Übungen zur Kryptographie und Datensicherheit

Andre Löffler

October 28, 2013

1 1. Übung

1.1 Aufgabe 1

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

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

Nebenüberlegung:
$\alpha(1-\alpha) = -(\alpha - \frac{1}{2})^2 + \frac{1}{4}$. α ist im Intervall $[\frac{1}{2}, 1]$ 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 $m = \underbrace{1\ldots1}_{n+1}$ 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
     $\Rightarrow$ nicht klar, ob Polynomialzeit möglich ist.
3. $\varepsilon(e, m)$ liefert $e \cdot \text{dya}^{-1}(m)$ für $m \in \{1, 2\}^*$
   $\Rightarrow$ Polynomialzeit-Algorithmus ✓

4. $D(d,c)$ liefert $\mathrm{dya}(\frac{c}{q})$, wobei q der größte Primfaktor von q ist. $\Rightarrow$ unklar ob im Polynomialzeit möglich, da Faktorisierung nötig.

5. Sei (e,d) ein von $K(1^n)$ genutzes Schlüsselpaar und $m \in \{1,2\}$
$\Rightarrow (e,d) = (q,1)$, wobei q die kleine Primzahl mit $|\mathrm{dya}(q)| > n$
$\Rightarrow \varepsilon(e,m) = q \cdot \mathrm{dya}^{-1}(m)$
$D(d, \varepsilon(e,m)) = D(1, q \cdot \mathrm{dya}^{-1}(m)) = \mathrm{dya}\left(\frac{\overbrace{q \cdot \mathrm{dya}^{-1}(m)}^{c}}{q'}\right)$, wobei q' der größte Primfaktor von c ist.
$q = q'$, weil $|m| = n < |\mathrm{dya}(q)|$, q größter Primfaktor von $q \cdot \mathrm{dya}^{-1}(m)$
$\Rightarrow D(d, \varepsilon(e,m)) = \mathrm{dya}(\mathrm{dya}^{-1}(m)) = m$ ✓

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.

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

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 <u>irreduzibel</u> über $\mathbb{F}_p$*
$\Leftrightarrow_{def}$ *es gibt keine Polynome $p_1, p_2 \in \mathbb{F}_p[x]$ mit Grad ≥ 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 $k \geq 1$.*

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

Satz 1.2 *[Addition in F]*
Addition der Polynome, wobei di 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* $p_2 = x_2 + 1 \in \mathbb{F}_2[x]/g$.

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

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

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

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 $\mathbb{F}_{2^8} = \mathbb{F}_2[x]/g = \{(a_7, \cdots, a_0) | a_0, \cdots, a_7 \in \{0, 1\}\}$ lassen sich als Bytes interpretieren.

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

$\Rightarrow 3 \cdot 161 = 248.$

2 Übung 2

2.1 Aufgabe 1

1. $(\{0,1,2,3,4\}, f)$ mit $f(x,y) = (x+y) \mod 5$ ist eine endliche kommutative Gruppe

   - $f : \mathbb{Z}_5 \times \mathbb{Z}_5 \to \mathbb{Z}_5$ ist total ✓
   - Assoziativität:

     $$\begin{aligned} f(f(a,b),c) &= f((a+b) \mod 5, c) \\ &= ((a+b) \mod 5 + c) \mod 5 \\ &= (a+b+c) \mod 5 = (a + (b+c) \mod 5) \mod 5 \\ &= f(a, f(b,c)) ✓ \end{aligned}$$

   - Neutrales Element: $f(x,0) = (x+0) \mod 5 = x$
     $f(0,x) = (0+x) \mod 5 = x$
   - Inverses Element: Sei $a \in \mathbb{Z}_5$:

     $$\begin{aligned} b &= (-a) \mod 5 \\ &= (a + (-a) \mod 5) \mod 5 \\ &= 0 \mod 5 = 0 \end{aligned}$$

