

# Übungen zur Kryptographie und Datensicherheit

Andre Löffler

October 24, 2013

# 1. Übung

## 1.1 Aufgabe 1

$A \subseteq \mathbb{N}$ ,  $\mu$  probabilistische Maschine mit  $P(\mu(x) = c_A(x)) = \alpha \geq \frac{3}{4}$ . O.B.d.A gibt  $\mu$  nur Werte aus  $0, 1$  zurück.  $\mu'$  arbeitet wie folgt:

1. simuliere  $\mu(x)$  und weise diesen Wert  $y_1$  zu.
2. simuliere  $\mu(x)$  und weise diesen Wert  $y_2$  zu.
3. simuliere  $\mu(x)$  und weise diesen Wert  $y_3$  zu.
4. simuliere  $\mu(x)$  und weise diesen Wert  $y_4$  zu.
5. simuliere  $\mu(x)$  und weise diesen Wert  $y_5$  zu.
6. simuliere  $\mu(x)$  und weise diesen Wert  $y_6$  zu.
7. simuliere  $\mu(x)$  und weise diesen Wert  $y_7$  zu.
8. Falls Mehrzahl der  $y_i$  gleich 1 ist, gib 1 zurück.

$$P(\mu'(x) \neq c_A(x)) = P(\text{mind. 4 der } y_i \text{ haben nicht den Wert } c_A(x))$$

$$\begin{aligned} &= \sum_{k=4}^7 P(\text{genau } k \text{ der } y_i \neq c_A(x)) \\ &= \binom{7}{4}(1-\alpha)^4\alpha^3 + \binom{7}{5}(1-\alpha)^5\alpha^2 + \binom{7}{6}(1-\alpha)^6\alpha + \binom{7}{7}(1-\alpha)^7 \end{aligned}$$

Nebenüberlegung:

$$\alpha(1-\alpha) = -(\alpha - \frac{1}{2})^2 + \frac{1}{4}. \quad \alpha \text{ ist im Intervall } [\frac{1}{2}, 1] \text{ monoton fallend:}$$

$$\alpha(1-\alpha) \leq \frac{3}{4} \cdot \frac{1}{4} = \frac{3}{16}.$$

Schätze damit  $1-\alpha \leq \frac{1}{4}$  ab. Damit ist obige Summe  $\leq 0,08$ .

$$P(\mu'(x) = c_A(x)) = 1 - P(\mu'(x) \neq c_A(x)) \geq 1 - 0,08 \geq \frac{11}{12}$$

## 1.2 Aufgabe 2

1. Alphabet  $\{1, 2\}$  ist endliche, nichtleere Menge. ✓
2.
  - $K$  ist deterministisch, also auch probabilistischer Algorithmus.
  - Legendres Vermutung: zwischen  $n^2$  und  $(n+1)^2$  liegt stets eine Primzahl.
  - Angenommen, die Vermutung gilt und wir suchen ab  $m = \underbrace{1 \dots 1}_{n+1}$  nach einer Primzahl, könnte es sein, dass wir erst bei  $(\sqrt{m} + 1)^2 = m + 2\sqrt{m} + 1$  fündig werden.
  - Testen also,  $O(\sqrt{n}) = O(n^{\frac{1}{2}}) = O(2^{\frac{1}{2}n})$  Zahlen  
⇒ nicht klar, ob Polynomialzeit möglich ist.
3.  $\varepsilon(e, m)$  liefert  $e \cdot \text{dya}^{-1}(m)$  für  $m \in \{1, 2\}^*$   
⇒ Polynomialzeit-Algorithmus ✓

4.  $D(d, c)$  liefert  $\text{dya}(\frac{c}{q})$ , wobei  $q$  der größte Primfaktor von  $c$  ist.  $\Rightarrow$  unklar ob im Polynomialzeit möglich, da Faktorisierung nötig.
5. Sei  $(e, d)$  ein von  $K(1^n)$  genutztes Schlüsselpaar und  $m \in \{1, 2\}$   
 $\Rightarrow (e, d) = (q, 1)$ , wobei  $q$  die kleine Primzahl mit  $|\text{dya}(q)| > n$   
 $\Rightarrow \varepsilon(e, m) = q \cdot \text{dya}^{-1}(m)$

$$D(d, \varepsilon(e, m)) = D(1, q \cdot \text{dya}^{-1}(m)) = \text{dya} \left( \overbrace{\frac{q \cdot \text{dya}^{-1}(m)}{q'}}^c \right), \text{ wobei } q' \text{ der}$$

größte Primfaktor von  $c$  ist.

