The Minimum Security Strength of Cryptography

Reading

30m

Status | Incomplete

Introduction

In cryptography, you secure a message by encrypting it with a specific key and then sending it over the network. The security of the encryption usually depends on the key length. In this article, you'll see why key length is a critical topic in cryptography.

Key length or key size is the number of bits of a key used to encrypt a message. The length is not a measure of how secure the ciphertext is. However, for secure ciphers, the longer the key, the stronger the encryption.

Why Does the Key Size Matter in Cryptography?

The security of a cipher does not depend on the attacker not knowing the algorithm that was used for encryption. The security depends on how hard it is, mathematically, to break the code.

There are two main types of attacks on a cipher: brute force and cryptanalysis.

In a brute force attack, the attacker will generate all possible keys and try each until one is successful. Therefore, the more possible keys, the better.

As you learned before, the Caesar cipher is a substitution/shift cipher that substitutes each letter in the plain message for the letter that is n positions after. Because the alphabet has 26 letters, there are only 26 possible keys to use with this cipher. So, it is elementary to try all the keys and break the code if you know how to read the encrypted text.

Other ciphers use a key of a specific length, measured in bits. A bit is a basic computer unit with only two values, 1 or 0. So, how many keys can we have if we use 128 bits, and each bit can have two values? This is a classic counting problem because this is quite a long number.

Because it is computationally infeasible to calculate the previous number of keys in our current computers, a brute force attack that must try all the possible keys is not practical.

Level of Security in Cryptographic Algorithms

The level of security of a cipher is considered a measure of the strength of a specific algorithm and is measured in bits. An algorithm that is 64-bit secure means that an attacker will have to perform 2^64 (**18,446,744,073,709,551,616**) operations to break the encryption, and algorithms are considered safe if they are at least 112-bit secure. So, the most used "normal" cryptographic function is the 128- and 256-bit.

128-bit AES Encryption:

- Highly robust.
- Nearly impossible to crack.
- Still the strong default choice for all traditional commercial applications.
- Accepted as providing a very high level of security.

256-bit AES Encryption:

- Current gold standard for future proofing against new technology.
- Even harder to compromise than 128-bit.
- Takes more processing power to encrypt and decrypt data, which can lower performance.
- No reason to deploy it unless it is genuinely needed in the military/government.

256-bit encryption is sufficient to protect against sustained attacks from sophisticated criminals or the resources associated with rogue state entities. Given the quality of this level of encryption, it is often mandated by standard bodies related to the financial, medical, and security industries.

The key sizes approved for the use of AES are 128, 192, and 256. Recommended key size for the most used cryptographic algorithms in some instances, it is recommended to use AES with a key size equal to or greater than 192.

Keys in Asymmetric Cryptography

Asymmetric cryptography's key strength is based on the complexity of integer factorization. This problem is hard to solve and needs a lot of time, but it takes less than a brute force attack. For this reason, asymmetric cryptographic algorithms need a longer key size to have a similar level of security than symmetric cryptographic algorithms.

Recommended Algorithms and Key Lengths

Below you will find a table with the recommended key size for different algorithms.

Algorithm	**Recommended Key Size**
AES	128
RSA	2048, 3072, 7680
Elliptic Curve	256, 384
DSA	2048, 3072, 6770
Diffie-Hellman	2048, 3072, 6770

The length of a public key depends on the algorithm used. Below is a table with possible key sizes for public keys.

Algorithm	**Key Size**
RSA	1024, 2048, 4096
Elliptic Curve	256, 384, 512
Diffie-Hellman	2048
Elgamal	1024

Conclusion

Every day, with the evolution of technology, computers get more processing power. Also, new mathematics methods and tools are discovered. Both of them influence how long a cryptographic protocol recommendation can be valid.

Usually, theories are discovered and published on how to break certain ciphers. Even though they might not be practical because of the lack of computational power needed, they shed light on possible vulnerabilities. Then, improvements are made to the algorithms so they don't become insecure.

References

- Just Cryptography - What is key length in cryptography and why is it important?
- Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
- Discussion Paper: The Transitioning of Cryptographic Algorithms and Key Sizes

Review Questions

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

Considering the computational limits of current technology, why is it generally impractical to use a brute force attack to break a 256-bit AES encryption?

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 key size in asymmetric cryptography compare to symmetric cryptography in terms of required length for similar levels of security, 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

Why might an organization choose to implement 256-bit AES encryption despite its higher computational demands compared to 128-bit AES encryption?

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
Cryptographic Methods

Next
Decrypting and Sending a File

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

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

W07D1

Mon Aug 5

- Lectures (1)
- Work (4)

  3 hrs

  - The Minimum Security Strength of Cryptography
  - Decrypting and Sending a File
  - Symmetric, Asymmetric Key and Hash Quiz
  - Using TLS and SSL

W07D1 Schedule »