15.1 AES encryption practical

Peter Rutschmann

26.11.2025

AES-Verschlüsselung anwenden

In diesem Jupyter Notebook wird die **AES-Verschlüsselung** angewendet:

- 1. AES Online anwenden
- 2. AES mit Python anwenden

AES Online Demo

Es gibt verschiedene Online-Demos, die die AES-Verschlüsselung anschaulich erklären und zeigen. Hier eine davon:

https://demo.kenhaggerty.com/demos/aescipher

Erklärungen zur Demo:

- Der Key muss geheim gehalten werden. Nur Sender um Empfänger dürfen ihn kennen.
- Der Key hat üblicherweise eine Länge von 128, 192 oder 256 Bit
- Der Key muss nicht ein lesbarer Text sein. Oft ist er eine Zufällige HEX-Folge
- BASE64 erlaubt es diese HEX-Folge in lesbare Zeichen zu kodieren, war die Übermittlung zBsp per Email vereinfacht.
- IV = Initialisierungsvektor, verhindert, dass bei gleichem Key und gleichem Plain-Text das Ergebnis gleich bleibt. Der IV darf mit der verschlüsselten Nachricht übermittelt werden.

Aufgabe: AES Online anwenden

- Verwenden Sie die oben angegebene Online-Demo
- Lässen Sie mit Refresh einen Key und IV generieren
- Schreiben Sie einen kurzen Klartext (Plain-Text)
- Codieren Sie den Text
- Halten Sie Key, IV, Plain-Text und Cipher-Text unten im Feld fest.
- Tauschen Sie den Codierten Text, den Schlüssel und den IV mit Ihrem Lernpartner aus
- Decodieren Sie den Codierten Text ihres Lernpartners mit den Angaben Ihres Lernpartners.
- Halten Sie Key, IV, Plain-Text und Cipher-Text unten im Feld fest.

```
\CommentTok{\# Hier ihren Key, IV, Plain{-}Tet und Cipher{-}Text festhalten}


\CommentTok{\# Hier die Angaben Ihres Lernpartners festhalten, inklusive
Ihrer Decodierung}
```

AES mit Python anwenden

Dieses Beispiel verwendet die Bibliothek *pycryptodome*. Wenn Sie das Notebook im VS-Code ausführen: - öffnen Sie ein Terminal (Menü von VSCode: Terminal -> Neues Terminal) - Geben Sie im Terminal folgendes ein und drücken Enter:

```
\ExtensionTok{/bin/python3} \AttributeTok{{-}m}\NormalTok{ pip install
}\AttributeTok{{-}{-}user}\NormalTok{ pycryptodome}
```

Danach müssen Sie einen Restart mit dem Notebook durchführen.

Alternative können Sie das Notebook im Colab ausführen, dort wird die Bibliothek direkt aus dem Notebook installiert: https://colab.research.google.com/

