Cryptography Recap

Reading

40m

Status Incomplete

Introduction

This reading will recap some of the foundational concepts in cryptography. Additionaly, this reading is designed to serve as a resource for you as you move through the rest of the course, providing you with a review of the most critical concepts and techniques in cryptography. By reviewing the various cryptographic algorithms and their applications, you will have a solid foundation for understanding the more advanced cryptographic methods and their practical applications in modern network security.

Ten Most Used Cryptographic Algorithms

It is essential to know what these types are and their main differences to understand how technologies, for example, digital certificates, manage to protect your data. Here is a list of the 10 most used cryptographic algorithms and an explanation of how each works.

1. DES is one of the first encryptions and is considered an essential protection of a few bits. It is the most widespread worldwide and performs 16 encryption cycles to protect information. The complexity and length of encryption keys are measured in bits. When encryption is done with 128 bits, 2128 is the number of possible keys to decrypt it, which is the number of bits currently considered secure.

   DES can be decrypted using the brute force technique (the program tests key possibilities automatically for hours). For this reason, developers need to look for more complex protection alternatives beyond DES.

2. Triple DES (3DES) was initially developed to replace DES, as hackers learned to overcome it relatively quickly. There was a time when 3DES was the recommended standard for security. This encryption gets its name because it works with three keys of 56 bits each, which generates a key with a total of 168 bits. Experts argue that a 112-bit key is sufficient to protect data.

3. DESX is another DES variant and a straightforward algorithm solution. Still, it exponentially increases resistance against brute force attacks without increasing its computational complexity, and 64 bits are added before encryption, which increases the brute force protection of 120 bits. This technology is no longer immune to more sophisticated attacks, such as cryptanalysis, as the program evolves with each decryption attempt.

4. AES is the standard algorithm of the United States government and several other organizations. It is reliable and exceptionally efficient in its 128-bit form, but you can also use 192-bit and 256-bit keys for information that needs more protection. The AES is widely considered immune to all attacks except brute force attacks, which attempt to crack code in all possible combinations of 128, 192, and 256 bits, which is immensely difficult today.

5. Camellia, developed in 2000, is a cryptographic method that decrypts blocks of information. It is a technology with security levels similar to AES since it can be processed in 128, 192, and 256 bits. The Camellia can be implemented both in software (programs) and hardware (physical computer parts). It is also compatible with less expensive 8-bit technologies (smartcards, real-time OSs, etc.) to more powerful 32-bit processors (desktop computers).

6. RSA pioneered public key cryptography. Its name is composed of the surnames of its creators, who are also founders of RSA Data Security. It is considered one of the safest algorithms on the market. For this reason, it was also the first to enable encryption in the digital signature.

   RSA works as follows: it creates two public and private keys (which must be kept confidential). All messages can be encrypted by the public but only decrypted by the private one. Currently, this technology is used in routine operations, such as sending emails, online shopping, and digital signature, among other activities.

7. Blowfish is another algorithm developed to replace DES. It is a symmetric cipher that divides information into 64-bit blocks and encrypts each individually. Blowfish is known for its encryption speed and overall effectiveness. This is a very secure technology, as there are experts on the subject who claim that the code cannot be broken.

8. Twofish is a Blowfish variation and consists of symmetric block encryption. The difference is that it is made up of blocks of 128 bits and keys of up to 256 bits. The technology is considered one of the fastest of its kind and is ideal for providing software and hardware security. Its source code is also free and can be manipulated and used by any programmer.

   There is another variation of the same cryptography called Threefish, and the difference is that the block sizes are 256, 512 and 1024 bits, with keys of the same size.

9. SAFER consists of 64-bit block encryption, which is why it is known as SAFER SK-64. However, weaknesses were found in this code, which resulted in the development of new versions with different key sizes, such as SK-40, SK-64, and SK-128 bits.

10. IDEA is a symmetric key developed in 1991 that operates on 64-bit blocks of information and uses 128-bit keys. The algorithm acts differently, using confusion and diffusion to encrypt the text. It uses three algebraic groups with mixed operations, which is how IDEA protects information.

Notable Cryptography

1. Quantum cryptography uses some fundamental characteristics of quantum physics, which ensure the secrecy of information and solves the issue of Quantum Key Distribution.

