NetSec Questions

Answers for the questions in the collection of questions (June 2020).
Done with ChatGPT that was given all the slide decks of the lecutures.
Most of the questions I checked manually if they look to be correct.
The ones that are **bold** in the question sheet are marked with a star (★).

Attack Types

1. ★ **What is the difference between viruses and worms?**
   A virus inserts itself into another program and needs the host program to run. A worm runs on its own and propagates a full working copy of itself over the network.
2. ★ **Explain SYN floods**
   A SYN flood fills the server's table of half-open TCP connections. The server sends SYN-ACKs and waits for ACKs that never arrive, so the backlog fills and new legitimate connections get rejected.
3. ★ **What is a horizontal scan?**
   A horizontal scan, also called a host scan, checks whether one specific port is open on many different hosts. The packets go to one destination port on multiple destination IP addresses. A vertical scan checks many destination ports on one destination IP.
4. ★ **Explain the DDoS reflection attack.**
   The attacker sends requests with the victim's spoofed source IP to many other hosts. Those hosts send replies to the victim, which overloads the victim.
5. **What is meant by backscatter?**
   Backscatter is the reply traffic sent to spoofed source addresses during attacks such as SYN floods or reflection attacks. Darkspace sensors often observe it.
6. **What are the phases of worm propagation?**
   Target finding, transferring, activation, infection.
7. ★ **Name 2 different topologies for a Botnet Command&Control structure. What are their advantages and disadvantages?**
   - **Centralized**: one central C&C structure sends commands to bots.
     - Pro: low latency
     - Con: easier to detect
     - Con: single point of failure, such as takedown or takeover of the C&C
   - **P2P**: bots communicate in a peer-to-peer structure.
     - Pro: robust
     - Con: higher latency and packet loss
     - Con: scalability problems
     - Con: more complex to manage
8. ★ **What is a monomorphic worm? Polymorphic? Metamorphic?**
   A monomorphic worm has a payload that does not change. It can still be fragmented in different ways, and this makes signature-based detection possible.
   Polymorphic means the payload changes but behavior stays the same.
   Metamorphic means both payload and behavior can change.

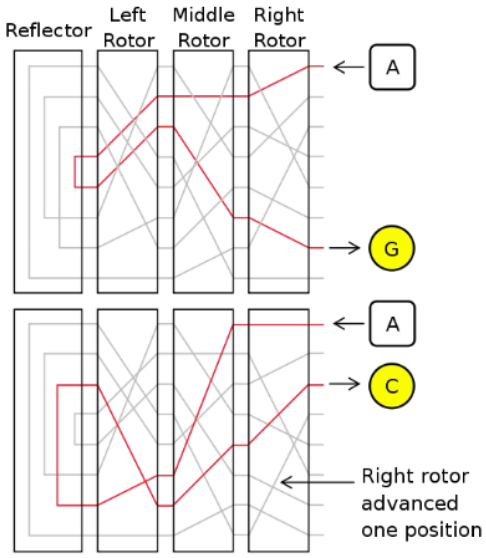
9. **In hybrid Command&Control structures, what are servent and client bots?**
   Servent bots act as server and client, often with public static IPs, and contact other servents. Client bots often sit behind firewalls or use private or dynamic IPs, contact servents, and do not accept incoming connections.
10. **List and explain the different evasion methods that are used to conceal the C&C.**
    Common methods are IP fluxing, double flux, domain flux, rogue DNS servers, and anonymization services such as Tor. These methods hide the real server, keep changing addresses or names, or route traffic through concealment layers.
11. **What are the most common obfuscation methods for botnet control traffic?**
    Encryption, tunneling such as HTTP or IPv6, traffic manipulation with low-volume traffic, and new channels such as social networks or steganography.

