كلية الهندسة - جامعة الزقازيق

2024/2023

الفرقة: الرابعة هندسة الحاسبات والمنظومات

المقرر: شبكات الحاسب

الإسم: عبدالرحمن رجب عبدالباقي احمد

الرقم في السكشن : 16

رقم الجروب :7

وإسم الموضوع :Cryptography

Modern Cryptography Techniques

1. Introduction

Encryption is a concept that involves manipulating strings (or text) to make them unreadable for an intermediary person. It provides an effective way to encrypt or decrypt text from other parties. Examples include Caesar Cipher, Columnar Cipher, and more. To develop a custom encryption algorithm, hybrid encryption algorithms can be utilized.

2. Custom Building Cryptography Algorithms (Hybrid Cryptography)

I Hybrid encryption is a cryptography concept that combines or merges one or two encryption algorithms to generate more effectively encrypted text.

2.1 Advantages of Hybrid Cryptography

Hybrid cryptography algorithms are highly effective, making it challenging to detect patterns and decode messages easily. In these algorithms, a combination of mathematical functions is employed to enhance the overall security of the encryption process.

2.2 Example of Hybrid Cryptography

- Symmetric Encryption:

In this type of encryption, the same key is used for both the encryption and decryption processes. In the example, the sender employs a custom algorithm and a single key to encrypt the message.

- Asymmetric Encryption:

Here, two different keys are used—one for encryption and the other for decryption. In the example, the custom key is encrypted using the recipient's public key. Only the recipient, with their private key, can decrypt this key and subsequently decrypt the message.

In essence, symmetric encryption uses the same key for both encryption and decryption, while asymmetric encryption uses two different keys. In the example, a custom algorithm is employed for symmetric encryption, and a standard algorithm (such as RSA) is used for asymmetric encryption.

2.3 Disadvantages of Custom Hybrid Cryptography

- Security Risks:

Custom algorithms may have security vulnerabilities due to limited scrutiny.

- Lack of Standardization:

Custom algorithms lack the widespread review that standardized algorithms benefit from.

- Maintenance Challenges:

Custom algorithms may lack ongoing updates and maintenance.

- Key Management Complexity:

Managing custom keys can be complex, especially with many users or systems.

- Interoperability Issues:

Custom algorithms may face issues when communicating with systems using standard algorithms.

3. An Overview of Cloud Cryptography

Cloud Cryptography involves encrypting data stored in the cloud to ensure its security. Various security measures are implemented in cloud cryptography to provide a robust layer of protection, preventing breaches, hacks, or malware attacks. Encryption is applied to any data hosted by cloud providers, enabling users to access shared cloud services securely and conveniently. Cloud Cryptography effectively secures sensitive data without causing delays in the delivery of information.

3.1 How does cryptography in the cloud work?

Cloud cryptography involves the application of cryptographic protocols and algorithms to secure data stored in the cloud. It ensures the confidentiality, integrity, and availability of sensitive information, even in a shared and dynamic cloud environment.

3.2 How is data in the cloud protected using cryptography

Securing data in the cloud through cryptography involves applying encryption methods to safeguard stored information. This ensures a similar level of security for cloud services without compromising data transmission speed. Various cryptographic protocols are defined by organizations to strike a balance between security and efficiency in cloud computing. Key cryptographic algorithms used for cloud security include:

- Symmetric Key Cryptographic Algorithm:

Provides authentication and authorization to data by encrypting it with a unique key that cannot be decrypted with any other key. Popular symmetric-key algorithms like DES, 3DES, and AES are widely used in cloud computing for cryptography.

- Asymmetric Key Cryptographic Algorithm:

Utilizes two separate keys for encryption and decryption to protect cloud data. Algorithms such as Digital Signature Algorithm (DSA), RSA, and Diffie-Hellman are employed in cloud computing for asymmetric encryption.

- Hashing:

Primarily used for indexing and retrieving items in a database. It employs two separate keys for encrypting and decrypting a message.

In summary, cloud cryptography employs a combination of symmetric and asymmetric encryption methods along with hashing to secure data in the cloud. These methods contribute to maintaining a secure and efficient environment for cloud computing services.

3.3 Advantages of Cloud Cryptography

- Privacy:

Users' data remains private, reducing the risk of cybercrime from hackers.

- Immediate Notifications:

Organizations receive instant notifications when unauthorized modifications are attempted, granting access only to users with cryptographic keys.

- Data Security in Transit:

Encryption safeguards data during transmission between computers.

3.4 Disadvantages of Cloud Cryptography

- Limited Security during Transit:

Cloud cryptography provides limited security to data in transit, necessitating additional security measures.

- Complex Systems Requirement:

Maintaining encrypted data requires highly advanced systems, posing a challenge for some organizations.

- Scalability Challenges:

Systems must be scalable for upgrades, contributing to increased expenses for organizations.

- Potential Recovery Difficulties:

Overprotective measures may create challenges for organizations in the recovery of data, impacting operational efficiency.

