Projekt 2 - Gruppe 8

Oliver Gebhard Noel Kuntze Andrey Nikolaev
Anna Ostrovskaya

9. Januar 2014

Inhaltsverzeichnis

1 Einleitung

1.1 Szenario

1.2 Problemstellung

2 Linear Feedback Shift Register

Linearesrückkopplungsschieberegister
Beschreibung

[1]

3 Vernam-Chiffre

3.1 One-Time-Pad

4 Analyse

```
Legende:
a - Schlüsselbyte
z - Verschlüsselungsbyte
 ⊕  steht für XOR mit Rotation um 5 Bit nach rechts.
 ⊞  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:
```

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

[1] http://en.wikipedia.org/LFSR

```
Von Runde 10 bis 14 werden zwei Schlüsselbytes die schon überschrieben wurden be
In Runde 15 wurde ein Schlüsselbyte bereits das zweite mal überschrieben.
```
[2]

4.1 Vollständige Suche

Probiere jede mögliche Kombination

4.2 Backtracking

Allgemeine Herangehensweise:
Pseudocode

```
Backtrack(input)

    //Prüfe Teillösung
    IF (Teillösung falsch) RETURN

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

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

[2] Anhang

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

$z_6 \leftarrow a_6 \boxplus a_9$
$a'_6 \leftarrow a_6 \oplus a'_1 \ , \ (a'_1 \leftarrow a_1 \oplus a_6)$

`Innerer Zustand in Runde 7:`
$a'_0 \mid a'_1 \mid a'_2 \mid a'_3 \mid a'_4 \mid a'_5 \mid a'_6 \mid a_7 \mid a_8 \mid a_9$

$z_7 \leftarrow a_7 \boxplus a'_0 \ , \ (a_0 \oplus a_5)$
$a'_7 \leftarrow a_7 \oplus a'_2 \ , \ (a_2 \oplus a_7)$

`Innerer Zustand in Runde 8:`
$a'_0 \mid a'_1 \mid a'_2 \mid a'_3 \mid a'_4 \mid a'_5 \mid a'_6 \mid a'_7 \mid a_8 \mid a_9$

$z_8 \leftarrow a_8 \boxplus a'_1 \ , \ (a_1 \oplus a_6)$
$a'_8 \leftarrow a_8 \oplus a'_3 \ , \ (a_3 \oplus a_8)$

`Innerer Zustand in Runde 9:`
$a'_0 \mid a'_1 \mid a'_2 \mid a'_3 \mid a'_4 \mid a'_5 \mid a'_6 \mid a'_7 \mid a'_8 \mid a_9$

$z_9 \leftarrow a_9 \boxplus a'_2 \ , \ (a_2 \oplus a_7)$
$a'_9 \leftarrow a_9 \oplus a'_4 \ , \ (a_4 \oplus a_9)$

`Innerer Zustand in Runde 10:`
$a'_0 \mid a'_1 \mid a'_2 \mid a'_3 \mid a'_4 \mid a'_5 \mid a'_6 \mid a'_7 \mid a'_8 \mid a'_9$

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

`Innerer Zustand in Runde 11:`
$a''_0 \mid a'_1 \mid a'_2 \mid a'_3 \mid a'_4 \mid a'_5 \mid a'_6 \mid a'_7 \mid a'_8 \mid a'_9$

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

`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`