Ciphers

1. **What are the basic building blocks of cryptography? And In modern ciphers?**
   The basic building blocks are substitution and transposition. In modern ciphers, these are implemented as S-boxes and P-boxes, often combined into product ciphers.
2. **★ Decrypt a message with the Caesar cipher, k=3**
   Shift each ciphertext letter 3 positions backward. Example from the slide: `VHFUHW -> SECRET`.
3. **What is Letter Frequencies analysis?**
   You count how often letters occur in the ciphertext and compare that pattern to normal language frequencies. It helps break simple substitution ciphers.
4. **How does Vignère cipher work? How can it be broken? Calculate the ciphertext given a message and a key.**
   Vigenère uses a repeated key word. Each key letter chooses a shifted alphabet. To break it, first find the key length, for example with repeated patterns or the Kasiski idea, then do frequency analysis column by column.
5. **★ How does a One-Time Pad work?**
   The plaintext is represented as bits and XORed with a secret key of the same length. Security holds only if the key is random, secret, at least as long as the message, and used exactly once. Reusing the key leaks information.
6. **★ What distinguishes a good and a bad key for OTP? Name 4 properties for a good key.**
   It must be at least as long as the message, chosen randomly, kept secret, and used only once.
7. **★ Why is it a bad idea to use a OTP key twice?**
   If you reuse the same OTP key, an attacker can combine ciphertexts and learn information about the plaintexts.
8. **What it is meant with perfect security (or perfect secrecy)? And with computational security?**
   Perfect security means even an attacker with unlimited computing power cannot learn anything from the ciphertext. Computational security means breaking the cipher is possible in theory, but not with practical resources.
9. **What is the main Kerchoff's principle?**
   The system must stay secure even if the attacker knows the algorithm. Security must rely on the key, not on secrecy of the design.
10. **Explain, with a simple drawing, how do rotor machines for encryption work.**

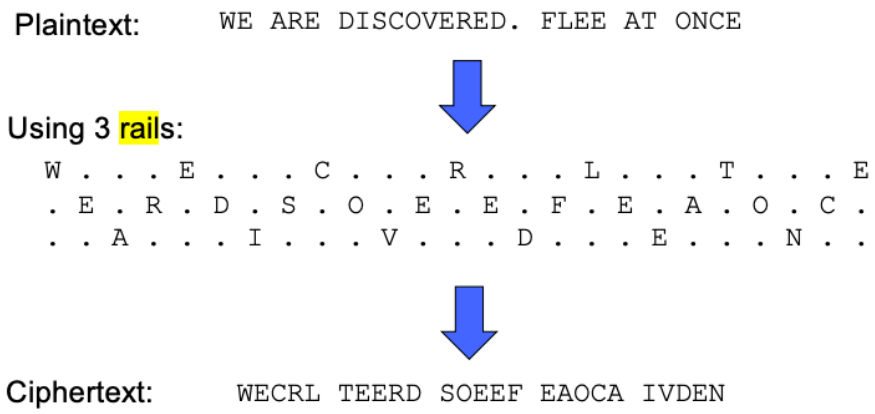
```
Keyboard -> Rotor 1 -> Rotor 2 -> Rotor 3 -> Reflector
            <- Rotor 1 <- Rotor 2 <- Rotor 3 <-
Lamp output
```

Each key press passes through rotating substitution stages, then back again.



11. **What is the difference between a substitution cipher and a transposition cipher?**
    A substitution cipher replaces units with other units. A transposition cipher keeps the units but changes their order.

12. **Encrypt a message using a Rail-Fence cipher with 3 rails.**
    Write the plaintext in a zig-zag over 3 rows, then read row by row. Example from the slide:
    `WE ARE DISCOVERED FLEE AT ONCE -> WECRLTEERDSOEEFEAOCAIVDEN`



13. **★ Can you use only Letter Frequencies analysis on a transposition cipher to get info about plaintext?**
    Yes, because the letters stay the same and their frequencies stay the same. It gives clues about the plaintext language, but it does not directly reveal the permutation.

14. **★ Explain the ciphertext-only, known-plaintext, chosen plaintext, and chosen ciphertext attacks.**
    Ciphertext-only means the attacker only has ciphertexts.
    Known-plaintext means the attacker knows some matching plaintext and ciphertext pairs.
    Chosen-plaintext means the attacker can choose plaintexts and get their ciphertexts.
    Chosen-ciphertext means the attacker can choose ciphertexts and get their plaintexts.