4. Image Steganography in Cryptography

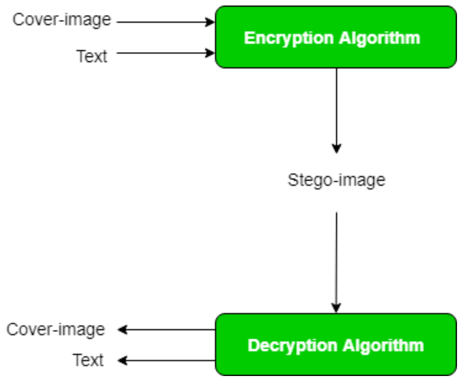
In the realm of covert communication, image steganography serves as a fascinating technique where information is concealed within seemingly innocuous images. Unlike encryption, which transforms data into an unreadable format, steganography hides the very existence of the information.

4.1 what is steganography?

cryptography and steganography are two methods used to protect or hide secret data, but they differ in their versatility. It is writing a secret message, where the message is visible, but its meaning is unclear. On the other hand, including hiding information inside something else, such as hiding a message inside a pair of socks.

4.2 How is it done?

Image steganography involves hiding a message within an image, typically represented as a matrix of pixel intensity values. For grayscale images, this matrix is NM, while for color images, it is NM*3. The process includes using an encryption algorithm to select specific pixels whose values are altered to embed the message. To decode the hidden message, the recipient must be familiar with the same algorithm to identify and extract the modified pixels.



4.3 example of image steganography

Encode message	Decode image
 Input data: CODE “Abdelrahman Ragab”	 output: “Abdelrahman Ragab”

It is noted that no change appears in the image, but the decoded image in the same way, but select specific pixels whose values have been changed to include the message.

In the decoding process of image steganography, the recipient follows a similar procedure to the encoding process. The algorithm used during encoding is employed to identify specific pixels whose values were altered to embed the message. By understanding the encryption algorithm, the recipient can pinpoint and extract the modified pixels, revealing the concealed message within the image. This symmetry in the decoding process ensures that both the sender and the recipient share a common understanding of the encryption method for successful communication through hidden messages.

4.4 Features in Image Steganography

Image steganography in cryptography has features such as confidentiality, capacity, robustness, security, efficiency, concealment and retrieval. It ensures confidential communication by hiding information within the image, making it difficult for unauthorized people to discover it. This technology must be robust against image manipulation, secure from attacks, effective at hiding data, and provide a means of recovery using the decryption key. Advantages include high security, capacity, confidential communications, and resistance to cryptanalysis. However, disadvantages include detectability, complexity, long transmission time, and potential for data loss.

5. DNA Cryptography

DNA cryptography represents a cutting-edge approach to information security, drawing inspiration from the intricate structure of DNA molecules. This novel technique explores the possibilities of using DNA sequences to encode and decode information securely.

5.1 Overview of DNA Cryptography

In DNA cryptography, information is encoded into DNA sequences, leveraging the four nucleotide bases: adenine (A), thymine (T), cytosine (C), and guanine (G). The sequence of these bases forms a unique genetic code that can be harnessed to represent digital information. Decoding the information requires a knowledge of the encoding method and the DNA sequence.

5.2 Potential Applications and Challenges

DNA cryptography holds promise in secure data storage and transmission, particularly in biological and medical contexts. The vast storage capacity of DNA, coupled with its stability, makes it an intriguing candidate for long-term data preservation. Challenges include the cost and complexity of synthesizing and sequencing DNA, as well as the potential for errors in the encoding and decoding process.

6. One Time Password (OTP) Algorithm in Cryptography

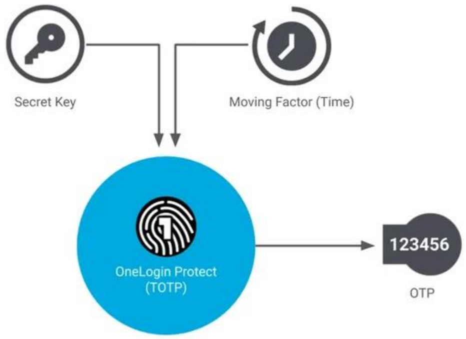
In the realm of authentication, the One Time Password (OTP) algorithm provides an additional layer of security by generating unique passwords for each login session.

6.1 Explanation of OTP as a Secure Authentication Method

The OTP algorithm generates a unique password that is valid for a single login session or transaction. This dynamic password adds an extra layer of security compared to static passwords. Even if a malicious actor intercepts the password, it is useless for subsequent logins.

6.2 How OTP Algorithms Work

OTP algorithms commonly involve the use of time-based or event-based tokens. Time-based tokens generate passwords that are valid for a specific time window, while event-based tokens generate passwords in response to specific events, such as a user request or transaction initiation. The dynamic nature of OTPs enhances security by reducing the risk of password reuse or interception.



6.3 Implementation Examples and Considerations

OTP algorithms are widely used in two-factor authentication (2FA) systems. Common implementations include the use of mobile apps, hardware tokens, or SMS messages to deliver OTPs to users.

However, considerations should be made for the secure distribution of OTPs and potential vulnerabilities, such as the risk of interception during transmission.