



26+ Years
of Experience

**PROGRAMMING
ADVICES** LEARN THE
RIGHT WAY

Mohammed Abu-Hadhoud

MSA, PMOC, PMP®, PRP®, PSE-ITP®, CS, ITIL, MCP®, MCSD



لا تنسى الاشتراك في قناتنا على اليوتيوب ومشاركة القناة مع اصدقائك
لتعم الفائدة للجميع وانقاذ الاف الناس من التشتت جزاكم الله خيرا

لا تنسونا من دعائكم وادعو لوالدي بالرحمة

www.ProgrammingAdvices.com



مهم جداً

هذا الملف للمراجعة السريعة واخذ الملاحظات عليه فقط ،لانه يحتوي على اقل من 20% مما يتم شرحه في الفيديوهات الاستعجال والاعتماد عليه فقط سوف يجعلك تخسر كميه معلومات وخبرات كثيره

يجب عليك مشاهدة فيديو الدرس كاملا

لاتنسى عمل لايك ومشاركة القناة لتعم الفائدة للجميع
لا تنسونا من دعائكم

ProgrammingAdvices.com

Mohammed Abu-Hadhoud



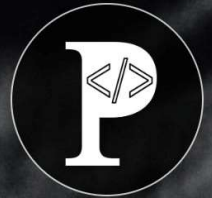


Programming - Level 2

Symmetric Encryption

Mohammed Abu-Hadhoud

MBA, PMOC, PgMP®, PMP®, PMI-RMP®, CM, ITILF, MCPD, MCSD



ProgrammingAdvises.com



**PROGRAMMING
ADVISES** LEARN THE
RIGHT WAY

What is Symmetric Encryption?

- Symmetric encryption is a type of encryption where the same key is used for both the encryption and decryption of the data.
- In C#, the .NET Framework and .NET Core provide classes in the System.Security.Cryptography namespace to perform symmetric encryption.
- The most commonly used symmetric encryption algorithms are DES (Data Encryption Standard), 3DES (Triple DES), AES (Advanced Encryption Standard), and RC4.

128-bit Key, What does that mean?

- The key size is commonly used for AES encryption is 128-bit, what does that mean?
- The "key size" in the context of AES (Advanced Encryption Standard) refers to the length of the cryptographic key used for encryption and decryption. In AES, the key size determines the number of bits in the key, and it directly affects the strength of the encryption.

128-bit How many characters?

- 16 characters, why?
- Each character represents one byte (8 bits), so
 $16 \text{ characters} * 8 \text{ bits/character} = 128 \text{ bits}$

AES supports three key sizes.

- 128-bit, 192-bit, and 256-bit.
- The number in each key size (128, 192, or 256) represents the length of the key in bits. Here's a breakdown of what each of these key sizes means:
- 128-bit Key:
 - The key is 128 bits long, which means it has 2^{128} possible combinations.
 - This is considered strong encryption and is widely used for many secure applications.
- 192-bit Key:
 - The key is 192 bits long, providing a higher level of security than 128-bit keys.
 - While it offers increased security, 192-bit keys are less commonly used than 128-bit and 256-bit keys.
- 256-bit Key:
 - The key is 256 bits long, providing the highest level of security among the three key sizes.
 - AES with a 256-bit key is often used in situations where maximum security is required.

The highest key size the harder to attack.

- The key size directly impacts the difficulty of a brute-force attack, where an attacker tries all possible combinations of the key to decrypt the data. As the key size increases, the number of possible combinations grows exponentially, making it significantly more difficult and time-consuming for an attacker to break the encryption through brute force.

Should we always use the highest key size?

- No.
- In practice, a 128-bit key is considered secure for most applications, and it is widely used in various cryptographic protocols and systems.
- However, for scenarios where an extra layer of security is desired or required, one might opt for a 192-bit or 256-bit key.
- It's important to note that the increased security comes with a trade-off in terms of computational overhead, as encryption and decryption with longer keys can be more computationally intensive.



programmingAdvices.com
Thank You

Mohammed Abu-Hadhoud

26+ Years of Experience

MBA, PMOC, PgMP®, PMP®, PMI-RMP®, CM, ITILF, MCPD, MCSd