15. **What is a related key attack?**
    The attacker gets ciphertexts under different unknown keys, but the relation between those keys is known, such as a one-bit difference.

16. **★ Explain what is the difference between stream and block ciphers.**
    A **stream cipher** generates a keystream and combines it with plaintext bit by bit or byte by byte. It is fast, simple, needs no padding, and handles transmission errors well.

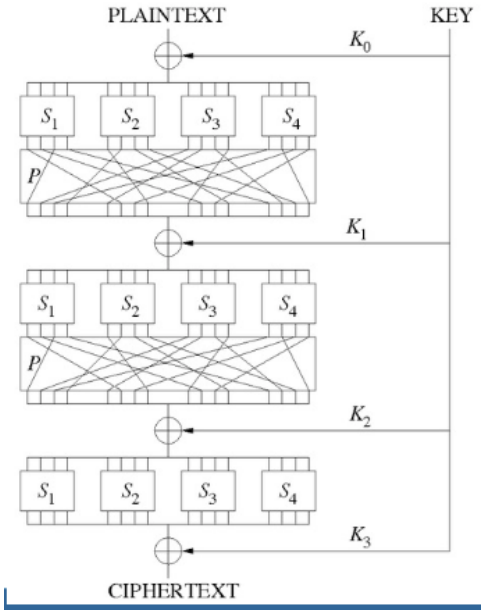
A **block cipher** processes fixed-size message blocks, often in sever al rounds using substitution and permutation. It is suited for bulk data, often offers stronger security, but is slower and can need padding.

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?**
    Advantage is the difference between the probabilities, so `0.9 - 0.2 = 0.7`. That is high, so this PRG is weak and not good.

Symmmetric Cryptography

1. **Draw the scheme of a SP (substitution-permutation) network**

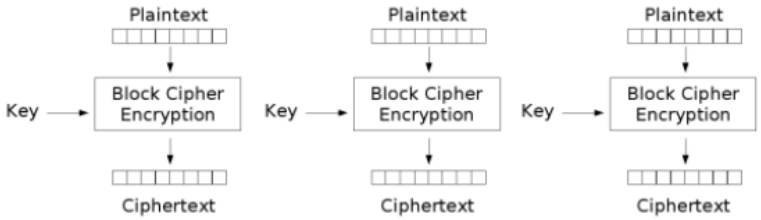
```
Plaintext -> Substitution layer -> Permutation layer -> Key addition -> rounds
-> Ciphertext
```



2. **A5/1: How is the encryption built?**
   Purpose: encryption of data in GSM networks
   A5/1 uses 3 linear feedback shift registers with lengths 19, 22, and 23 bits. They are clocked by a majority rule. A 64-bit seed initializes the registers, and the generated keystream is used to encrypt GSM traffic.
3. **RC4: How is the algorithm initialized?**
   Set `S[i] = i` for `i = 0..255`. Fill `K[i]` with the key repeated as needed. Then for each `i`, compute `j = (j + S[i] + K[i]) mod 256` and swap `S[i]` with `S[j]`. Finally set `i = j = 0`.
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)**
   Increase `i`, update `j`, swap `S[i]` and `S[j]`, then compute `t = (S[i] + S[j]) mod 256`. Output `S[t]`.
5. **What is an improper implementation of RC4, that lead to a known vulnerability in networks?**
   WEP used RC4 with a 24-bit IV prepended to a long-term key, and sent the IV in plaintext. This enabled the Fluhrer-Mantin-Shamir attack.
6. **★ Draw the functional blocks and the structure of a Feistel cipher**

