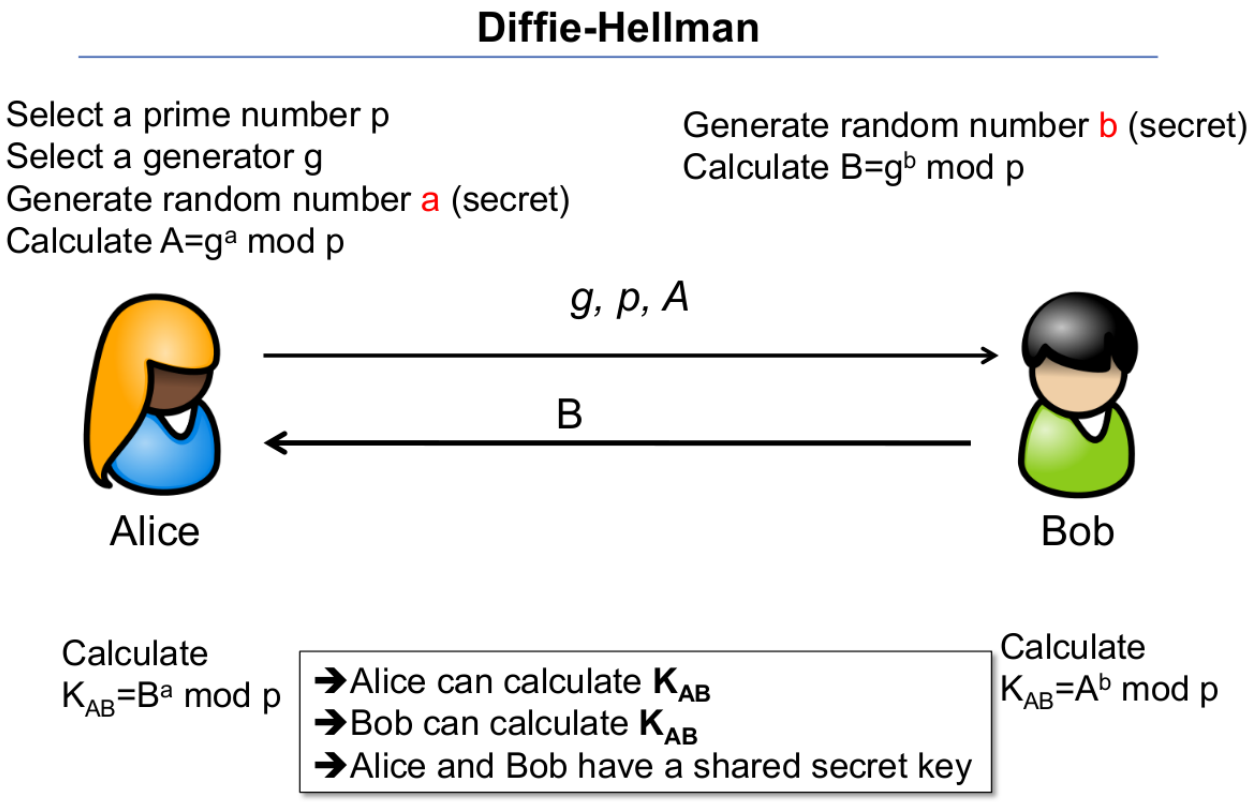
Compression
Efficiency
One-way
Weak collision resistance
Strong collision resistance

D Asymmetric Cryptography

1) Given are 2 prime numbers p and q and the integer n=pq. What function can be used to calculate how many integers <= n are relative prime to n?

(p-1)(q-1)

2) Sketch the Diffie-Hellman key exchange.



3) What is perfect forward secrecy?

It means that an attacker is unable to decrypt (previously) recorded messages if he

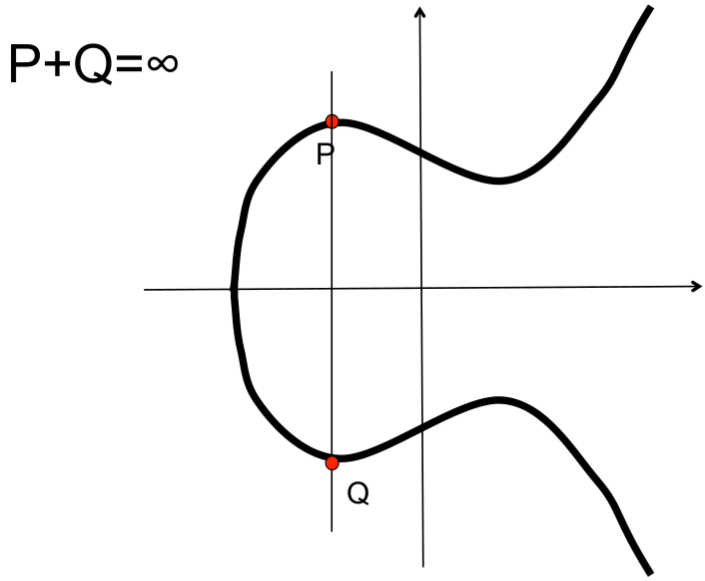
gets access to the long-term key.
Use an session key and prevent that it gets known.