Starten Sie danach den folgenden Code-Block. Welcher Schritt ergibt welchen Output?

```
\OperatorTok{!}\NormalTok{pip install pycryptodome}

\ImportTok{from}\NormalTok{ Crypto.Cipher }\ImportTok{import}\NormalTok{ AES}
\ImportTok{from}\NormalTok{ Crypto.Random }\ImportTok{import}\NormalTok{ get\_random\_bytes}
\ImportTok{import}\NormalTok{ base64}

\CommentTok{\# {-}{-}{-} Hilfsfunktionen für Padding (PKCS\#7) {-}{-}{-}}

\NormalTok{BLOCK\_SIZE }\OperatorTok{=} \DecValTok{16}  \CommentTok{\# AES{-}Blockgröße in Bytes}

\KeywordTok{def}\NormalTok{ pad(data: }\BuiltInTok{bytes}\NormalTok{) }\OperatorTok{{-}\textgreater{}} \BuiltInTok{bytes}\NormalTok{:}
    \CommentTok{"""PKCS\#7 Padding hinzufügen"""}
\NormalTok{    padding\_len }\OperatorTok{=}\NormalTok{ BLOCK\_SIZE }\OperatorTok{{-}}\NormalTok{ (}\BuiltInTok{len}\NormalTok{(data) }\OperatorTok{\%}\NormalTok{ BLOCK\_SIZE)}
    \ControlFlowTok{return}\NormalTok{ data }\OperatorTok{+} \BuiltInTok{bytes}\NormalTok{([padding\_len]) }\OperatorTok{*}\NormalTok{ padding\_len}

\KeywordTok{def}\NormalTok{ unpad(data: }\BuiltInTok{bytes}\NormalTok{) }\OperatorTok{{-}\textgreater{}} \BuiltInTok{bytes}\NormalTok{:}
    \CommentTok{"""PKCS\#7 Padding entfernen"""}
\NormalTok{    padding\_len }\OperatorTok{=}\NormalTok{ data[}\OperatorTok{{-}}\DecValTok{1}\NormalTok{]}
    \ControlFlowTok{return}\NormalTok{ data[:}\OperatorTok{{-}}\NormalTok{padding\_len]}

\CommentTok{\# {-}{-}{-} 1. Key und IV erzeugen {-}{-}{-}}

\NormalTok{key }\OperatorTok{=}\NormalTok{ get\_random\_bytes(}\DecValTok{16}\NormalTok{)  }\CommentTok{\# 16 Bytes = 128 Bit (AES{-}128)}
\NormalTok{iv }\OperatorTok{=}\NormalTok{ get\_random\_bytes(}\DecValTok{16}\NormalTok{)   }\CommentTok{\# 16 Bytes IV für CBC}

\CommentTok{\# {-}{-}{-} 2. Klartext vorbereiten {-}{-}{-}}

\NormalTok{plaintext }\OperatorTok{=} \StringTok{"Wir treffen uns mit Paul am Mittwoch in der Gruft"}
\NormalTok{plaintext\_bytes }\OperatorTok{=}\NormalTok{ plaintext.encode(}\StringTok{"utf{-}8"}\NormalTok{)}

\CommentTok{\# {-}{-}{-} 3. Verschlüsseln (Encrypt) {-}{-}{-}}

\NormalTok{cipher\_encrypt }\OperatorTok{=}\NormalTok{ AES.new(key, AES.MODE\_CBC, iv)}
```

```
\NormalTok{ciphertext\_bytes }\OperatorTok{=}\NormalTok{
cipher\_encrypt.encrypt(pad(plaintext\_bytes))}

\CommentTok{\# {-}{-}{-} 4. Für Transport/Anzeige in Base64 kodieren
{-}{-}{-}}

\NormalTok{key\_b64 }\OperatorTok{=}\NormalTok{
base64.b64encode(key).decode(}\StringTok{"utf{-}8"}\NormalTok{)}
\NormalTok{iv\_b64 }\OperatorTok{=}\NormalTok{
base64.b64encode(iv).decode(}\StringTok{"utf{-}8"}\NormalTok{)}
\NormalTok{ciphertext\_b64 }\OperatorTok{=}\NormalTok{ base64.b64encode(cip
hertext\_bytes).decode(}\StringTok{"utf{-}8"}\NormalTok{)}

\BuiltInTok{print}\NormalTok{(}\StringTok{"AES Key (Base64):
"}\NormalTok{, key\_b64)}
\BuiltInTok{print}\NormalTok{(}\StringTok{"AES IV  (Base64):
"}\NormalTok{, iv\_b64)}
\BuiltInTok{print}\NormalTok{(}\StringTok{"Ciphertext (Base64):
"}\NormalTok{, ciphertext\_b64)}

\CommentTok{\# {-}{-}{-} 5. Entschlüsseln (Decrypt) {-}{-}{-}}

\CommentTok{\# In der Praxis käme Key/IV z.B. aus Base64{-}Strings:}
\NormalTok{key\_decoded }\OperatorTok{=}\NormalTok{
base64.b64decode(key\_b64)}
\NormalTok{iv\_decoded }\OperatorTok{=}\NormalTok{
base64.b64decode(iv\_b64)}
\NormalTok{ciphertext\_decoded }\OperatorTok{=}\NormalTok{
base64.b64decode(ciphertext\_b64)}

\NormalTok{cipher\_decrypt }\OperatorTok{=}\NormalTok{
AES.new(key\_decoded, AES.MODE\_CBC, iv\_decoded)}
\NormalTok{decrypted\_padded }\OperatorTok{=}\NormalTok{
cipher\_decrypt.decrypt(ciphertext\_decoded)}
\NormalTok{decrypted }\OperatorTok{=}\NormalTok{
unpad(decrypted\_padded).decode(}\StringTok{"utf{-}8"}\NormalTok{)}

\BuiltInTok{print}\NormalTok{(}\StringTok{"Entschlüsselter Text:
"}\NormalTok{, decrypted)}
```

```
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: pycryptodome in
/home/vscode/.local/lib/python3.10/site-packages (3.23.0)
AES Key (Base64):      xSWzpVy2pA/QauBbMmh71g==
AES IV  (Base64):      9yZ90TPiJaYmY1wZnkHNIw==
Ciphertext (Base64):   D/SaYU3roeqXFsB8F2XPIs5iEFeX9mzcEcTFvq/vleHue7Cxv1kH
mq0Ch+XyT1M7ImUdWU2B1+iGg6YRBQyGJw==
Entschlüsselter Text:  Wir treffen uns mit Paul am Mittwoch in der Gruft
```

Aufgabe : AES mit Python anwenden

Kopieren Sie den obigen Code. Kodieren Sie einen kurzen Text. Tauschen Sie den codierten Text, den Schlüssel und den IV mit Ihrem Lernpartner aus. Decodieren Sie den codierten Text ihres Lernpartners mit den Angaben Ihres Lernpartners.

```
1 \CommentTok{\# Mein eigenes Beispiel}
```