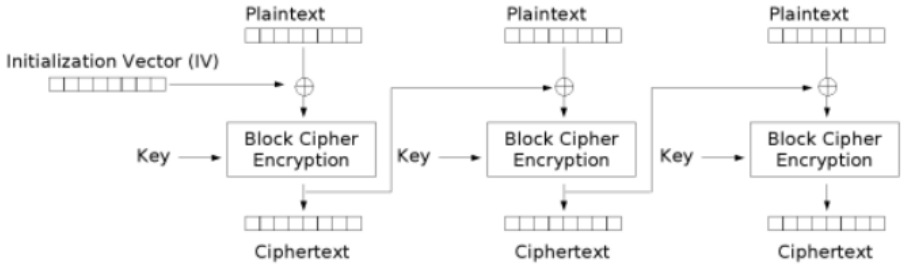
```
Input split into L and R

Round i:
L(i+1) = R(i)
R(i+1) = L(i) XOR F(R(i), K(i))
```

7. **DES: Which building blocks does DES use?**
   DES is a 16-round Feistel cipher with a 64-bit block size and a 56-bit key. Its round function uses expansion, XOR with subkey, S-box substitution, and P-box permutation. It also uses initial and final permutations.
8. **★ 2DES: If E(m,kA) is the encryption function for Single-DES: How does the encryption function for Double DES look like?**
   If single DES is `E(m, kA)`, then Double DES is `E(E(m, kA), kB)`.
9. **★ 3DES: Why isn't 3DES's encryption function E(E(E(m,k1),k2),k3)?**
   3DES uses encrypt-decrypt-encrypt for backward compatibility. If all three keys are equal, it reduces to single DES.
10. **AES: What are the 4 operations/steps of the AES cipher? How many rounds are performed?**
    The four steps are SubBytes, ShiftRows, MixColumns, and AddRoundKey. AES uses 10 to 14 rounds, depending on key length.
11. **★ How does Electronic Code Book (ECB) mode work?**
    Split the message into equal-size blocks, pad if needed, and encrypt each block independently.
12. **★ What can be used in an attack of ECB-encrypted messages?**
    Repeated plaintext blocks create repeated ciphertext blocks. An attacker can use these patterns to infer structure.
13. **Name and draw the five most common block cipher modes named in the lecture.**
    - **Electronic Codebook (ECB)**



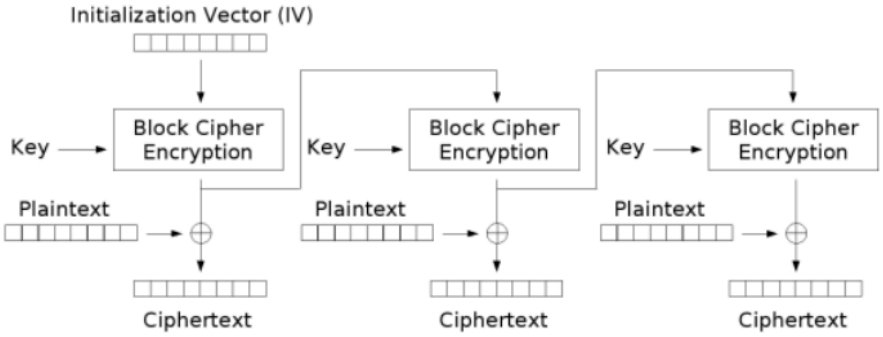
Electronic Codebook (ECB) mode encryption

