Onderzoek cryptographic failures

Mike van den Hoef

Fontys ICT

Inhoud

[What is a cryptographical algorithm? 2](#_Toc137628387)

[What are the essential features of cryptographic algorithms? 2](#_Toc137628388)

[What are the different types of cryptographic algorithms? 2](#_Toc137628389)

[How do symmetric and asymmetric cryptographic algorithms differ? 2](#_Toc137628390)

[Which are the most commonly used cryptographic algorithms? 3](#_Toc137628391)

[What are the strengths and weaknesses of each cryptographic algorithm? 3](#_Toc137628392)

[Which cryptographic algorithm provides the best security for specific applications? 3](#_Toc137628393)

[How does the key length affect the security of cryptographic algorithms? 3](#_Toc137628394)

[What are the potential threats and vulnerabilities of cryptographic algorithms? 4](#_Toc137628395)

[Which cryptographic algorithm would I use in my projects? 4](#_Toc137628396)

[Sources 5](#_Toc137628397)

Which type of cryptographic algorithm in software systems is most secure?

Cryptographic algorithms play a crucial role in securing data in various applications. With the increasing number of cyber-attacks, it is essential to determine which cryptographic algorithm is the most secure. In this research, I will compare and analyse some of the most commonly used cryptographic algorithms in terms of their security features. And figure out which one I would use for my personal projects.

# What is a cryptographical algorithm?

For data encryption, authentication, and digital signatures, a cryptographic algorithm is the mathematical formula that is used to scramble plain text and render it unintelligible (What Is Cryptography or a Cryptographic Algorithm? | DigiCert FAQ, n.d.).

# What are the essential features of cryptographic algorithms?

The essential security features of cryptographic algorithms include confidentiality, integrity, authenticity, and non-repudiation. Confidentiality refers to the ability to keep data secure and prevent unauthorized access. Integrity ensures that the data has not been tampered with or altered during transmission. Authenticity ensures that the data is from a trusted source and has not been modified by a third party. Non-repudiation ensures that the sender cannot deny sending the data.

# What are the different types of cryptographic algorithms?

There are two main types of cryptographic algorithms: symmetric and asymmetric. Symmetric algorithms use the same secret key for encryption and decryption. Asymmetric algorithms use a public key for encryption and a private key for decryption. There are also different types of algorithms within these two categories, such as block ciphers, stream ciphers, and hash functions.

# How do symmetric and asymmetric cryptographic algorithms differ?

Symmetric and asymmetric cryptographic algorithms differ in their key management and security levels. Symmetric algorithms are faster and more efficient for encrypting large amounts of data, but they are less secure because the same key is used for encryption and decryption. Asymmetric algorithms are slower but more secure because they use different keys for encryption and decryption.

# Which are the most commonly used cryptographic algorithms?

Some of the most commonly used cryptographic algorithms include AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), and SHA (Secure Hash Algorithm). AES is a symmetric algorithm used for encrypting data in various applications. RSA is an asymmetric algorithm used for secure data transmission and digital signatures. SHA is a hash function used for data integrity and authentication.

# What are the strengths and weaknesses of each cryptographic algorithm?

Each cryptographic algorithm has its strengths and weaknesses. For example, AES is fast, efficient, and widely used, but it is vulnerable to side-channel attacks. RSA is secure and widely used, but it is slower and requires more processing power. SHA is fast and efficient, but it is susceptible to collision attacks. And SHA is also very easy to use and commonly used in projects.

# Which cryptographic algorithm provides the best security for specific applications?

The best cryptographic algorithm for specific applications depends on the security requirements, performance, and key management. For example, AES is suitable for encrypting large amounts of data, while RSA is suitable for secure data transmission and digital signatures. SHA is suitable for data integrity and authentication.

# How does the key length affect the security of cryptographic algorithms?

Stubbs, R. (n.d.). *Classification of Cryptographic Keys*. https://www.cryptomathic.com/news-events/blog/classification-of-cryptographic-keys-functions-and-properties

The key length affects the security of cryptographic algorithms because longer keys provide more security against brute force attacks. For example, a 128-bit key provides more security than a 64-bit key. However, longer keys also require more processing power and can affect the performance of the algorithm.

# What are the potential threats and vulnerabilities of cryptographic algorithms?

The potential threats and vulnerabilities of cryptographic algorithms include brute force attacks, side-channel attacks, key management, and implementation flaws. Brute force attacks involve trying all possible keys to decrypt encrypted data. Side-channel attacks involve exploiting weaknesses in the implementation of the algorithm. Key management involves keeping the keys secure and preventing unauthorized access. Implementation flaws involve errors in the design or implementation of the algorithm.

# Which cryptographic algorithm would I use in my projects?

Because SHA is basically everywhere and most easy to start with, I use SHA algorithms in my projects.

It is fast and efficient, and relatively safe to use. And for a simple project such as our school projects these are all the requirements our cryptographic algorithms need.

# ****Sources****

Stubbs, R. (n.d.). *Classification of Cryptographic Keys*. https://www.cryptomathic.com/news-events/blog/classification-of-cryptographic-keys-functions-and-properties

(What Is Cryptography or a Cryptographic Algorithm? | DigiCert FAQ, n.d.).