PROGRAMMING ADVICES
LEARN THE RIGHT WAY

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

26+ Years of Experience

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

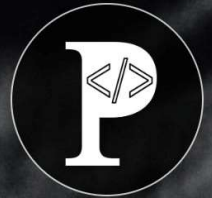## ProgrammingAdvices.com

Mohammed Abu-Hadhoud

What is Asymmetric Encryption?

- Asymmetric encryption, also known as <u>public-key cryptography</u>, is a cryptographic system that uses pairs of keys:
  - Public keys, which are widely shared or distributed.
  - Private keys, which are kept secret.

- This system enables two parties to secure their communication over an insecure channel without having to share a secret key beforehand.

A brief overview of how asymmetric encryption works:

- Key Pairs:
  - Public Key: This key is made available to anyone and can be freely distributed. It's commonly used for encryption.
  - Private Key: This key is kept secret and is known only to the owner. It's used for decryption.

- Encryption and Decryption:
  - If Party A wants to send an encrypted message to Party B, Party A uses Party B's public key to encrypt the message.
  - Only Party B, who possesses the corresponding private key, can decrypt and read the message.

Mohammed Abu-Hadhoud
MBA, PMOC, PgMP®, PMP®, PMI-RMP®, CM, ITILF, MCPD, MCSD
26+ years of experience

A brief overview of how asymmetric encryption works:

- Digital Signatures:
  - The roles can be reversed for digital signatures. If Party A wants to sign a message and prove its authenticity, Party A uses its private key to create a digital signature.
  - Anyone with access to Party A's public key can verify that the signature is valid, confirming that the message has not been tampered with and is indeed from Party A.

Mohammed Abu-Hadhoud
MBA, PMOC, PgMP®, PMP®, PMI-RMP®, CM, ITILF, MCPD, MCSD
26+ years of experience

A brief overview of how asymmetric encryption works:

- Key Distribution:
  - Asymmetric encryption helps solve the key distribution problem inherent in symmetric key cryptography. <u>In a symmetric key system</u>, <u>both parties need to have the same secret key</u>, which can be challenging to distribute securely.
  - With asymmetric encryption, each participant has their own pair of public and private keys.

Algorithms used in asymmetric encryption:

- Popular algorithms used in asymmetric encryption include:
  - RSA (Rivest–Shamir–Adleman)
  - ECC (Elliptic Curve Cryptography)
  - and DSA (Digital Signature Algorithm).

- Asymmetric encryption is often used in combination with symmetric encryption for efficiency and security in various cryptographic protocols and applications, such as secure communication over the internet, digital signatures, and key exchange in secure protocols like SSL/TLS.

Mohammed Abu-Hadhoud
MBA, PMOC, PgMP®, PMP®, PMI-RMP®, CM, ITILF, MCPD, MCSD
26+ years of experience

ProgrammingAdvices.com

Thank You

Mohammmed Abu-Hadhoud
26+ Years of Experience
MBA, PMOC, PgMP®, PMP®, PMI-RMP®, CM, ITILF, MCPD, MCSD

PROGRAMMING
ADVICES   LEARN THE RIGHT WAY