    - **Cipher Block Chaining (CBC)**



Cipher Block Chaining (CBC) mode encryption

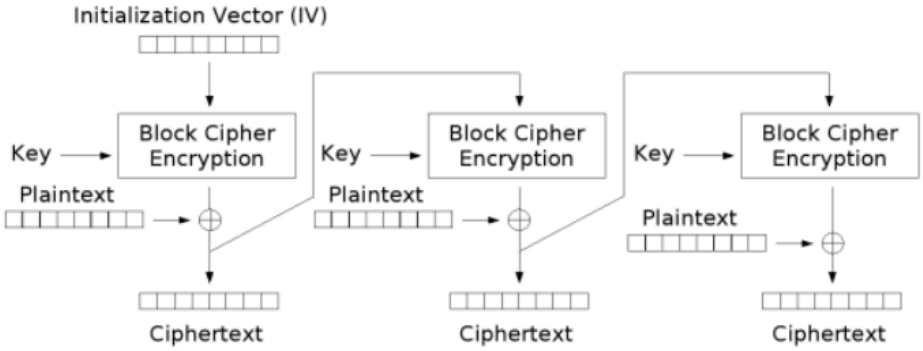
    - **Output Feedback (OFB)**



Output Feedback (OFB) mode encryption

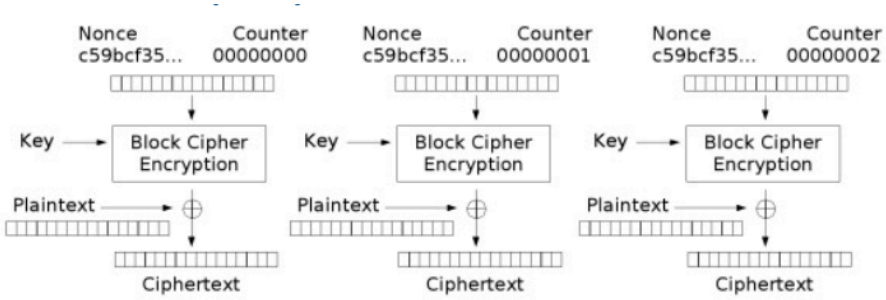
Source: wikipedia

- **Cipher Feedback (CFB)**



Cipher Feedback (CFB) mode encryption

- **Counter Mode (CTR)**

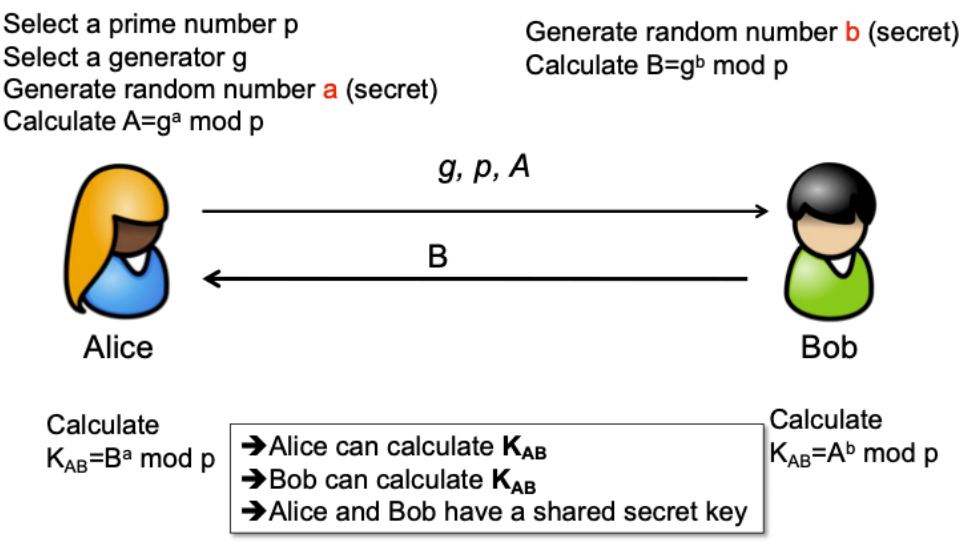


Counter (CTR) mode encryption

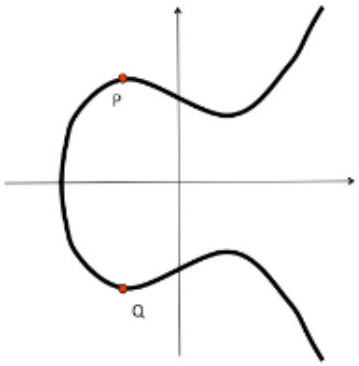
14. **What are the options for authenticated encryption?**
    Encrypt-and-MAC, MAC-then-encrypt, encrypt-then-MAC. The lecture states encrypt-then-MAC is the best option.
15. **Why isn't a CRC a good Message Authentication Code?**
    CRC uses no secret key. An attacker can modify the message and recompute the CRC.
16. **What is meant with CBC-MAC? What is the problem associated with it?**
    CBC-MAC uses the CBC residue, often the last block, as the MAC. Raw CBC output alone is not secure. Also, using the same key for encryption and MAC creates problems, so separate keys should be used.
17. **How is an HMAC built?**
    Adjust the key to block size. Compute an inner hash over `(key XOR ipad) || message`. Then compute an outer hash over `(key XOR opad) || inner_hash`.
18. **★ Name 5 properties that should be fulfilled by a cryptographic hash function.**
    Compression, efficiency, one-wayness, weak collision resistance, strong collision resistance.