$q = q'$ , weil  $|m| = n < |\text{dya}(q)|$ ,  $q$  größter Primfaktor von  $q \cdot \text{dya}^{-1}(m)$

$\Rightarrow D(d, \varepsilon(e, m)) = \text{dya}(\text{dya}^{-1}(m)) = m \checkmark$

### 1.3 Hinweise zu Übungsblatt 2

1. Sei  $p$  eine Primzahl.  
 $\mathbb{F}_p =_{\text{def}} (\mathbb{Z}_p, +_p, \cdot_p)$  mit  $+_p, \cdot_p$ : Addition und Multiplikation modulo  $p$ .  
 $\mathbb{F}_p$  ist ein endlicher Körper, der (bis auf Isomorphie) einzige endliche Körper mit genau  $p$  Elementen.  
 Beispiel:  $\mathbb{F}_2$ : 1 ist das Einselement, 0 ist das Nullelement.  $5 \cdot 3 = 1$ , also ist 3 das inverse Element zu 5.
2. Sei  $q = p^n$  mit einer Primzahl  $p$  und  $n \geq 2$ . Ziel: der Körper  $\mathbb{F}_q$  mit  $q$  Elementen.

$$\begin{aligned} \mathbb{F}_p[x] &= \text{Menge aller Polynome mit Koeffizienten aus } \mathbb{F}_p \\ &= \{a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x^1 + a_0 \mid n \geq 0, a_0, \dots, a_n \in \mathbb{F}_p\} \\ &= \{(a_n, \dots, a_0) \mid n \geq 0, a_n, \dots, a_0 \in \mathbb{F}_p\} \end{aligned}$$

Die Multiplikation von Elementen aus  $\mathbb{F}_p[x]$  entspricht der Polynommultiplikation.

Beispiel:  $\mathbb{F}_2[x]: (x^2 + 1)(x^2 + 1) = x^4 + 2x^2 + 1 = x^4 + 1$

**Definition 1** Ein Polynom  $g \in \mathbb{F}_p[x]$  heißt irreduzibel über  $\mathbb{F}_p$   
 $\Leftrightarrow_{\text{def}}$  es gibt keine Polynome  $p_1, p_2 \in \mathbb{F}_p[x]$  mit  $\text{Grad} \geq 1$  mit  $g = p_1 \cdot p_2$

**Satz 1.1**  $x^8 + x^4 + x^3 + x + 1$  ist irreduzibel über  $\mathbb{F}_p$ .

**Definition 2** Sei  $g \in \mathbb{F}_p[x]$  irreduzibel und vom Grad  $k \geq 1$ .

$$\begin{aligned} \mathbb{F}_p[x]/g &=_{\text{def}} \{f \in \mathbb{F}_p[x] \mid \text{Grad von } f < k\} \\ &= \text{Reste bei Polynomdivision durch } g \\ &= \{(a_{k-1}, \dots, a_0) \mid a_0, \dots, a_{k-1} \in \mathbb{F}_p\} \end{aligned}$$

**Satz 1.2** [Addition in  $F$ ]

Addition der Polynome, wobei die Koeffizienten entsprechend  $\mathbb{F}_p$  addiert werden.

**Satz 1.3** [Multiplikation in  $F$ ]

$\underbrace{p_1 \cdot p_2}_{\text{Multiplikation in } \mathbb{F}_p[x]/g} = \text{Rest von } \underbrace{p_1 \cdot p_2}_{\text{Multiplikation in } \mathbb{F}_p[x]} \text{ bei Division durch } g.$

Beispiel:  $p = 2$  und  $g(x) = x^8 + x^4 + x^3 + x + 1 \in \mathbb{F}_2[x]$ .

Sei  $p_1 = x^7 + x^2 + 1$  und  $p_2 = x_2 + 1 \in \mathbb{F}_2[x]/g$ .

$$\begin{aligned} p_1 \cdot p_2 &= ((x^7 + x^2 + 1) \cdot (x^2 + 1)) \bmod g \\ &= (x^9 + x^4 + x^2 + x^7 + x^2 + 1) \bmod g \\ &= (x^9 + x^7 + x^4 + 1) \bmod g \\ &= ((x^9 + x^7 + x^4 + 1) - x \cdot g) \bmod g \\ &= ((x^9 + x^7 + x^4 + 1) - (x^9 + x^5 + x^4 + x^2 + x)) \bmod g \\ &= (x^7 + x^5 + x^2 + x + 1) \bmod g \\ &= (x^7 + x^5 + x^2 + x + 1) \end{aligned}$$

**Satz 1.4** Sei  $p$  eine Primzahl,  $k \geq 2$  und  $g \in \mathbb{F}_p[x]$  irreduzibel und vom Grad  $k$ . Dann ist

$$\mathbb{F}_{p^k} = \text{def}(\mathbb{F}_p[x]/g, +, \cdot)$$

der einzige endliche Körper mit  $p^k$  Elementen (bis auf Isomorphie).

Beispiel: Sei  $g = x^8 + x^4 + x^3 + x + 1$ . Die Elemente von  $\mathbb{F}_{2^8} = \mathbb{F}_2[x]/g = \{(a_7, \dots, a_0) | a_0, \dots, a_7 \in \{0, 1\}\}$  lassen sich als Bytes interpretieren.

$$\begin{aligned} 0x03 \cdot 0xa1 &= 0b00000011 \cdot 0b10100001 \\ &= (x + 1) \cdot (x^7 + x^5 + 1) \bmod g \\ &= (x^8 + x^6 + x + x^7 + x^5 + 1) \bmod g \\ &= (x^7 + x^6 + x^5 + x^4 + x^3) \\ &= 0b11111000 = 0xf8 \end{aligned}$$

$$\Rightarrow 3 \cdot 161 = 248.$$