Typical Levels of Cryptography

Reading

25m

Status Incomplete

Introduction

Choosing the ideal type of encryption is essential to avoid making mistakes and leaving your data unprotected, which can be accessed by other malicious users. In this unit, you will learn about the main types of cryptography existing at the moment. An essential note to understand the complexity of the encryption that is being talked about, is to consider that the more bits used, the greater the number of keys are needed to decrypt a document. Another ratio involved is that the higher the number, the higher your security.

As you learned before, the symmetric key is the most common and straightforward model. In it, the same key is used by both the sender and the receiver of the message, or it is used both for encoding and decoding data.

Reading

Data Encryption Standard (DES)

This is one of the most basic models, having been one of the first to be created (by IBM in 1977) and implemented. Consequently, it is one of the most widespread worldwide, providing essential protection of only about 56 bits, offering up to 72 quadrillion combinations. This method can be deciphered using a technique called "brute force". In this case, a program automatically tests all possibilities for hours. As it is a fundamental protection system, it offers reduced security for the user.

International Data Encryption Algorithm (IDEA)

Created in 1991, this symmetric key operates on 64-bit blocks of information and uses 128-bit keys. It acts differently, creating confusion to encrypt the text, protecting the data and preventing the realignment for its reading correctly. Its structure is quite similar to that of DES.

Secure and Faster Encryption Routine (SAFER)

In this model, encryption is done in 64-bit blocks. Not infrequently, the user can find it by SAFER SK-64. However, it is cryptography in which many experts have found several weaknesses, leading to the development of new, more complex options, such as SK-40 and SK-128 bits.

Advanced Encryption Standard (AES)

It is one of the most secure encryption algorithms today, used by the United States Government and several security organizations. Its encryption is done in 128-bit blocks, but the keys can also be applied in 192 and 256 bits, making this key extremely difficult to break in conventional cybercriminal attacks.

As you learned before, an asymmetric key, also known as a "public key", works in private and public modes. In the first, the key is secret. In the public model, the user must create an encryption key and forward it to the receiver so that he can access the content.

In asymmetric cryptography, the transmitter and the receiver have different keys, with sizes ranging between 512 and 2048 bits, and it is used in Block mode (which you will study later).

DSA

The algorithm is a standard for digital signatures. It was introduced in 1991 by the NIST as the best method of creating digital signatures. Along with RSA, DSA is considered one of the most widely used digital signature algorithms today.

RSA

The RSA algorithm was described in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. It is one of the first asymmetric encryption algorithms that work with two distinct keys. It is also one of the most used and secure encryption systems worldwide. The RSA model uses prime numbers as a base of calculation; meaning the higher the number, the more secure the key is.

Diffie-Hellman

Diffie-Hellman key exchange is a cryptographic method for securely exchanging keys over a public channel. Whitfield Diffie and Martin Hellman developed it. It was one of the first practical examples of key exchange methods implemented within the field of cryptography, having been published in 1976. Traditionally, secure encrypted communication between two parties required them to exchange keys in advance by some secure physical medium, such as a paper list of keys carried by a trusted messenger. The Diffie-Hellman key exchange method allows two parties to share a secret key over an insecure communication channel without prior knowledge. Such a key can encrypt further messages using a symmetric key cipher scheme.

Conclusion

Now that you have learnt about important encryption algorithms, let's learn how to use cryptography in the next activity.

W06D5

Fri Aug 2

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
- Code a Python Playfair Cipher
- Cryptographic Encryption
- Cryptographic Methods with GPG

W06D5 Schedule »