htw saar

Studiengang Kommunikationsinformatik (Master)
Studiengang Praktische Informatik (Master)
Prof. Dr.–Ing. Damian Weber

Projekt Kryptographie (Stromchiffren)

Das Projekt Kryptographie ist gedacht als Teamarbeit in einem 2er–Team für eine der folgenden Aufgaben. Die jeweilige Aufgabe kann auch alleine gelöst werden mit reduzierter Aufgabenstellung.

Aufgabe: A5/1 und A5/2

Implementieren Sie A5/1 und A5/2.

Verifizieren Sie Ihre Implementierung anhand von Testvektoren.

Implementieren Sie die Attacken von Barkan, Biham, Keller auf die GSM-Verschlüsselungen A5/1 und A5/2

```
Barkam, Elad; Biham, Eli; Keller, Nathan (2008),
"Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication"
```

Aufgabe: E0

Implementieren Sie E0 aus

```
Cryptanalysis of the Bluetooth Stream Cipher (2001)

Christophe De Canniere, Thomas Johansson, Bart Preneel
```

Verifizieren Sie Ihre Implementierung anhand von Testvektoren.

Finden Sie algebraische Ausdrücke für die Zustandsbits nach mehreren Iterationen und möglichst viele Keystream Bits.

Aufgabe: Bivium

Implementieren Sie Bivium aus

```
Havard Raddum (2006)

Cryptanalytic Results on Trivium, Abschnitt 3
```

Verifizieren Sie Ihre Implementierung anhand von Testvektoren.

Finden Sie algebraische Ausdrücke für die Zustandsbits nach mehreren Iterationen und möglichst viele Keystream Bits.