4) RSA: How is a digital signature generated based on RSA?

- Calculate hash of message h = H(m)
- Sign hash with private key $h' = h^d \bmod n$
- Send signature together with message h', m
- Verify hash with public key

$$h = (h')^e \bmod n$$

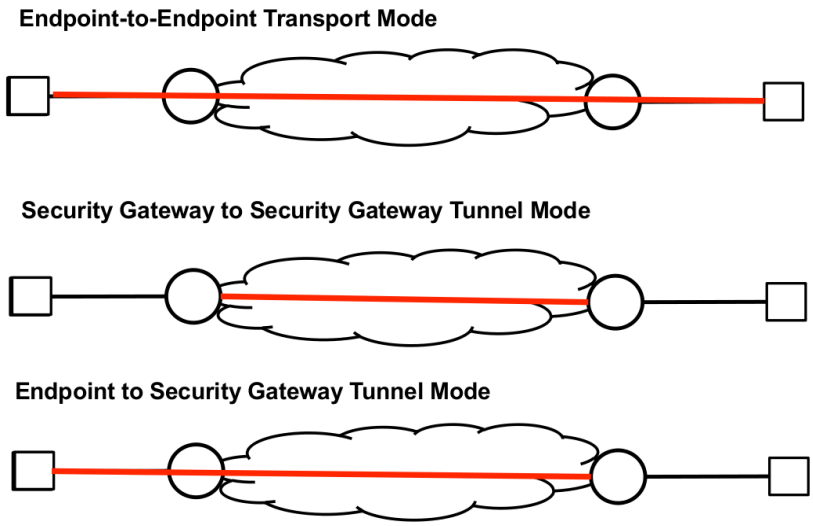
5) ECC: What is the result of an addition of the points P and Q if elliptic curve arithmetic is used?



Identity element ∞ ➔ Q=-P

E Security Protocols

1) What are the 3 modes of use for IPsec protocol?



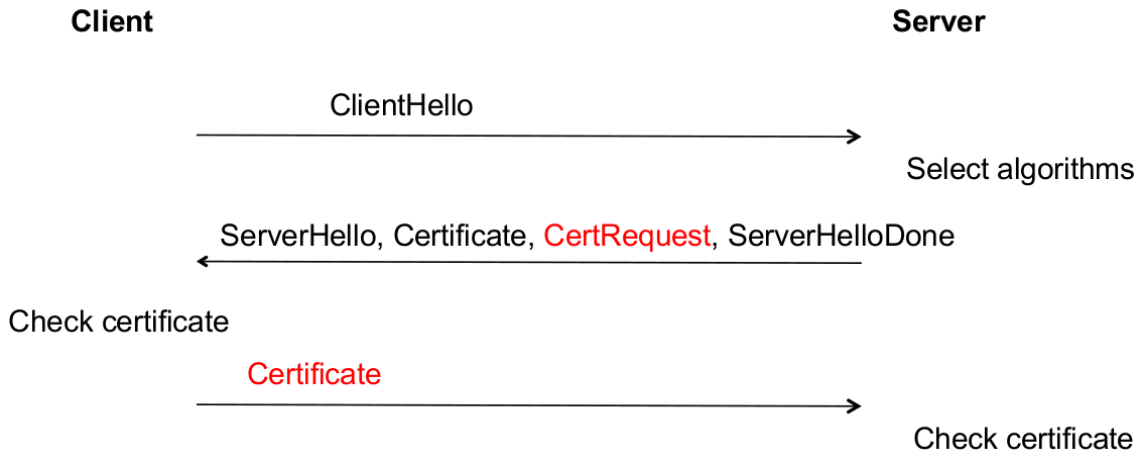
2) Why is the Authentication Header (AH) only optional and not mandatory for IPsec implementations?

The Authentication Header is not encrypted like the Encapsulated Security Payload. If the firewall sees AH header , it knows that the payload is not encrypted and it´s just able to check the TCP header .

