Untitled

November 5, 2019

1 Frage 1

One-Time-Pad

Sie haben eine mit einem One-Time-Pad verschlüsselte Nachricht. Welche Information kann ein*e *Angreifer*in 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]:
```

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 = 13 und F ist ein AND. Berechnen Sie den Klartext. Die verschlüsselte Binärzahl lautet: 00001111

```
In [352]: ''' Leider haben sich fehler bei dieser Aufgabe eingeschlichen.
              TODO: LOESEN'''
          def Feistel_decrypt(key, L, R, rounds):
              if rounds == 0:
                  print('Result R: ' + R + ' Result L: ' + L)
              elif rounds % 2 != 0:
                  R_0 = R
                  L_0 = L
                  R_n = bin(int(F(key, R_0), 2) ^ int(L_0, 2))[2:]
                  L_n = R
                  Feistel_decrypt(key, R_n, L_n, rounds-1)
                  print(L_n + ' ungerade ' + R_n)
              else:
                  R_0 = L
                  L_0 = R
                  R_n = bin(int(F(key, R_0), 2) ^ int(L_0, 2))[2:]
                  L_n = R_0
                  Feistel_decrypt(key, L_n, R_n, rounds-1)

          def F(key, half):
              result = int(half,2)
              return bin(result ^ key)[2:]

In [353]: #Wrong result
          Feistel_decrypt(13, '0000', '1111', 3)

Result R: 0 Result L: 1111
0 ungerade 1111
1111 ungerade 10
```

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 k1 und k2 gearbeitet und beim Verschlüsseln entweder encrypt(k1) -> decrypt(k2) -> encrypt(k1) (EDE-Modus) oder encrypt(k1) -> encrypt(k2) -> encrypt(k1) (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. encrypt(k1) -> encrypt(k2) -> encrypt(k3). Geben Sie das Ergebnis als 2 hoch x an, wobei x eine natürliche Zahl ist.

Antwort: 2^{112} 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 Schlüsektexten und Schlüsseln auf Nachrichten. 4. Der*die Empfänger*in 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 [ ]:
```