# Cryptography Assignment

## Section 1: Short answer questions: (24 points)

### 1. What is cryptography, and what are its main goals?

The process of encoding and decoding data using mathematical computations to ensure its confidentiality, reliability, and validity is known as cryptography. The key purposes of cryptography are:

* Privacy: To ensure that sensitive information isn't accessible to unauthorized parties. With the help of cryptographic procedures, plaintext can be converted into ciphertext, which is unintelligible to anyone who lacks the necessary decoding key.
* Respectability: To ensure that no alterations or tampering were made to the data while it was being transmitted. Cryptographic calculations can detect any unauthorized alterations made to the data, no matter how minor they may be.
* Validation: To verify the character of the parties involved in a correspondence. Calculations using cryptography can prove that the communication originated from the claimed source and wasn't created by a fraud.
* Non-disavowal: To prevent the sender of a message from retracting responsibility for sending it. A message was unquestionably transmitted by the promised shipper and received by the predicted beneficiary, according to cryptographic computations.

### 2. What is a block cipher, and what is a stream cipher?

A symmetric encryption calculation known as a block figure encrypts fixed-size blocks of data, typically 64 or 128 pieces at a time. The block figure processes the data in a deterministic manner, suggesting that when encoded with a comparable key, similar data would always yield similar results. For secure information transmission, such as in the calculation of the High-level Encryption Standard (AES), block figures are typically used.

Instead of encoding data in fixed-size blocks, a stream figure uses symmetric encryption to encode characters or bits of information one at a time. Since they can process the information as it is being supplied, stream figures are suitable for continuous applications like scrambling web-based audio or video. Stream figures are frequently faster than block figures and require less memory, but they can also be less secure because a single error in the encryption cycle can result in several pieces in the decoded output.

The choice between block codes and stream figures depends on the specific security requirements and execution requirements of the program. Both block ciphers and stream figures have advantages and disadvantages.

### 3. Explain the difference between asymmetric encryption and symmetric encryption.

Asymmetric encryption and symmetric encryption are two distinct types of encryption methods that are used to secure sensitive data and enable communication.

A similar key is used for both encryption and decoding in symmetric encryption, also known as shared secret encryption. In this method, the message's sender and receiver each possess a comparable mystery key, which they use to encrypt and decrypt the message, respectively. While symmetric encryption is rapid and efficient, it has the drawback that the shipper and collector must safely share the secret key, which can be challenging in some situations.

A public key and a private key are used for encryption and decoding in asymmetric encryption, also known as public-key encryption. The communication is encrypted using the confidential key to decrypt it and the public key to scramble it. Anyone can send a message to the owner of the confidential key that has been encrypted using the public key, which can be freely distributed, but only that person has the ability to decode the message. Asymmetric encryption provides a solution to the symmetric encryption problem with key circulation, but it is slower and requires more processing resources.

In summary, asymmetric encryption provides a secure technique for key exchange and lays out a fundamental mystery for symmetric encryption, whereas symmetric encryption is used to efficiently encrypt and decrypt large amounts of data. Practically speaking, many encryption systems combine symmetric and asymmetric encryption to provide security and performance.

### 4. What is a hash function, and why is it used in cryptography?

An information (or "message") is passed through a hash function, a mathematical operation that outputs a fixed-size yield that is typically a "review" or "hash esteem." Since the hash function is designed to be a one-way function, switching the cycle and reproducing the first input from the hash value is computationally impossible. It should be computationally impossible to identify two different data sources that yield the same hash value or to find information that produces a certain hash value because hash functions also possess the qualities of crash blockage and preimage opposition.

Several purposes of hash functions in cryptography include:

* Message integrity: To ensure that a message has not been altered while in transit, a hash function can be used to create a digital fingerprint of the message. This fingerprint can then be delivered along with the message. The message's recipient can recompute the hash value and compare it to the original value to verify that the message has not been changed.
* Stockpiling of secret words: By registering a hash value of the secret phrase and storing the hash value rather than the secret phrase itself, hash functions can be used to securely store passwords.
* When a client inputs their secret phrase, the system logs the hash value of the entered secret phrase and compares it to the stored hash value to verify the client's identity.
* Hash functions can be used to sign electronic messages or verify the validity of electronic endorsements. The sender of the message can calculate its hash value, encrypt it using a secret key, and deliver both the message and the scrambled hash value to the recipient. The beneficiary can use the source's public key to decode the message's scrambled hash value, calculate the message's hash value again, and compare it to the message's unscrambled hash value to verify the message's authenticity.

### 5. What is digital signature, and how does it ensure authenticity and integrity of a message?

A digital signature is a method for ensuring the validity and reliability of a digital communication or record. A digital signature provides proof that the communication originated from a certain source and was not changed during transmission.