2. Homomorphic cryptography refers to a class of cryptography methods devised by Rivest, Adleman, and Dertouzos as early as 1978 and first constructed by Craig Gentry in 2009. Homomorphic cryptography differs from typical cryptography methods in that it allows computation directly into encrypted data without requiring access to a secret key. The result of such a calculation remains encrypted and can later be revealed by the owner of the private key.

Cryptography Components

First, you need to understand that the encryption system's effectiveness and secrecy are vital factors for the security of encrypted data. The main components involved in this encryption are:

- Algorithm
- Key secrecy
- Key length
- Initialization vectors

Goals of Data Encryption

Looking at the side of those who need cryptography, data encryption has four main objectives:

1. **Confidentiality:** this guarantees that only authorized people will have access to the information that needs to be protected.
2. **Authenticity:** ensures that the content of the information is genuine and legitimate.
3. **Integrity:** it guarantees that the data is complete and the message was not lost in parts or entirely.

4. **Non-repudiation:** the assurance that the person who originated the message is who he claims to be. An example would be an email sent with a digital certificate. This certificate guarantees that the person who sent the message is named as the sender and not a third party using his identity.

Types of Encryptors

Now that you know what the components of data encryption are and what the objectives of this protection are, you can learn about the types of data encryption.

- **Replacement:** replaces bits, characters, or blocks of characters with others different from the same alphabet.
- **Transposition:** the characters are not replaced but scrambled.
- **Running key cipher:** this method does not use electronic means to generate the key. It just defines actions that the recipient of the message must perform.

- **Steganography:** this is the encryption method in which we hide information of one format inside another of a different format. For example, we could add text inside a scanned image, a watermark on a digital photo to prevent copying, etc. This trick does not require algorithms or protocols, but some software today encrypts the information before it is hidden.

The Most Crucial Part is the Key

The key used to encrypt the data is the data encryption key. The security of your encryption entirely depends on how your key is stored.

Symmetric keys characterize cryptography, where both sides (sender/recipient) use the same key to encrypt and decrypt data. Keys are also called secret keys; each pair of individuals needs to have a key to read and process the data. The total number of keys involved in a communication must be obtained as follows:

N(N-1)/2 (N is the number of people)

Example: For 15 people, you would have = 15(15-1)/2 = 105 keys

Some advantages of symmetric keys: they perform better than asymmetric encryption. It is also harder to break if you use big keys.

Some disadvantages of symmetric keys: they require a security system for sending keys; each pair of users needs a unique pair. It is a type of encryption that provides confidentiality but does not guarantee authenticity and non-repudiation.

Further Reading

To learn more about cryptography with a more in-depth reading, review the following article: [Cryptography by NIST](#).

Review Questions

Answer all of the questions below to review your understanding. Try to answer them in your own words.

? Considering the cryptographic algorithms discussed, which would you recommend for a company that needs to secure highly sensitive data and why?

Your Answer

Type in your answer here and Compass will let you reveal our answer below. Compass will auto-save your answer as you type. Once you click Toggle Answer below, your answer cannot be changed.

Toggle Answer

? How does the use of RSA in digital signatures contribute to the goals of data encryption, specifically authenticity and non-repudiation?

Your Answer

Type in your answer here and Compass will let you reveal our answer below. Compass will auto-save your answer as you type. Once you click Toggle Answer below, your answer cannot be changed.

Toggle Answer

? What are the potential risks associated with the use of symmetric keys in data encryption, and how can these risks be mitigated?

Your Answer

Type in your answer here and Compass will let you reveal our answer below. Compass will auto-save your answer as you type. Once you click Toggle Answer below, your answer cannot be changed.

Toggle Answer

✓ Mark Completed

← Previous
Case Studies: Encyption & Data Breach

Next
Cryptographics Algorithms →

How well did this activity help you to understand the content?

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

W07D2

Tue Aug 6

› Outline & Notes (1)

› Lectures (1)

Work (6)

5 hrs

- Case Studies: Encyption & Data Breach
- Cryptography Recap
- Cryptographics Algorithms
- Common Encryption Methods Quiz
- Differences Between SSL and TLS
- Unpacking Linux Commands Using AI Tools

W07D2 Schedule »