

Projekt 2 - Gruppe 8

Oliver Gebhard Noel Kuntze Andrey Nikolaev
Anna Ostrovskaya

10. Januar 2014

Inhaltsverzeichnis

1	Einleitung	3
1.1	Szenario	3
1.2	Problemstellung	3
2	Umsetzung	3
2.1	Zufallszahlengenerator	4
2.2	Backtracking	4
3	Analyse	5
3.1	Vernam-Chiffre	5
3.2	One-Time-Pad	5
3.3	Vollständige Suche	5
A	Anhang	6
A.1	LFSR Runden	6

1 Einleitung

Im Zuge dieser Projektarbeit soll ein Known-Plaintext-Angriff auf eine einfache Stromchiffre realisiert werden. Und im zweiten Schritt geknackt werden. Hierbei soll es möglich sein mit einem gegebenen Klartext/ Chiffretext-Paar den Schlüssel (oder einen Schlüssel), der zum verschlüsseln des Klartextes verwendet wurde, berechnet werden. Nachfolgend wird der Klartext mit m (Message) der Chiffretext mit c (Cipher) und der Schlüssel je nach Kontext mit k (Key) oder a (lt. Aufgabenstellung) abgekürzt. Das Ergebnis aus Klartext XOR Chiffretext wird mit z abgekürzt (lt. Aufgabenstellung).

1.1 Szenario

Gegeben ist die Funktionsweise eines Pseudozufallszahlengenerator mit dem Namen Crappy-One, der die Basis für eine Stromchiffre darstellt. Diese Stromchiffre wird mit einem 10 Byte langen Schlüssel gefüttert und verschlüsselt damit ein 16 Byte langen Klartext. Aus dem Klartext und dem resultierenden Chiffretext soll nun der Schlüssel wiederhergestellt werden. Der Wiederherstellungsprozess des Schlüssels soll über einen Backtracking-Algorithmus realisiert werden.

1.2 Problemstellung

Das Problem besteht im Groben aus zwei Komponenten:

- den Zufallszahlengenerator, um den die Stromchiffre gebaut wird
- dem Backtracking-Algorithmus, zum finden eines passenden Schlüssels

2 Umsetzung

Legende:

a - Schlüsselbyte

z - Verschlüsselungsbyte

\oplus steht für XOR mit Rotation um 5 Bit nach rechts.

\boxplus steht für Addition MOD 256.

Um die Verwirrung in Grenzen zu halten wird ab 0 beginnend gezählt.

Allgemein:

Wobei i die aktuelle Runde bzw. der aktuelle Takt darstellt.

Für die Runden 0 bis 6 gilt für z (das Verschlüsselungsbyte):

$$z_i \leftarrow a_i \boxplus a_{i+3}$$

Ab Runde 7 bis 9 wird das erste mal ein bereits überschriebenes Schlüsselbyte verwendet:

$$z_i \leftarrow a_i \bmod 10 \boxplus (a_{i+3} \bmod 10 \oplus a_{i+8} \bmod 10)$$

Von Runde 10 bis 14 werden zwei Schlüsselbytes die schon überschrieben wurden benutzt. In Runde 15 wurde ein Schlüsselbyte bereits das zweite mal überschrieben.

¹

2.1 Zufallszahlengenerator

Linearesrückkopplungsschieberegister
Beschreibung

²

2.2 Backtracking

Allgemeine Herangehensweise:
Pseudocode

Backtrack(input)

```
//Prüfe Teillösung
IF (Teillösung falsch) RETURN

//Prüfe Gesamtlösung
IF (Lösung korrekt)
    OUTPUT Lösung
    RETURN
ELSE
    RETURN
```

¹Anhang

²<http://en.wikipedia.org/LFSR>

```
//Erweitere Teillösung
FOR ALL
    Backtrack(input + 1)
```

3 Analyse

3.1 Vernam-Chiffre

$$c_i = m_i \oplus z_i$$

3.2 One-Time-Pad

3.3 Vollständige Suche

Probiere jede mögliche Kombination

A Anhang

A.1 LFSR Runden

Was passiert in jeder Runde?

