# Cryptography Task - Theoretical

# Question 1

**What is encryption? Why do we need it?**  
Cryptography is the practice and study of techniques for securing communication and data in the presence of adversaries.  
It take a plaintext message and converts it to a sequence of random characters and numbers illegible to humans.  
Encryption is essential for communicating or sharing information over the network because it allows you to detect and flag tampering.

# Question 2

**Name three features of encryption and why encryption is beneficial to us.**  
It may secure data security, protect data from unwanted modification, and authenticate data sources.  
  
Confidentiality: It means ensuring that no one can read a message except the intended receiver.   
It also means keeping data secret from those without the proper credentials, even if this data passes through an insecure network.  
  
Integrity (Anti-Tampering): It means ensuring the receiver that the received message has not been altered in any way from the original.  
  
Authentication: It is the process of proving one’s identity.   
  
Non-Repudiation: A repudiation is a rejection or denial of something's validity, such as refusing to fulfill a legal contract. Non-repudiation refers to mechanisms that prove that the sender sent the message.

# Question 3

**Name at least five major applications for cryptography.**  
Authentication/Digital Signatures  
Time Stamping  
Electronic Money  
Secure Network Communications(SSL,Kerberos)  
Anonymous Remailers  
Disk Encryption

# Question 4

**A cypher works in conjunction with a key to encrypt plaintext. Different keys will generate different cyphers for the same plaintext.  
  
There are two types of key cryptography: symmetric and asymmetric. Explain each type of cryptography and the techniques behind it.&nbsp;  
  
  
Symmetric &nbsp;  
Asymmetric**  
Symmetric: The sender and receiver of a message share a single key for encrypting and decrypting the message.  
  
Asymmetric: Asymmetric cryptography, also known as public-key cryptography, is a cryptographic algorithm that requires two separate keys, one private and the other public. The message is encrypted with the public key and decrypted with the private key. As a result, anyone with the public key can encrypt but not decrypt information. The information can only be decrypted by someone who has the corresponding private key.

**Why do we need asymmetric key cryptography?**

**Name at least two advantages and disadvantages of both symmetric and asymmetric key cryptography.**

# Question 5

**Explain what RSA is and its main uses.**  
RSA, which stands for Rivest-Shamir-Adleman, is a widely used cryptographic algorithm for public-key encryption and digital signatures.  
  
-Public-Key Encryption: RSA is primarily used for secure communication and data transmission over insecure networks, such as the internet.   
  
-Digital Signatures: RSA is used for creating digital signatures, which provide integrity, authenticity, and non-repudiation of digital documents or messages.   
  
-Key Exchange: RSA can also be used for secure key exchange between two parties. By encrypting a shared symmetric key with the recipient's public key, the sender can securely transmit the key to the recipient, who can then decrypt it using their private key. This allows them to establish a shared secret key for further secure communication using symmetric encryption algorithms.  
  
-SSL/TLS Encryption: RSA is an integral part of the SSL/TLS (Secure Sockets Layer/Transport Layer Security) protocols, which provide secure communication between clients and servers over the internet. RSA is used during the initial handshake process to establish a secure connection and exchange session keys.

# Question 6

**What is SSL, and what is an SSL certificate?**  
SSL is a global standard security technology that enables encrypted communication between a web browser and a web server. An SSL certificate authenticates the identity of the website and encrypts the data that’s being transmitted.

# Question 7

**What is hashing?**  
Hashing is the process of converting an input into a fixed-size string of text using a mathematical function, making it unreadable. Each hash value is unique.

# Question 8

**Hashing has several uses.&nbsp;Name three of these.**  
oFile verification   
oPassword storage   
oDatabase searching

**Choose one of the uses you named in the previous question and explain it.**  
oFile verification – to check the integrity of a downloaded file, you can generate its hash and compare it to the hash provided by the site where the file originated. If they match, the file has not been altered.  
oPassword storage – when you create a password on a secure system, it first hashes the password, then stores the hash. This way, if the hashed database is stolen, it cannot be read by bad actors.  
oDatabase searching – hashing can enable faster database searches, if the hash value is shorter than the input.

# Question 9

**What is the main difference between encryption and hashing?**  
While hashing output cannot be converted back to its original form, encrypted messages can be converted back to their original form.

# Question 10

**Give examples of cases in which hashing should be used and cases in which encryption should be used. Explain your answers.**  
Hashing is used for:   
oFile verification - Checking the hashed value of a file, users can verify that the file is indeed the correct file and hasn’t been tampered with.   
oPassword storage – When the hash-value of passwords are saved, rather than their plaintext value, systems compare the hashed value of an entered password against the value stored in the system to verify the identity of a user. This adds an extra layer of protection and prevents attackers from retrieving passwords in plaintext form.   
Encryption is used for:   
oTransferring information that will need to be converted back into its original form. The sender encrypts the data using the recipient's public key. Only the intended recipient can decrypt the file using their private key. Even the sender cannot decrypt the information once it has been encrypted.