     Eindeutigkeit: $0 \mod 5 = 0$ ✓
     Angenommen $f(a,b') = 0 = f(a,b)$ mit $b' \in \mathbb{Z}_5$
     $\Rightarrow b' \mod 5 = b \mod 5$
     $\Rightarrow b' = b$
     $\Rightarrow$ genau ein inverses Element.
   - Kommutativität:
     $f(a,b) = f(b,a) = (a+b) \mod 5 = (b+a) \mod 5 = f(b,a)$✓

2. $(\mathbb{Z}_6, f, g)$ mit $f(x,y) = (x+y) \mod 6$, $g(x,y) = (x \cdot y) \mod 6$ ist kein Körper:
   Damit $(\mathbb{Z}_6), f, g)$ ein Körper ist, muss $(\{1,2,3,4,5\}, g)$ kommutative Gruppe sein.
   $\Rightarrow \forall a \in \{1,2,3,4,5\} \exists! b \in 1,2,3,4,5 : [g(a,b) = 1]$

   - $g(2,1) = 2$
   - $g(2,2) = 4$
   - $g(2,3) = 0$
   - $g(2,4) = 2$
   - $g(2,5) = 4$

   $\Rightarrow$ 2 besitzt kein inverses Element in $(\{1,2,3,4,5\}, g)$
   $\Rightarrow (\mathbb{Z}_6, f, g)$ ist kein Körper.

2.2 Hinweise zu Übungsblatt 3

Monoalphabetische Verschlüsselung (Substitutionschiffre):
ABCDEFGHJKLMNOPQRSTUVWXYZ
pfeile und so

$S = (\Sigma, \mathcal{K}, \mathcal{E}, \mathcal{D})$

- $\Sigma = \{A, \cdots, Z\}$
- Schlüssel: $\pi : \Sigma \to \Sigma$ Bijektion

$$\begin{aligned} P &= \text{ Menge aller Permutationen auf } \Sigma \\ &= \{\pi : \Sigma \to \Sigma | \pi \text{ bijektiv}\} \end{aligned}$$

- $\mathcal{K}(1^n)$ liefert gleichverteilt Element aus $\{(\pi, \pi) | \pi \in P\}$
- $\mathcal{E}(\pi, m_1, m_2, \cdots, m_n) = \pi(m_1)\pi(m_2)\cdots\pi(m_n)$
- $\mathcal{D} = \pi^{-1}(c_1)\pi^{-1}(c_2)\cdots\pi^{-1}(c_n)$

Ist S perfekt sicher?

- Betrachte Klartext der Länge 1
  $P_{\Sigma^1}(a) = \frac{1}{26}$ für alle $a \in \Sigma$
  Sei nun $m \in \Sigma^1$ beliebig.
  $P(E_m) = \frac{1}{26}$ [Wahrscheinlichkeit, das Klartext m gewählt wird.]
  Sei $c \in C_1$ beliebig. [$C_1 = \Sigma$ alle möglichen Chiffretexte der Länge 1]

$$\begin{aligned} P(E_m | E_c) &= P(\mathcal{K}(1) \text{ liefert Permutation } \pi \text{ mit } \pi(m) = c) \\ &= \frac{25!}{26!} = \frac{1}{26} = P(E_m) \end{aligned}$$

  $\Rightarrow$ S ist perfekt sicher bezüglich P_{Σ^1}

- Betrachte gleichverteilte Klartexte der Länge 2
  $P_{\Sigma^2}(m) = \frac{1}{26^2}$ für alle $m \in \Sigma^2$ [$|\Sigma^2| = 26^2$]
  Wähle $m = AF \in \Sigma^2$:
  $P(E_m) = \frac{1}{26^2}$
  $C_2 = \Sigma^2$
  Sei $c = ww \in C_2$

$$\begin{aligned} P(E_m | E_c) &= P(\mathcal{K}(11) \text{ liefert Permutation } \pi \text{ mit } \pi(A) = w \text{ und } \pi(F) = w) \\ &= 0 \neq P(E_m) \end{aligned}$$

  $\Rightarrow$ S nicht perfekt sicher bezüglich P_{Σ^2}
  $\Rightarrow$ S nicht perfekt sicher