15 AES encryption

Peter Rutschmann

26.11.2025

AES Verschlüsselung

Verfahren der digitalen Verschlüsselung

Die Techniken der digitalen Verschlüsselung lassen sich unter *Transformation* als Oberbegriff zusammenfassen.

Eine Transformation kann aus diesens Schritten bestehen:

- **Substitution** : Ersetzen von Symbolen durch andere Symbole
- **Transposition/Permutation** : Vertauschung von Zeichen oder Bits
- **Diffusion** : Streuung der Klartext-Information über viele Bits im Geheimtext
- **Konfusion** : Komplexe, nichtlineare Beziehung zwischen Schlüssel und Geheimtext
- **Rundensystem** : Mehrfache Wiederholung von Substitution und Permutation
- **Key Schedule** : Algorithmus zur Ableitung von Rundenschlüsseln :
- **Blockchiffre |** Verschlüsselt Daten blockweise (z. B. 128 Bit bei AES)
- **Stromchiffre |** Verschlüsselt Bit für Bit oder Byte für Byte

Substitution

- UTF8 wendet Substituation an, es ersetzt anhand der UTF8 Code-Tabled ein Buchstabe durch eine Bitfolge
- **XOR** wendet Substitution an, es ersetzt die Bits auf Grund des Schlüssel durch andere Bits.

Transposition/Permutation

A = 01000001 key = 3

Meine eigene Regel:

- Buchstabencodierung UTF8, nur 7-Bit Buchstaben.
- Rechtes, fehlende Bit mit 1 auffüllen
- Teile die Bitfolge in Gruppen von 3 bit. Ergänze die Folge mit 1, falls es nicht aufgeht.
- Innerhalb jeder 3er-Gruppe vertauschen wir die Positionen nach Muster (1,2,3) -> (3,1,2)

```
010 000 01 A
010 000 011  auffüllen
001 000 101 (1,2,3) -> (3,1,2)

Auflösen:
001 000 101
010 000 011 (1,2,3) -> (3,1,2)
010 000 01  A
```

Aufgabe Anwenden Transponieren

- Wenden Sie die obige Transposition auf einen 4 stellige Dezimale Zahl an.
- Wandeln Sie die Zifferen der Zahl mit UTF8 in eine binäre Zahlenfolge um. (ergibt 4 Bytes) Liste der UTF8 Codierung
- Transponieren Sie mit dem key=3 gemäss obiger Regel
- Tauschen Sie das Ergebnis mit Ihrem Lernpartner aus, findet er die ursprüngliche Zahl heraus?

Lösung

```
Aufgabe Anwenden Transponieren
gezeigt wird nur eine Teillösung

Wie transponieren:
Nr: 1 2 3
Bit 0 1 0
Regel Reihenfolge 1,2,3 wird neu 3,1,2
Nr: 3 1 2
Bit 0 0 1

Meine vierstellige Zahl:
4589
Ziffern 4 5 8 9
und darunter binär nach UTF8

4          5          8         9
00110100'  00110101'  00111000  ...

Bits in 3er Gruppen transponieren:
Der ' hilft zu sehen, wann die nächste Ziffer (
 ↪  4..5..8...9 ) beginnt.
Regel für die Bits: (1,2,3) (3,1,2)
123 123 12 3 123 123 123
001 101 00'0 011 010 1'00 ...
312 312 31 2 312 321 3 21
100 110 00 0 101 001 010

Entschlüsseln
Regel für die Bits: (1,2,3) (3,1,2) ABER: umgekehrt
 ↪  anwenden!!
312 312 312 ...
100 110 000 ...
123 123 123 ...
001 101 000 ...
Bits wieder zu einer 8er Gruppe zusammenfügen:
00110100' 0 ...
Und wieder mit UFT8 umwandeln --> Ziffer 4
```

Aufgabe Anwenden eines mehrfachen Transponieren

- ausprobieren: Permutation-Demo
- analysieren Sie die Schritte

- notieren Sie die Schritte auf.
- Codieren Sie einen von Ihnen gewählten Buchstaben.
  - Buchstabe mit UTF8 Tabelle in Bits umwandeln.
  - In der Permutations-Demo codieren, eigenen Schlüssel und Anzahl Runden wählen.
  - Mit Lernpartner Codierten Code, Schlüssel und Anzahl Runden austauschen.
  - Kann Ihr Lernpartner den richtigen Buchstaben herausfinden?

Anwendung in der Praxis mit Beispiel AES Verschlüsselung

AES Verfahren

AES ist ein modernes Verschlüsselungsverfahren. AES verschlüsselt, indem es den Klartext blockweise (128 Bit) in mehreren Runden mit dem Schlüssel verarbeitet. In jeder Runde passieren vier Schritte:

- Substitution: SubBytes -> jedes Byte wird durch die S-Box ersetzt
- Permutation: ShiftRows -> die Zeilen werden verschoben
- Diffusion: MixColumns -> die Spalten werden gemischt.
- AddRoundKey → der Block wird mit dem Rundenschlüssel per XOR verknüpft.
- Nach 10 (12 / 14) Runden entsteht der Geheimtext.

AES Verfahren Demo

Das sind einige Schritte. Die *AWS web demo* zeigt das anschaulich.

- Link anklicken, Random wählen, die Schritte beobachten.
- Das Resultat auch wieder dekodieren.

Eine AES-Animation, die das Verfahren versucht zu verdeutlichen.

- Probieren Sie es aus.

AES selber anwenden

Laden Sie das Notebook herunter, um AES praktisch anzuwenden. Lesen und lösen Sie:

Notebook zu AES herunterladen