Kein Anspruch auf Richtigkeit:

Innerer Zustand in Runde 0:

$$a_0 \mid a_1 \mid a_2 \mid a_3 \mid a_4 \mid a_5 \mid a_6 \mid a_7 \mid a_8 \mid a_9$$

$$z_0 \leftarrow a_0 \boxplus a_3$$

$$a'_0 \leftarrow a_0 \oplus a_5$$

Innerer Zustand in Runde 1:

$$a'_0 \mid a_1 \mid a_2 \mid a_3 \mid a_4 \mid a_5 \mid a_6 \mid a_7 \mid a_8 \mid a_9$$

$$z_1 \leftarrow a_1 \boxplus a_4$$

$$a'_1 \leftarrow a_1 \oplus a_6$$

Innerer Zustand in Runde 2:

$$a'_0 \mid a'_1 \mid a_2 \mid a_3 \mid a_4 \mid a_5 \mid a_6 \mid a_7 \mid a_8 \mid a_9$$

$$z_2 \leftarrow a_2 \boxplus a_5$$

$$a'_2 \leftarrow a_2 \oplus a_7$$

Innerer Zustand in Runde 3:

$$a'_0 \mid a'_1 \mid a'_2 \mid a_3 \mid a_4 \mid a_5 \mid a_6 \mid a_7 \mid a_8 \mid a_9$$

$$z_3 \leftarrow a_3 \boxplus a_6$$

$$a'_3 \leftarrow a_3 \oplus a_8$$

Innerer Zustand in Runde 4:

$$a'_0 \mid a'_1 \mid a'_2 \mid a'_3 \mid a_4 \mid a_5 \mid a_6 \mid a_7 \mid a_8 \mid a_9$$

$$z_4 \leftarrow a_4 \boxplus a_7$$

$$a'_4 \leftarrow a_4 \oplus a_9$$

Innerer Zustand in Runde 5:

$$a'_0 \mid a'_1 \mid a'_2 \mid a'_3 \mid a'_4 \mid a_5 \mid a_6 \mid a_7 \mid a_8 \mid a_9$$

$$z_5 \leftarrow a_5 \boxplus a_8$$

$$a'_5 \leftarrow a_5 \oplus a'_0, (a_0 \oplus a_5)$$

Innerer Zustand in Runde 6:

$$a'_0 \mid a'_1 \mid a'_2 \mid a'_3 \mid a'_4 \mid a'_5 \mid a_6 \mid a_7 \mid a_8 \mid a_9$$

$$\begin{aligned} z_6 &\leftarrow a_6 \boxplus a_9 \\ a'_6 &\leftarrow a_6 \oplus a'_1, (a'_1 \leftarrow a_1 \oplus a_6) \end{aligned}$$

Innerer Zustand in Runde 7:

$$a'_0 \mid a'_1 \mid a'_2 \mid a'_3 \mid a'_4 \mid a'_5 \mid a'_6 \mid a_7 \mid a_8 \mid a_9$$

$$\begin{aligned} z_7 &\leftarrow a_7 \boxplus a'_0, (a_0 \oplus a_5) \\ a'_7 &\leftarrow a_7 \oplus a'_2, (a_2 \oplus a_7) \end{aligned}$$

Innerer Zustand in Runde 8:

$$a'_0 \mid a'_1 \mid a'_2 \mid a'_3 \mid a'_4 \mid a'_5 \mid a'_6 \mid a'_7 \mid a_8 \mid a_9$$

$$\begin{aligned} z_8 &\leftarrow a_8 \boxplus a'_1, (a_1 \oplus a_6) \\ a'_8 &\leftarrow a_8 \oplus a'_3, (a_3 \oplus a_8) \end{aligned}$$