Asymmetric Cryptography

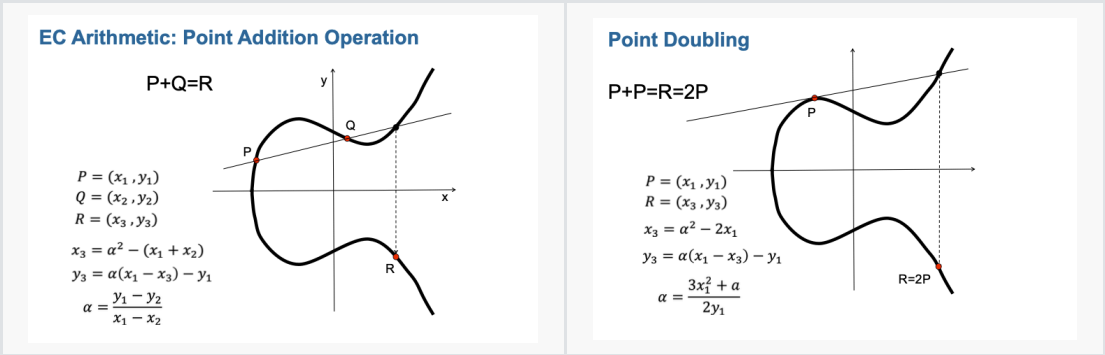
1. **★ What are private and public keys? What is the relation between them? When are these used to sign, encrypt, decrypt and verify a signature?**
   The private key is secret. The public key is published. They form a related key pair. Use the receiver's public key to encrypt. Use the receiver's private key to decrypt. Use the sender's private key to sign. Use the sender's public key to verify the signature.
2. **How can authentication be performed via asymmetric cryptography?**
   A simple method uses a nonce. Bob encrypts a random nonce with Alice's public key. Alice decrypts it with her private key and returns the nonce to prove possession of the private key.
3. **What is meant with discrete logarithm problem?**
   Given a generator `g`, a prime `p`, and `y = g^x mod p`, find `x`. For large cyclic groups, this is hard.
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.**
   Euler's totient function `φ(n)`. For a prime `p`, `φ(p) = p − 1`. For `n = pq` with distinct primes, `φ(n) = (p − 1)(q − 1)`.
5. **How does the Rivest-Shamir-Adleman trapdoor function work?**
   Choose large primes `p` and `q`. Compute `n = pq` and `φ(n)`. Choose `e` coprime to `φ(n)`. Compute `d` as the inverse of `e mod φ(n)`. Publish `(n, e)` and keep `d` secret. Encrypt with `e`. Decrypt with `d`.
6. **★ RSA: How are encryption and decryption functions for RSA?**
   Encryption is `c = m^e mod n`. Decryption is `m = c^d mod n`.
7. **★ RSA: How is a digital signature generated based on RSA?**
   Compute a hash of the message, sign the hash with the private key, and verify with the public key by checking that the recovered value matches the message hash.
8. **What is a Forward Search attack?**
   The attacker guesses a message, encrypts it with the public key, and compares the result to the observed ciphertext.
9. **Why do we need to introduce a random padding in messages encrypted with public-key cryptography?**
   Raw RSA is deterministic. The same message gives the same ciphertext. Random padding makes identical messages encrypt differently and hides structure.
10. **★ Sketch the Diffie-Hellman key exchange.**
    Public values are `p` and `g`. Alice chooses secret `a` and sends `A = g^a mod p`. Bob chooses secret `b` and sends `B = g^b mod p`. Alice computes `K = B^a mod p`. Bob computes `K = A^b mod p`. Both get the same shared key.