3) What does the IPsec standard say about supporting the cryptographic method AES-CBC for Encapsulating Security Payload (ESP)? (MUST,SHOULD,MAY oder SHOULD NOT)

MUST

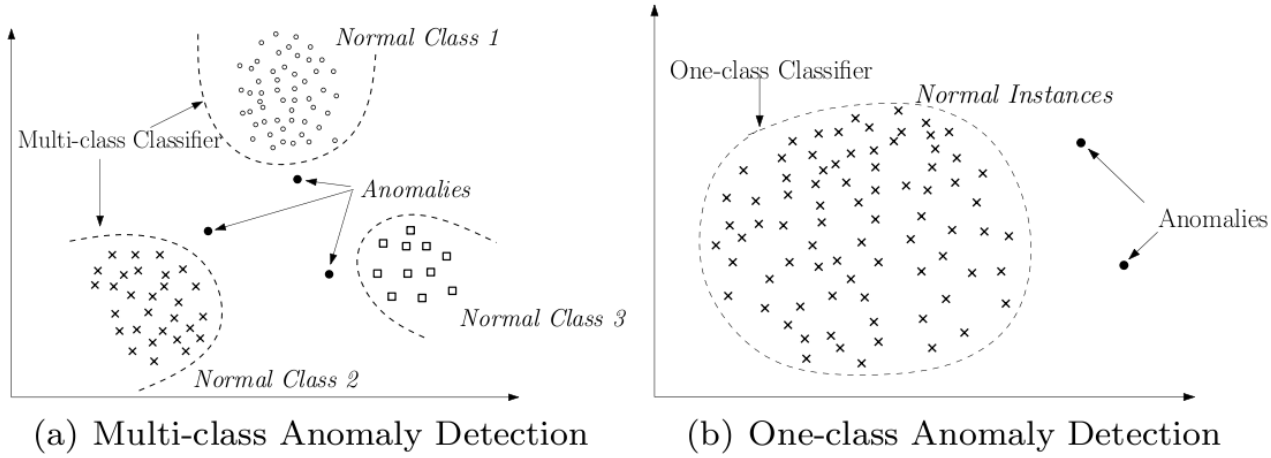
4) Sketch the initial TLS Handshake message exchange if client authentication is used.



F Anomaly Detection

1) What is a point anomaly?

A point anomaly is an event (e.g. Request to an unusual port) outside of a normal class (e.g. Request which is normal like TCP request to port 80 on a web-server).

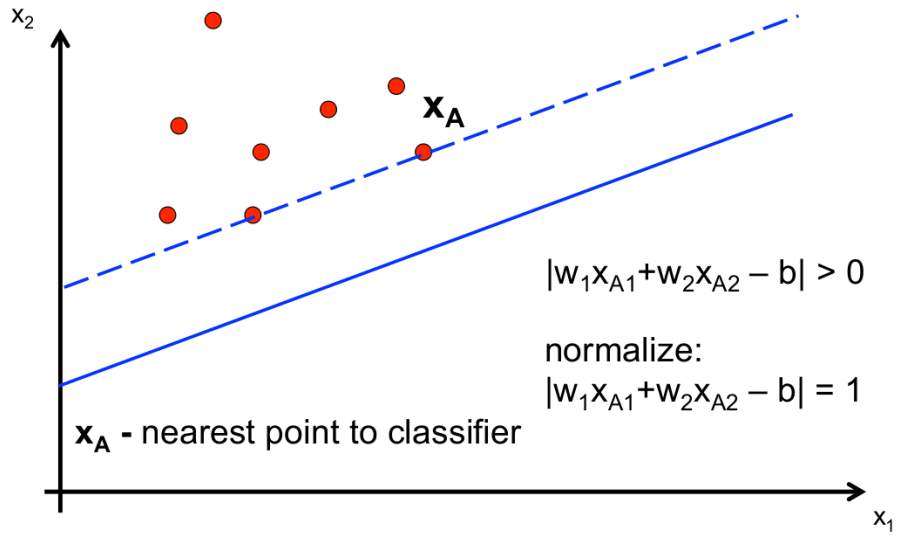


(a) Multi-class Anomaly Detection (b) One-class Anomaly Detection

2) How can entropy values be used to detect attacks?

3) What is the support vector in Support Vector Machines?

The distance to the nearest point.



4) What can be done if you only have a technique to learn a alinear classifier but the data is not linear seperable?

Transform the non-linear seperable data to higher dimensions and make them linear seperable.