Hochschule für
Technik und Wirtschaft
des Saarlandes
University of Applied Sciences

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

Sicherheit und Kryptographie – Praktische Übung

Aufgabe 1 (Polynome $\mathbf{F}_2[X]$)

Implementieren Sie eine Arithmetik-Library `libf2x.a` für Polynome $\in \mathbf{F}_2[X]$ in C oder C++.

a) Datenstruktur:

```
struct f2poly
{
        int n; /* Grad des Polynoms */
        unsigned long *a; /* Bits = Koeffizienten des Polynoms */
/* allokiert werden müssen n/sizeof(long)+1 Bytes */
}
```

Beispiel:

$$f(X) = X^{32} + X^2 + 1 \tag{1}$$

Dann ist `a[0]=5` und `a[1]=1`.

b) Entwickeln Sie zuerst diverse Hilfsfunktionen

- `set_bit(...)` Setzen des i–ten Koeffizienten auf 1
- `clear_bit(...)` Setzen des i–ten Koeffizienten auf 0
- `find_leading_bit(...)` Finden des höchsten Koeffizienten

c) Ausgabe: `to_string(...)`
Ein Polynom vom Typ `f2poly` soll in folgender Form in einen String umgewandelt werden, z.B.

```
x^32+x^2+1
```

für das Polynom aus (1).

d) Eingabe: `to_f2poly(...)`
Ein String soll in ein `f2poly` umgewandelt werden.

e) Addition: `add(...)`

$$h(X) = f(X) + g(X)$$

Die Funktion gibt $h(X)$ zurück.

f) Multiplikation: `mul(...)`

$$h(X) = f(X) \cdot g(X)$$

g) Potenzierung: `power(...)`

$$h(X) = f(X)^m$$

Die Funktion gibt $h(X)$ zurück.

h) Division von f durch g mit Rest: `div_rem(...)`

$$f(X) = q(X) \cdot g(X) + r(X)$$

Die Funktion gibt $q(X)$ und $r(X)$ zurück. Der Grad von $r(X)$ muß kleiner als der Grad von g sein.

Aufgabe 2 (Irreduzibilitätstest $\mathbf{F}_2[X]$)

Benutzen Sie Ihre `libf2x.a`, um für ein gegebenes Polynom entscheiden zu können, ob es irreduzibel sind. Falls es nicht irreduzibel ist, soll ein Faktor ausgegeben werden. Nennen Sie das Programm `irred_test`.

Versuchen Sie für alle Grade n mit $2 \leq n \leq 100$ ein irreduzibles Polynom mit höchstens drei oder fünf von 0 verschiedenen Koeffizienten zu finden. Nennen Sie das Programm `irred_search`

Aufgabe 3 (Erzeugertest $\mathbf{F}_{2^n}$)

Das Programm soll für ein gegebenes irreduzibles Polynom vom Grad $n \leq 31$ einen Erzeuger für $\mathbf{F}_{2^n}$ finden. Nennen Sie das Programm `gen_search`.