The following innovations are frequently present in the most typical method of creating a digital signature:

* Hashing: A hash capability is used to handle the message and provide a new, fixed-size output known as a hash value or message digest.
* With the help of the sender's private key, the hash value is then encrypted.
* Transmission: The beneficiary receives the first message and the hash value that has been scrambled.

The beneficiary then does the supporting actions to verify the veracity and honesty of the message:

* Decoding: The sender's public key is used to decode the scrambled hash value.
* Hashing: The beneficiary uses a capability that is comparable to the shipper's to process the first message's hash value.
* Examination: The beneficiary compares the recently processed hash value to the unscrambled hash value. The recipient can be certain that the communication originated with the shipper and was not changed during transmission if the attributes match.

The use of a private key to encrypt the hash value and a public key to decode it ensures that only the owner of the private key could have created the digital signature, and it enables anybody with the public key to verify the authenticity and validity of the message.

In summary, a digital signature is a great tool for ensuring the truth and veracity of digital communications and reports, and it is frequently used in secure communication, online commerce, and digital declaration of authority.

### 6. Diffi-hellman and RSA are two asymmetric encryption methods. Explain the similarities and difference between the two.

Two well-known asymmetric encryption techniques used to obtain communication and protect sensitive data are Diffie-Hellman and RSA. They both use public key cryptography, which has the advantage of enabling communication between two groups without the need for an earlier shared secret.

The following are some similarities between RSA and Diffie-Hellman:

* Both use public key cryptography, which encrypts and decrypts data using two keys: a public key and a confidential key.
* Both allow the creation of a common mystery between two groups without the need for an earlier shared key, thus providing a solution to the key conveyance problem of symmetric encryption.
* Both guarantee the confidentiality, truthfulness, and reliability of the information being conveyed.

The distinctions between RSA and Diffie-Hellman include:

* Key exchange versus encryption: While RSA may also be used for encryption and advanced marks, Diffie-Hellman is mostly used for key exchange.
* Key age: Diffie-Hellman establishes a common mystery due to the use of measurable mathematics, whereas RSA does so due to the factorization of extremely large indivisible numbers.
* Speed: RSA often runs slower than Diffie-Hellman, especially for larger key sizes.
* Key size: Compared to Diffie-Hellman, RSA requires larger key sizes to provide equivalent security.

### 7. What is a cipher, and give an example of a popular cipher used today?

A cipher is a calculation that is used to encode and decode data, converting plain text into ciphertext and vice versa. A cipher's goal is to render the initial message undecipherable to anybody without access to the key.

There are several different types of ciphers, including block ciphers, stream ciphers, symmetric ciphers, and lopsided ciphers.

The High-Level Encryption Standard is arguably one of the most well-known ciphers currently in use (AES). The U.S. government decided on the symmetric block cipher AES as the standard for encryption and decryption. AES allows key length of 128, 192, or 256 pieces and uses an appropriate block size of 128 pieces. AES is typically used for encryption of sensitive information, such as financial transactions, military coordination, and secure data storage in devices like PCs and mobile phones.

### 8. What is a key, and why is it important in cryptography? What does a key do the plain text?

In cryptography, a key is a value that is used to encode and decode data. The key determines the outcome of the code calculation, making it a fundamental component of the encryption interaction. Similar data and calculations in cryptography will provide different results depending on the key used.

The role that the key plays in maintaining the confidentiality and safety of the information being communicated in cryptography is important. If the key is known to an unauthorized party, they can use it to decrypt the scrambled data and access sensitive information. On the other hand, if the key is kept secret and protected, the data will remain scrambled and secure.

Using the encryption calculation and the key, the plain text is converted into ciphertext during the encryption cycle. The key functions as a set of instructions for the encryption algorithm, determining how plain text is converted into ciphertext. The encryption is reversed and the ciphertext is transformed back into the original plain text using the key in the unscrambling system.

In summary, the key is a crucial component of cryptography since it provides the means to access and protect sensitive data. The key functions as the encryption algorithm's rules, determining how plain text is converted to ciphertext and how that text can be decoded back into the original plain text.

### 9. What is a certificate authority, and why is it important in cryptography?

An organization called a Certificate Authority (CA) is in charge of issuing and managing digital certificates that are used to securely verify the identity of individuals, organizations, and systems. The role of a CA is to assist a trusted outsider who can verify a substance's personality and then issue a digital certificate to that component.

A digital certificate includes information on the character of the element, such as its name and public key, as well as information about the CA that issued the certificate, such as its name and mark. The certificate is used to establish confidence between the element and other parties, such as customers or systems.

The importance of a Certificate Authority in cryptography is seen in its role in establishing confidence in encrypted communication. A certificate issued by a reputable CA can be used to verify an element's identity, enabling secure communication without the risk of eavesdropping or alteration.