Innerer Zustand in Runde 9:

$$a'_0 \mid a'_1 \mid a'_2 \mid a'_3 \mid a'_4 \mid a'_5 \mid a'_6 \mid a'_7 \mid a'_8 \mid a_9$$

$$\begin{aligned} z_9 &\leftarrow a_9 \boxplus a'_2, (a_2 \oplus a_7) \\ a'_9 &\leftarrow a_9 \oplus a'_4, (a_4 \oplus a_9) \end{aligned}$$

Innerer Zustand in Runde 10:

$$a'_0 \mid a'_1 \mid a'_2 \mid a'_3 \mid a'_4 \mid a'_5 \mid a'_6 \mid a'_7 \mid a'_8 \mid a'_9$$

$$\begin{aligned} z_{10} &\leftarrow a'_0 \boxplus a'_3, (a_0 \oplus a_5) \boxplus (a_3 \oplus a_8) \\ a''_0 &\leftarrow a'_0 \oplus a'_5, (a_0 \oplus a_5) \oplus (a_5 \oplus (a_0 \oplus a_5)) \end{aligned}$$

Innerer Zustand in Runde 11:

$$a''_0 \mid a'_1 \mid a'_2 \mid a'_3 \mid a'_4 \mid a'_5 \mid a'_6 \mid a'_7 \mid a'_8 \mid a'_9$$

$$\begin{aligned} z_{11} &\leftarrow a'_1 \boxplus a'_4, (a_1 \oplus a_6) \boxplus (a_4 \oplus a_9) \\ a''_1 &\leftarrow a'_1 \oplus a'_6, (a_1 \oplus a_6) \oplus (a_6 \oplus (a_1 \oplus a_6)) \end{aligned}$$

Innerer Zustand in Runde 12:

$$a''_0 \mid a''_1 \mid a'_2 \mid a'_3 \mid a'_4 \mid a'_5 \mid a'_6 \mid a'_7 \mid a'_8 \mid a'_9$$

$$z_{12} \leftarrow a'_2 \boxplus a'_5, (a_2 \oplus a_7) \boxplus (a_5 \oplus (a_0 \oplus a_5))$$

$$a''_2 \leftarrow a'_2 \oplus a'_7, (a_2 \oplus a_7) \oplus (a_7 \oplus (a_2 \oplus a_7))$$

Innerer Zustand in Runde 13:

$$a''_0 \mid a''_1 \mid a''_2 \mid a'_3 \mid a'_4 \mid a'_5 \mid a'_6 \mid a'_7 \mid a'_8 \mid a'_9$$

$$z_{13} \leftarrow a'_3 \boxplus a'_6, (a_3 \oplus a_8) \boxplus (a_6 \oplus (a_1 \oplus a_6))$$

$$a''_3 \leftarrow a'_3 \oplus a'_8, (a_3 \oplus a_8) \oplus (a_8 \oplus (a_3 \oplus a_8))$$

Innerer Zustand in Runde 14:

$$a''_0 \mid a''_1 \mid a''_2 \mid a''_3 \mid a'_4 \mid a'_5 \mid a'_6 \mid a'_7 \mid a'_8 \mid a'_9$$

$$z_{14} \leftarrow a'_4 \boxplus a'_7, (a_4 \oplus a_9) \boxplus (a_7 \oplus (a_2 \oplus a_7))$$

$$a''_4 \leftarrow a'_4 \oplus a'_9, (a_4 \oplus a_9) \oplus (a_9 \oplus (a_4 \oplus a_9))$$

Innerer Zustand in Runde 15:

$$a''_0 \mid a''_1 \mid a''_2 \mid a''_3 \mid a''_4 \mid a'_5 \mid a'_6 \mid a'_7 \mid a'_8 \mid a'_9$$

$$z_{15} \leftarrow a'_5 \boxplus a'_8, (a_5 \oplus (a_0 \oplus a_5)) \boxplus (a_8 \oplus (a_3 \oplus a_8))$$

$$a''_5 \leftarrow a'_5 \oplus a''_0, (a_5 \oplus a_0) \oplus ((a_0 \oplus a_5) \oplus (a_5 \oplus (a_0 \oplus a_5)))$$

Literatur

- [1] LFSR <http://en.wikipedia.org/LFSR>