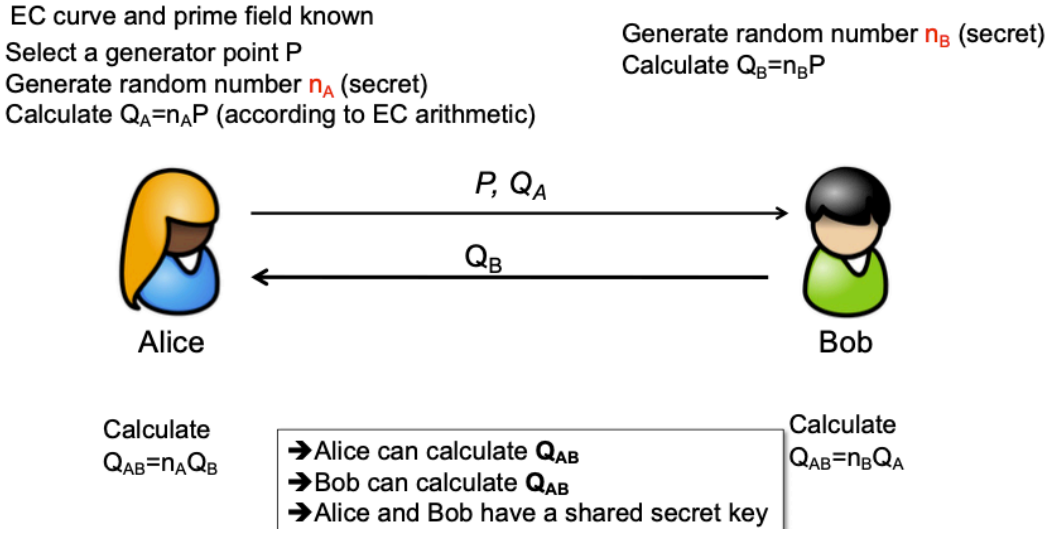
11. ★ **What is perfect forward secrecy?**
    If long-term keys leak later, past recorded sessions still stay protected. Ephemeral Diffie-Hellman gives this by using fresh temporary secrets and deleting them after the exchange.
12. ★ **Can you prove that a message signed from Bob (RSA) is valid (e.g. at court)?**
    Yes, in principle, because digital signatures provide non-repudiation. This requires that Bob's public key is correctly bound to Bob, for example by a certificate.
13. ★ **What is the difference between a message authentication code and a digital signature?**
    A MAC uses a shared secret key, so anyone with the key can create it. A digital signature uses asymmetric cryptography, so only the owner of the private key should be able to create it.
14. **ECC vs RSA, what is the advantages of using ECC in place of RSA?**
    ECC gives the same security level with smaller keys because the elliptic-curve discrete log problem is harder. This cuts computation, bandwidth, and storage.
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?**



`P + Q` gives another point on the curve, usually called `R`. `P + P` is point doubling, written `2P`.



16. **ECC: What is used as generator in elliptic curve encryption?**
    A generator point `P` on the elliptic curve.
17. **ECC: What are public and private parameters of ECC?**
    Public system parameters include the curve, the finite field, and the generator point. A user's private key is a secret scalar `n`. The public key is `Q = nP`.
18. **★ ECC: Sketch the Elliptic-Curves Diffie-Hellman key exchange.**
    Publicly choose curve parameters and generator point `P`. Alice picks secret `nA` and sends `QA = nA P`. Bob picks secret `nB` and sends `QB = nB P`. Alice computes `nA QB`. Bob computes `nB QA`. Both get the same shared point.

