

# Untitled

November 6, 2019

## 1 Frage 1

One-Time-Pad

Sie haben eine mit einem One-Time-Pad verschlüsselte Nachricht. Welche Information kann eine *Angreiferin* aus der Nachricht ableiten, wenn er\*sie diese abfangen kann?

Antwort: Die Länge der originalen Nachricht.

## 2 Frage 2

### 2.1 Visuelle Kryptographie

Sie haben zwei Folien gegeben die Schlüssel eines visuellen Kryptografie Verfahrens darstellen. Geben Sie das Geheimnis an, das verschlüsselt wurde.

```
In [10]: from PIL import Image
         import PIL

In [6]: im1 = Image.open("Key1.png")
         im2 = Image.open("Key2.png")

In [19]: # Antwort: Wissen ist Nacht
         PIL.ImageChops.add(im1,im2)
```

Out [19]:

troupe de danse

### **3 3 Feistel - Eigenschaften**

Welche der folgenden Eigenschaften lässt sich dem Feistel-Verfahren zuordnen?

Antwort: Bijektivität

### **4 4 Visuelle Kryptographie - Theorie**

Auf wie viele Folien kann bei visueller Kryptographie das Geheimnis theoretisch maximal verteilt werden?

Antwort: beliebig viele

Das Verfahren der visuellen Kryptografie bei 2 erzeugten Folien pro Secret hat Ähnlichkeiten zu einem anderen bekannten kryptografischen Verfahren. Welchem?

Antwort: One-Time-Pad

## 5 5 Feistel Beispiel

Sie haben eine Binärzahl gegeben, die mit dem Feistel-Verfahren verschlüsselt wurde. Es wurden 3 Runden durchlaufen, der Schlüssel ist  $k = 3$  und  $F$  ist ein AND. Berechnen Sie den Klartext. Die verschlüsselte Binärzahl lautet: 00001111

```
In [395]: def Feistel(key, L, R, rounds):
          bit_list = [L,R]
          tmp = ['null']
          for runde in range(rounds):
              tmp[0] = bin(int(F(key, bit_list[1]), 2) ^ int(bit_list[0], 2))[2:]
              bit_list[0] = bit_list[1]
              bit_list[1] = tmp[0]
          return list(reversed(bit_list))

          def F(key, half):
              return bin(bin_to_int(half) & key)[2:]

          def bin_to_int(get_bin):
              return int(get_bin,2)

In [399]: print('Result = ' + str(Feistel(3, '0000', '1111', 3)))

Result = ['11', '1100']
```

## 6 6 Triple-DES - Theorie

- 1) Um der Kritik des DES bezüglich seiner zu geringen Schlüssellänge von 56 Bit zu begegnen, wurde Triple-DES (3-DES) vorgeschlagen. Dabei wird mit zwei 56 Bit langen Schlüsseln  $k_1$  und  $k_2$  gearbeitet und beim Verschlüsseln entweder  $\text{encrypt}(k_1) \rightarrow \text{decrypt}(k_2) \rightarrow \text{encrypt}(k_1)$  (EDE-Modus) oder  $\text{encrypt}(k_1) \rightarrow \text{encrypt}(k_2) \rightarrow \text{encrypt}(k_1)$  (EEE-Modus) ausgeführt.

Warum begnügt man sich bei Triple-DES aus Sicherheitsgründen nicht mit zwei Verschlüsselungen? Gehen Sie von einem Known-plaintext-Angriff aus. Geben Sie die Ziffer der Antwort an, die Sie für richtig halten.

1. Der Sicherheitsgewinn wäre nur 1 Bit (durch Anwendung eines Meet-in-the-Middle-Angriffs).
- 2) Welchen Modus benutzt man bevorzugt bei Triple-DES? Geben Sie die Nummer der Antwort an, die Sie für richtig halten.
  1. EDE
- 3) Berechnen Sie die theoretische und die effektive Schlüssellänge des Triple-DES unter einem Known-plaintext-Angriff mit drei 56-Bit-Schlüsseln, d.h.  $\text{encrypt}(k_1) \rightarrow \text{encrypt}(k_2) \rightarrow \text{encrypt}(k_3)$ . Geben Sie das Ergebnis als  $2^x$  an, wobei  $x$  eine natürliche Zahl ist.

Antwort: 2<sup>112</sup> <https://crypto.stackexchange.com/questions/25623/meet-in-the-middle-attack-on-3des>

Symmetrische Konzelationssysteme

Wählen Sie die korrekten Aussagen zu symmetrischen Konzelationssystemen aus. Wählen Sie eine oder mehrere Antworten:

Antworten: 1. Der Verschlüsselungsalgorithmus enc bzw. Entschlüsselungsalgorithmus dec sind öffentlich bekannt. 3. Die Entschlüsselungsfunktion dec beschreibt die Abbildung von Paaren aus Schlüssektexen und Schlüsseln auf Nachrichten. 4. Der *die Empfängerin* erhält den Schlüsseltext c über einen unsicheren Kanal und entschlüsselt ihn mithilfe einer Dekodierungsfunktion dec und dem Schlüssel k. 6. Die Schlüsselgenerierung für Schlüssel k muss in einem Vertrauensbereich stattfinden.

## 7 7 Gütekriterien

Welche der Folgenden Aussagen ist korrekt? Wählen Sie eine oder mehrere Antworten:

Antworten: 1. Der Grad der Vollständigkeit wird mit  $k/n$  angegeben, d.h. im Mittel hängen k Output-Zeichen von n Input-Zeichen ab. 3. Output-Zeichen können als lineare Input-Zeichen beschrieben werden, wenn ihre Verschlüsselungsfunktion linear ist. 4. Um eine lineare Verschlüsselungsfunktion zu brechen, kann ein Gleichungssystem aufgestellt und gelöst werden.

In [ ]: