Cryptographic Encryption

Reading

35m

Status | Incomplete

Introduction

The term cryptography is derived from the Greek word "Kryptos," which means hidden. It is closely associated with scrambling the text, known as ciphertext and then returning to its original plaintext. Cryptography covers information using techniques such as merging. For example, when transmitting electronic data, the most common use of Cryptography is emailing.

The simplest method uses the symmetric or secret key system. In this case, the data is encrypted using a private key, and the encoded message is sent to the recipient for decryption.

> Reflection Question: What problem can you think of when using symmetric encryption?

If the message is intercepted, a third party has everything it needs to decrypt and read. But to solve this problem, professionals developed the asymmetric or "public key" system. In this case, each user has two public and private keys. Senders request the intended recipient's public key, encrypt the message, and send it

Why do we need Cryptography?

The great need for using cryptography is to protect the user's identity and data. If there is any intrusion attempt, the cryptography system protects all important information: the user's data and the content of files.

Taking into account the recent cases of data leakage that caused real scandals on the internet, users are also exposed in the domestic environment. We are constantly looking for or sharing information online, so our data is stored somewhere. In many cases, it is impossible to be sure whether the storage environment is secure. Therefore, it is also essential to protect yourself with Cryptography and increase your security and privacy when using it at home.

Even ordinary users should always encrypt all messages they send, preferably using a form of public-key cryptography. It's also a good idea to encrypt critical or confidential files – anything from sets of family photos to company data like personal records or accounting history.

For that, it is always important to look for a security solution with strong Cryptography algorithms and an easy-to-use interface. This helps ensure regular use of Cryptography functions and prevents data loss even if a mobile device, hard drive or storage medium falls into your hands.

Data Cryptography

When it comes to your data, cryptography gains much more importance, as it guarantees your privacy, protection and security of your intellectual property. In private use, you can increase your protection with cryptography, which adds an extra layer of protection for sensitive information on your PC and devices, as well as data stored on removable media.

1. **Protect your email information**: We currently resolve many issues via email. If it is common in your daily life to send sensitive information, such as your SIN, credit card number or any other type of personal data, using cryptography can represent a good additional layer of security. By using encryption, the data is accessible only to the recipient, who will have access to the key to decode the content.

2. **Protect data stored in the clouds**: Many users store files using online services such as Google Drive, Dropbox and iCloud. However, what few know is that there is also exposure to invaders when using these services. It is common to see cases of leaked files from cloud storage services. To increase your security and ensure the privacy of files stored in this environment, you can resort to services that encrypt data on the cloud.

3. **Protect files from unauthorized access**: In the same way as when your smartphone is lost/stolen, you can remotely erase all your data, it is also essential to have this protection with your computer. You don't need to block access to all your files stored on your PC, but you do need to block access to sensitive data to stay protected. That way, if you ever lose your computer, the most significant loss will be financial, but no one will have access to your data. It is worth remembering that by protecting your data with Cryptography on your computer, you prevent unauthorized people from accessing your content and personal information.

4. **Protect browsing data**: An essential piece of information that few people know is that when using Wi-Fi to connect to the Internet, you are more exposed to interception, which can result in stolen credentials or other sensitive user data. That's why many websites use a protocol called HTTPS (security certificate) to encrypt data sent between websites. While this is not necessarily a guarantee, the risks are reduced as the transmitted information can only be decoded by the website to which it was sent.

Modern cryptographic techniques for today's cybersecurity needs

Cybersecurity and cryptography are separate concepts, but they are connected. Cybersecurity refers to maintaining data security, while Cryptography is a method used to protect sensitive information.

The two concepts are aligned and comply with the intent of data security.

However, cybersecurity and cryptography are terms that cannot be used interchangeably. Cryptography is a subset of cybersecurity and is one of the methods professionals use to keep data safe. On the other hand, they say that the two are separate units, neither containing the other, but they are not equal. However, both are vital to keeping important information private.

Cybersecurity involves risk management, policy, disaster planning and access control, and cryptography relies on confidentiality, authentication and data integrity. They are two separate fields that are equally essential to keep systems secure.

How important is cryptography for cyber security?

The practice of cryptography in security refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations, called algorithms, for transforming messages in ways that are difficult to decipher.

These algorithms are then used for cryptographic key generation, digital signing, and verification to protect data privacy, internet browsing, and confidential communication such as credit card transactions and emails.

Cryptography achieves several goals related to information security, including confidentiality, integrity, and authentication. Your participation in cybersecurity is indispensable and very important.

Cryptography Data protection techniques

Modern cryptographic techniques make a significant contribution to today's fast-paced cybersecurity needs. To that end, the following are the techniques used for cybersecurity. The most successful method of data protection is through encryption.

- **3DES** - Triple Data Encryption Standard is a block cipher and a modern encryption standard and is similar to the previous encryption method of the same type, namely Data Encryption Standard. Although triple-encrypted data is more secure in storage or during the transition, the process is slower than other encryption techniques. Furthermore, as the method uses smaller block lengths in comparison, it is easier for experienced hackers to decrypt valuable data and exploit it. Commercial institutions and financial companies often use this encryption method, as they did in previous iterations. The technique is also commonly used for electronic payments.
- **AES** - Advanced Encryption Standard is one of the most secure encryption methods. The symmetric encryption algorithm uses a block cipher, which fixes data points one at a time with blocks of fixed size. Unlike other forms of encryption, AES does not encrypt data in small batches. Stream ciphers represent an example of an advanced encryption standard. Since AES uses symmetric key cryptography, the key needs to be shared with other parties to access the encrypted data.
- **Two fish** - is based on the previous version of the block cipher called Blowfish, and it is also a symmetric block cipher. The method works best for smaller CPUs as well as low-end hardware. Like the AES system, it integrates encryption rounds to turn plaintext into ciphertext. This cryptographic technique is more flexible due to the option to select the key configuration and the rate of the encryption process. You can set the key format to run quickly and the encryption process to run slower, and vice versa. Twofish encryption can also be used as often as desired as it does not require a license and has no restrictions.
- **RSA** - Named after the three researchers who first described it (Ron Rivest, Adi Shamir, and Len Adelman), the RSA algorithm uses public-key cryptography to transmit data over an insecure network. It's an asymmetric encryption algorithm, and the first key must always be kept private. When using this form of encryption, you need both keys to gain access to the encrypted data. One of the keys can be used to encrypt the data; the other is used to decrypt it.

  RSA is comparatively secure, as it factors integers derived from a pair of large primes. The key size is larger, which increases the algorithm's security. Most RSA keys are in the 1024-2048 bit range. Despite the larger key size, the encryption method is not slower than other techniques.

Conclusion

Many cryptographic methods are used for a wide range of information security applications, and using the most tried and trusted techniques and algorithms is best for consistent and ongoing data security.

✓ Mark Completed

Previous
Code a Python Playfair Cipher

Next
Cryptographic Methods with GPG

Outline & Notes (1)

Lectures (1)

Work (10)

7 hrs

- Cryptanalysis
- The Use of the Historical vs. Modern Encryption
- Cryptanalysis Quiz
- Cryptography Features and Objectives
- Typical Levels of Cryptography
- The Use of Cryptography
- Code a Python Playfair Cipher
- Cryptographic Encryption
- Cryptographic Methods with GPG

W06D5 Schedule »