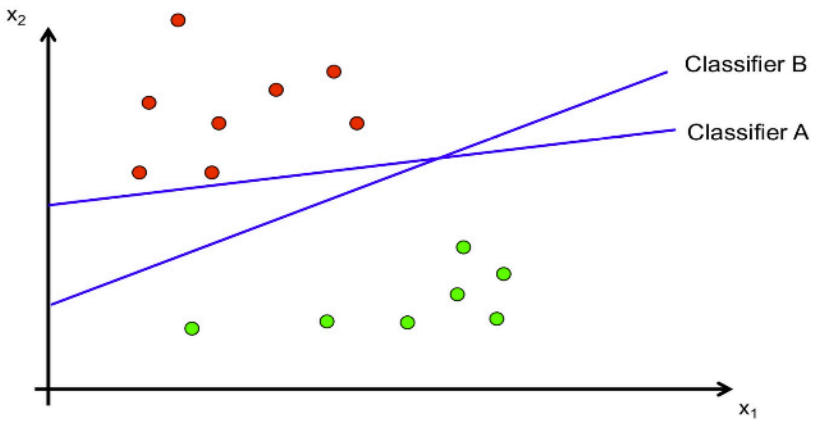


Anomaly Detection

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?**
   - Endpoint-to-endpoint transport mode
   - Security-gateway-to-security-gateway tunnel mode
   - Endpoint-to-security-gateway tunnel mode
3. **What is the Internet Key Exchange and what is its relation with IPsec?**
   IKE is the Internet Key Exchange protocol. It performs mutual authentication, negotiates algorithms, and establishes security associations and keying material for IPsec.

4. ★ **In TLS: (Multiple choice)**
   - ✓ The TCP Port is not encrypted
   - ✓ Client auth is optional
   - ✓ DH can be used for key exchange

   All three listed statements are true. The TCP port is not encrypted, client authentication is optional, and Diffie-Hellman can be used for key exchange.
5. **What are the main differences between IPsec and TLS?**
   IPsec works at the network layer and secures device-to-device communication, often for VPNs. TLS works above the transport layer, usually over TCP, and secures application-to-application communication.
6. **What is a traffic flow?**
   A flow is a set of packets with common properties.
7. **What are the four steps for traffic aggregation?**
   Timestamping, classification, selection, aggregation.
8. ★ **What is the darkspace?**
   Routed IP address space with no hosts attached. It mainly sees unidirectional unsolicited traffic such as scans, probing, and backscatter.
9. ★ **What is entropy? Distinguish between two samples, which one has higher entropy.**
   Measures *information content* of a message.
   Entropy measures how concentrated or dispersed a distribution is. A more dispersed sample has higher entropy. A highly concentrated sample has lower entropy.
10. ★ **How can entropy values be used to detect attacks?**
    Attacks change address and port distributions. Random scans create dispersion. Targeted attacks create concentration. DDoS and backscatter create characteristic entropy shifts. Comparing current entropy to normal values helps detect anomalies.
11. **What are the two detection techniques for attacks? What are their pros and cons?**
    Signature-based detection finds known patterns, is simple, and often has few false positives, but misses unknown attacks.
    Anomaly detection can find novel attacks, but needs a model or training and can produce false positives.
12. ★ **What is a point anomaly? Contextual anomaly? Collective anomaly?**
    A point anomaly is one unusual instance. A contextual anomaly is unusual only in a certain context. A collective anomaly is a group of instances that looks anomalous together.
13. ★ **What is the purpose of Support Vector Machines (SVMs)?**
    SVMs learn a classifier that separates classes by maximizing the margin between them.
14. ★ **What can be done if you only have a technique to learn a linear classifier but the data is not linear separable?**
    Transform the data into a higher-dimensional space where a linear separator can work.
15. ★ **Which classifier is better? How do we know? Which points are the support vectors?**



Classifier B is better.
In SVM, the better classifier is the one with the larger margin. You know this by comparing the distance from the decision boundary to the nearest data points. The support vectors are the points closest to the boundary, the ones that lie on the margin.

16. **What is meant with Area under the ROC curve?**
    This is the area under the curve of true positive rate versus false positive rate. A larger AUC means better overall discrimination.