For instance, when a user accesses a website that uses SSL/TLS encryption, their browser will check the site's digital certificate to make sure it was issued by a reputable CA. The application will set up a protected relationship with the site, allowing the client to exchange data with the site safely, if the certificate is valid and was issued by a reputable CA.

In summary, the Certificate Authority plays a crucial role in cryptography by acting as a trusted third party that can verify the legitimacy of substances and issue digital certificates, enabling secure communication and protecting against eavesdropping and alteration.

### 10. Discuss the challenges and limitations of cryptography and explain how they are being addressed by researchers and practitioners.

The discipline of cryptography is complex and is subject to various limitations. Some of the basic challenges and limitations of cryptography include:

* Key management: One of the biggest challenges in cryptography is safely managing cryptographic keys. If the key is misplaced or compromised, the encrypted data can be easily decoded by an unauthorized party. This can be particularly challenging in frameworks with broad scope and lots of customers and keys.
* Cryptanalysis: As encryption computations and protocols advance, attackers also advance in their ability to crack the encryption. Cryptanalysis, which is challenging for cryptography, is the study of methods for overturning encryption calculations and standards.
* Flexibility: Cryptography calculations can become computationally expensive, which makes scaling their use in large-scale frameworks difficult. Limitations on execution and increased expenditures may result from this.
* Usefulness: Cryptography can be difficult for users to understand and apply, which can lead to poor reception and misconfiguration. As a result, security vulnerabilities may arise that attackers may exploit.

These challenges are being addressed by researchers and practitioners in a variety of ways, including:

* Key management: New important management frameworks and standards that are safer and easier to use are being developed by researchers. To reliably store and manage cryptographic keys, innovations like quality administration servers and hardware security modules (HSMs) are being developed.
* Cryptanalysis: To make encryption algorithms and conventions more resistant to attacks, researchers are constantly evaluating and improving them. This takes into account the development of new encryption formulas and practices that are meant to be more resistant to cryptanalysis.
* Adaptability: New cryptography computations and standards are being developed by researchers that are more effective and versatile, making it possible to integrate cryptography into larger systems with less impact on performance and cost.
* Convenience: Researchers are working to improve cryptography's usability, making it easier for users to understand and use securely. This includes the development of new user interfaces and tools that are designed to improve the use of cryptography and reduce the risk of misconfiguration.

### 11. List two symmetric encryption algorithms.

There are two well-known symmetric encryption algorithms:

* High level Encryption Standard (AES): AES is a widely used encryption algorithm that is renowned for its excellent presentation and strong points. It supports key sizes of 128, 192, or 256 pieces and uses a correct block size of 128 pieces.
* Blowfish: Blowfish is a symmetric encryption algorithm that is quick, safe, and designed to be basic and easy to use. It uses a configurable block size and accommodates keys with 32–448 pieces.

For some applications, AES and Blowfish are both widely used and regarded as secure. The choice between the two is based on the application's specific requirements, such as implementation, security, and execution complexity.

### 12. What determines the strength of an encryption key?

There are still a few unknowns that could affect how strong an encryption is, such as:

* Key size: The size of the key may be the primary factor determining its strength. Given that there are more possible mixes, a longer key provides greater security than a shorter one. According to a commonly used rule, symmetric encryption with a key size of 128 pieces is considered secure, while lopsided encryption with a key size of 2048 pieces or more is considered secure.
* Key entropy: Key entropy refers to the key's arbitraryness, is still another important factor determining its strength. Since it is easier to imagine or use brute force, a key with a high entropy is considered to be safer than one with a low entropy.
* Key management: Key management techniques, such as key pivot, strengthening, and capacity, are also crucial in determining the reliability of an encryption key. Unlucky key management procedures may result in a key being lost or compromised, lowering the encryption's overall security.
* Computation strength: A factor used to determine the strength of the key is the strength of the encryption computation used to scramble the information. Even if the actual key is weak, a strong encryption calculation allows a facility to obtain encryption.

## Section 2: Vernam/ XOR Encryption Exercise (16 points)

Using the following 8 bit key choose two letters from the ASCII table and reveal the ciphertext you get for each character after applying the key. (Remember the decimal value of an ASCII character can be converted into a 8 bit binary number).

**Key 10011010 | 8 bit key**

**===============================**

**ASCII Character 1: M**

**Cipher Text character 1: Ô**

**===========================**

**ASCII Character 2: K**

**Cipher Text character 2: Ñ**

**===========================**

|  |  |  |
| --- | --- | --- |
| ASCII Character | M | K |
| Decimal Value | 77 | 75 |
| Binary Value | 01001101 | 01001011 |
| Encryption Key | 10011010 | 10011010 |
| XOR Operation Value | 11010111 | 11010001 |
| Decimal Value of XOR | 215 | 209 |
| Cipher Text Character | Ô | Ñ |