**Cryptography Task – Answers**

Theoretical Questions:

1. What is encryption? Why do we need it?

Encryption is a method of disguising plaintext to hide its contents. It ensures that information is hidden from everyone but its intended recipients, even if they can see the encrypted data.

2. Name 3 features of encryption and explain why it benefits us.

* Confidentiality
* Integrity
* Authentication
* Non-repudiation

3. Name at least 5 major application for cryptography in the modern world.

* Chip based payment cards
* Computer and other passwords
* E-commerce
* Defense communications
* Digital currencies
* Designing protocols
* Data authenticity

4. A cipher is a function used for encryption and decryption. A cipher works in combination with a key to encrypt the plaintext. The same plaintext encrypts to different ciphertext with different keys.

* There are two types of key cryptography: symmetric and asymmetric. Explain what every type of cryptography is and how each of these techniques work.
  + Symmetric – an encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message.
  + Asymmetric – an encryption system that requires two separate keys, one of which is private and one of which is public. The public key is used to encrypt the message, and the private one is used to decrypt it.
* Why do we need an asymmetric key cryptography?

If a sender and a recipient are in different physical locations, they need to trust a network to protect the confidentiality of the secret key during their communication. Asymmetric key cryptography solves the problem of getting the key to a recipient without it being intercepted.

* Name at least 2 advantages and disadvantages for symmetric and asymmetric key cryptography.

| **Cryptography** | **Advantages** | **Disadvantages** |
| --- | --- | --- |
| Symmetric | Simple and easy to use  Very fast | Key storage and recovery  Key distribution  Key distribution |
| Asymmetric | Enables key exchange in secure networks | Very slow  More difficult to use |

5. Explain what RSA is and what are its main uses.  
RSA is an algorithm for asymmetric key cryptography. It is suitable for signing as well as encryption, and one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols and is believed to be secure given sufficiently long keys and the use of up-to-date implementation.

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.

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.

8. There are several uses for hashing.

* Name 3 uses of hashing:
  + File 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.
  + Password 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.
  + Database searching – hashing can enable faster database searches, if the hash value is shorter than the input.
* Choose one of the uses you named in the previous question and explain it.

In the previous answer.

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.

10. In which cases would you use hashing and in which cases would you use encryption? Explain your answers.

* Hashing is used for:
  + File 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.
  + Password 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:
  + Transferring 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.

11. There are several threats for a cryptographic system.

* Explain at least 3 of these threats. You may use the following article: <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 cyber security 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.

12. Read the following article and fill in the table: [https://www.commonlounge.com/discussion/c229f8b825d249b8aeab9f4135bb4f42](http://www.commonlounge.com/discussion/c229f8b825d249b8aeab9f4135bb4f42)

|  | **MD5** | **SHA-2** |
| --- | --- | --- |
| Stands for | Message Digest 5 | Secure Hash Algorithm 2 |
| Main uses | Checksum calculations and data integrity verification | Cryptographic 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 |

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.

**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.