# Question 11

**Cryptographic systems face several threats.&nbsp;Explain at least three of these. You may use the following article&nbsp;for reference.**  
http://www.crypto-it.net/eng/attacks/index.html   
  
Ciphertext-only attack – only the ciphertext is known to the attacker. If the hacker is in statistics, then they can use various statistical techniques to break the ciphertext back into the plaintext.   
  
Known-plaintext attack – this occurs when the hacker knows some aspect of either the letter pairings, and then can consequently break the ciphertext back into the plaintext.  
  
Chosen-plaintext attack – the hacker can choose the plaintext and view the encrypted output which is transmitted across the network. Then they can reverse-engineer it back into ciphertext to figure out the encryption.   
  
Adaptive chosen-plaintext attack – like a chosen-plaintext attack, except the attacker can choose subsequent plaintexts based on information learned from previous encryptions.   
  
Related-key attack – like a chosen-plaintext attack, except the attacker can obtain ciphertexts encrypted under two different keys. The keys are unknown, but the relationship between them is known.

**Choose one of the threats you explained in the previous question and explain how you, as a future cybersecurity expert, can protect your network from it.**  
Protecting against a ciphertext-only attack involves implementing strong encryption practices and security measures. For example:  
  
-Use strong encryption algorithms: Ensure you use modern, well-vetted encryption algorithms, such as AES (Advanced Encryption Standard), which is widely regarded as secure. Avoid older or deprecated algorithms that may have known vulnerabilities.  
  
-Choose a long and complex encryption key: The strength of your encryption relies heavily on the encryption key. Select a key that is long, complex, and randomly generated. Longer keys provide greater resistance against brute-force attacks.  
  
-Implement key management best practices: Safeguard your encryption keys carefully. Employ secure key management practices, such as storing keys in protected environments, using hardware security modules (HSMs), or employing key management systems that adhere to industry standards.  
  
-Use secure key exchange protocols: When exchanging encrypted data or keys, employ secure key exchange protocols like Diffie-Hellman (DH) or Elliptic Curve Diffie-Hellman (ECDH) to prevent eavesdropping or interception.  
  
-Protect against insider threats: Be vigilant against insider threats that might compromise the security of the ciphertext. Implement access controls, monitor user activities, and follow the principle of least privilege to minimize the risk of unauthorized access.  
  
-Employ multi-factor authentication (MFA): Utilize MFA to add an extra layer of protection. By requiring multiple factors (e.g., password, physical token, biometric), you reduce the likelihood of unauthorized access to the encrypted data.  
  
-Regularly update and patch systems: Keep your encryption software and systems up to date with the latest security patches and updates. This ensures that any known vulnerabilities are addressed promptly.  
  
-Implement strong network security: Protect the network infrastructure where the ciphertext is transmitted or stored. Utilize firewalls, intrusion detection systems (IDS), and secure communication protocols (e.g., HTTPS) to prevent unauthorized access or eavesdropping.  
  
-Perform regular security audits: Conduct periodic security audits and penetration tests to identify any vulnerabilities in your encryption implementation or infrastructure. Address any findings promptly to maintain the security of your ciphertext.

# Question 12

https://www.commonlounge.com/discussion/c229f8b825d249b8aeab9f4135bb4f42  
 MD5 SHA-2  
Stands forMessage Digest 5 Secure Hash Algorithm 2  
Main usesChecksum calculations   
 and data integrity verificationCryptographic applications (password   
 storage and proof-of-work for the Bitcoin   
 cryptocurrency)  
Length 128 bits 256 bits  
Security Vulnerable to collision attacks and   
 brute-force attacks Vulnerable to length extension attacks  
Speed Faster than SHA-2 Slower than MD5

# Question 13

**Which hash type is preferable, MD5 or SHA-2? Why?**  
SHA-2 (Secure Hash Algorithm 2) is a family of cryptographic hash functions that includes SHA-224, SHA-256, SHA-384, and SHA-512, among others. These algorithms provide stronger security properties compared to MD5. SHA-2 hash functions produce hash values of different lengths (e.g., 256-bit, 512-bit) and are designed to be resistant to various attacks, including pre-image attacks, second pre-image attacks, and collision attacks.  
  
The security of SHA-2 algorithms has been extensively analyzed and scrutinized by the cryptographic community, and they have stood up to rigorous scrutiny so far. Consequently, SHA-2 is widely recommended for various cryptographic applications, including password hashing, digital signatures, and data integrity checks.

# Question 14

**Which encryption techniques discussed in this task would you implement in your network and why?**  
To prevent cryptography attacks, it is essential to have a strong cryptographic system in place. Some of the ways to achieve this are:  
  
-Regularly update the cryptographic algorithms and protocols to ensure they are not obsolete.  
-Ensure that the data is appropriately encrypted so that even if it falls into the wrong hands, it will be unreadable.  
-Use strong and unique keys for encryption.  
-Store the keys in a secure location.  
-Ensure that the cryptographic system is implemented correctly.  
-Regularly test the system for vulnerabilities.  
-Educate employees about cryptography attacks and how to prevent them.