

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 und 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, was 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
- Lassen 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 Codierte Text, den Schlüssel und den IV mit Ihrem Lernpartner aus
- Decodieren Sie den Codierte Text ihres Lernpartners mit den Angaben Ihres Lernpartners.
- Halten Sie Key, IV, Plain-Text und Cipher-Text unten im Feld fest.

```
1 # Hier ihren Key, IV, Plain-Text und Cipher-Text festhalten
2
3
4 # Hier die Angaben Ihres Lernpartners festhalten, inklusive
   ↪ Ihrer Decodierung
```

AES mit Python anwenden

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

```
1 /bin/python3 -m pip install --user 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?

```

1  !pip install pycryptodome
2
3  from Crypto.Cipher import AES
4  from Crypto.Random import get_random_bytes
5  import base64
6
7  # --- Hilfsfunktionen für Padding (PKCS#7) ---
8
9  BLOCK_SIZE = 16 # AES-Blockgröße in Bytes
10
11 def pad(data: bytes) -> bytes:
12     """PKCS#7 Padding hinzufügen"""
13     padding_len = BLOCK_SIZE - (len(data) % BLOCK_SIZE)
14     return data + bytes([padding_len]) * padding_len
15
16 def unpad(data: bytes) -> bytes:
17     """PKCS#7 Padding entfernen"""
18     padding_len = data[-1]
19     return data[:-padding_len]
20
21 # --- 1. Key und IV erzeugen ---
22
23 key = get_random_bytes(16) # 16 Bytes = 128 Bit (AES-128)
24 iv = get_random_bytes(16) # 16 Bytes IV für CBC
25
26 # --- 2. Klartext vorbereiten ---
27
28 plaintext = "Wir treffen uns mit Paul am Mittwoch in der
29 ↪ Gruft"
30 plaintext_bytes = plaintext.encode("utf-8")
31
32 # --- 3. Verschlüsseln (Encrypt) ---
33
34 cipher_encrypt = AES.new(key, AES.MODE_CBC, iv)
35 ciphertext_bytes =
36 ↪ cipher_encrypt.encrypt(pad(plaintext_bytes))
37
38 # --- 4. Für Transport/Anzeige in Base64 kodieren ---
39
40 key_b64 = base64.b64encode(key).decode("utf-8")
41 iv_b64 = base64.b64encode(iv).decode("utf-8")
42 ciphertext_b64 =
43 ↪ base64.b64encode(ciphertext_bytes).decode("utf-8")
44
45 print("AES Key (Base64):      ", key_b64)
46 print("AES IV (Base64):      ", iv_b64)

```

```

44 print("Ciphertext (Base64): ", ciphertext_b64)
45
46 # --- 5. Entschlüsseln (Decrypt) ---
47
48 # In der Praxis käme Key/IV z.B. aus Base64-Strings:
49 key_decoded = base64.b64decode(key_b64)
50 iv_decoded = base64.b64decode(iv_b64)
51 ciphertext_decoded = base64.b64decode(ciphertext_b64)
52
53 cipher_decrypt = AES.new(key_decoded, AES.MODE_CBC,
54     ↪ iv_decoded)
54 decrypted_padded = cipher_decrypt.decrypt(ciphertext_decoded)
55 decrypted = unpad(decrypted_padded).decode("utf-8")
56
57 print("Entschlüsselter Text: ", decrypted)

```

```

Defaulting to user installation because normal site-packages is not write
Requirement already satisfied: pycryptodome in /home/vscode/.local/lib/pyt
packages (3.23.0)
AES Key (Base64):      xSWzpVy2pA/QauBbMmh71g==
AES IV (Base64):      9yZ90TPiJaYmY1wZnkHNIw==
Ciphertext (Base64):  D/SaYU3roeqXFsb8F2XPIs5iEFex9mzcEcTFvq/vleHue7C xv1
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 # Mein eigenes Beispiel

```