Exercise 9 and 10

Question 1

a)
The brute-force cryptanalytic attack is countered by a strong encryption algorithm with large key sizes.
TLS uses strong symmetric ciphers like AES, which is 128 bits, making brute force attacks computationally infeasible with modern hardware.

b)
The known plaintext dictionary attack is countered by per session keys & initialization vectors.
The TLS uses unique session keys for each connection via key exchange, so all plaintext is known, the ciphertext will differ per session.
Also, forward secrecy ensures past sessions remain secure even if keys are compromised.

c)
The replay attack is countered by nonces, sequence numbers and per-session keys.
The TLS handshakes include random nonces and sequence numbers to ensure freshness. Any replayed handshake or data massage can fail verification due to mismatched session state or MAC.

d)
The MitM attack is countered by authentication via digital certificates. The server presents a digital certificate signed by a trusted Certificate Authority which allows the client to verify the server's identity.

e)
The password sniffing is countered by end-to-end encryption of application data.
Once the TLS handshake is complete, all HTTP data is encrypted so the password entered are not visible in the plaintext on the wire.

f)
The IP spoofing is countered by MACs and the session state tied to key exchange.
If an attacker fakes an IP address, they cannot generate valid encrypted and MAC-protected TLS records without the shared keys from the handshake. The TLS checks the integrity and aesthetics of a message.

h)
The SYN flooding is countered by TCP layer protections like: SYN cookies, firewalls or IPS. These defenses operate below the TLS layer and are designed to prevent the impact of a SYN flooding.

Question 2

a)
In the SSH protocol, the MAC is not encrypted because it is meant to authenticate the encrypted message. The MAC is computed over the plaintext packet data(before encryption) or the ciphertext (after encryption) depending on the exact mode, but it is always sent together with the encrypted data and is not itself encrypted.

b)
Some security advantages are:

1. Early detection of tampering: If the MAC is verified before decryption, the SSH can discard modified packets very early which will reduce the risk of ciphertext-based attacks like padding oracle attacks.
2. Prevention of resource-based DoS: If the MAC is invalid, the ssh does not waste resources trying to decrypt it. This will protect it against "denial of service" attacks that aim to overload the server with bugged packets.

Some performance advantages are:

1. Streamlined processing pipeline: The verification of MAC is efficiently done because packets are received without waiting for full decryption.
2. Efficiency with handling invalid data: Invalid spent packets are detected before the more expensive decryption step which is saving CPU cycles.

Question 3

a)
The PGP uses both symmetric and asymmetric encryption so it can have the best of both methods. The PGP generates a one-time symmetric key which will be used to encrypt the actual message using a fast symmetric algorithm. The message is being encrypted efficiently even if it is a large one. It encrypts the symmetric key with the percipient's public key using asymmetric encryption. This small piece of data is now secure and only the recipient can decrypt it using their private key. Both the encrypted message and the encrypted session key are sent both

When the recipient gets the message: they first use their private key to decrypt the symmetric key and then they use the symmetric key to decrypt the actual message.

b)
Some advantages of using this hybrid approach are:

1. Good performance: the symmetric encryption is fast and efficient for large messages while asymmetric encryption is slow and computationally heavy, especially for big data, being used only to encrypt the small symmetric key.
2. Security: the symmetric key is never transmitted in the clear, it's encrypted using recipient's public key. This ensures confidentiality even if the message is intercepted, the symmetric key is protected.
3. Scalability and flexibility: a small part of the message needs to be encrypted for each recipient. This means that we can send the same encrypted message to multiple recipients by encrypting the same symmetric key with each recipient's

4. Key management: Asymmetric keys are used for identity and key exchange. They separate long-term keys which are asymmetric from temporary keys which are symmetric, improving overall security.