2024-07-08#AES-NI

IT-SEC

AES-NI

- [**A**dvanced **E**ncryption **S**tandard-**N**ew **I**nstructions]
- **Was ist AES-NI:**
  - ist eine Erweiterung des x86-Befehlssatzes von Intel- und AMD-Prozessoren.
  - Symmetrischer Schlüssel
  - sicherste Verschlüsselungsalgorithmus
  -
- **Aufgabe:**
  - Diese Erweiterung beschleunigt
    - die Verschlüsselung und
    - Entschlüsselung des Advanced Encryption Standard (AES).
- **Anwendung**
  - AES-NI wird verwendet, um die AES-Verschlüsselung und -Entschlüsselung in verschiedenen Anwendungen wie z.B. in der Kryptographie, in der Datenverschlüsselung und in der Netzwerk-Sicherheit zu beschleunigen.
- **Wie funktioniert AES-NI?**
  - Wenn ein System mit AES-NI-Unterstützung auf AES-Verschlüsselungs- oder Entschlüsselungsvorgänge stößt, kann die CPU diese Aufgaben an die AES-NI-Engine ausladen. Diese Engine verwendet dedizierte Hardware, um die Verschlüsselung und Entschlüsselung durchzuführen, anstatt sich auf softwarebasierte Implementierungen zu verlassen.

AES-NI Engine

1. **Key expansion**: Erweitert den geheimen Schlüssel in eine Reihe von runden Schlüsseln, die zum Verschlüsseln und Entschlüsseln verwendet werden.
2. **Encryption**: Verschlüsselt die Klartextdaten mit den runden Tasten.
3. **Decryption**: Entschlüsselt die Chiffretextdaten mit den runden Tasten.