Modul Diskrete Mathematik WiSe 2011/12

Ergänzungsskript zum Kapitel 4.2. Hinweis: Dieses Manuskript ist nur verständlich und von Nutzen für Personen, die regelmäßig und aktiv die zugehörige Vorlesung besuchen (also nicht nur körperlich anwesend sind), und es wurde auch nur für diesen Hörerkreis geschrieben. Es erhebt keinen Anspruch auf Vollständigkeit, Fehler sind zwar ärgerlich, aber leider nicht auszuschließen!

4 Kryptographie

2 Public–Key–Kryptographie

Wir stellen zunächst eine Methode vor, die in der Schule behandelt werden kann, aber nur für Nichtmathematiker nicht leicht zu knacken ist.

Beispiel: Eine Nachricht $m \in \{1, 2, \ldots, 342\}$ an E wird mit Hilfe des offiziell bekannten Zahlenpaars $(n = 343, e = 109)$ folgendermaßen verschlüsselt:

$$c := (e \cdot m) \bmod n = (109 \cdot m) \bmod 343$$

Die Rechnung ergibt den Geheimtext $c = 50$.

Wie entschlüsselt der Empfänger E diese Nachricht? Er besitzt den geheimen, nur ihm bekannten Schlüssel $d = 107$ und rechnet einfach

$$m = (d \cdot c) \bmod n = (107 \cdot 50) \bmod 343 = 205$$

Wir machen die Probe: Die Nachricht $m = 205$ wird in der Tat zu $c = (109 \cdot 205) \bmod 343 = 50$ verschlüsselt.

Zur Anwendung dieses Algorithmus hat sich E zwei Zahlen $e, n \in \mathbb{N}$ mit $\mathrm{ggT}\,(e, n) = 1$ ausgesucht. Die Verschlüsselung geschieht durch den öffentlichen Algorithmus $f(x) := (e \cdot x) \bmod n$. Damit verschiedene Nachrichten unterschiedlich chiffriert werden, muss f injektiv sein. Dies ist durch die Voraussetzung der Teilerfremdheit von e und n gewährleistet. Der von E öffentlich bekannt gemachte Schlüssel besteht aus dem Zahlenpaar (n, e).

(Wie) kann ein Angreifer A, der zwar c, n und e, aber nicht d kennt, an die geheime Originalnachricht m gelangen?

Um m aus $50 = (109 \cdot m) \bmod 343$ bestimmen zu können, muss er ein $\alpha \in \mathbb{N}$ finden mit

$$109 \cdot m = \alpha \cdot 343 + 50 \iff m = \frac{\alpha \cdot 343 + 50}{109} \in \{1, 2, \ldots, 342\}$$

Selbst bei den relativ kleinen Zahlen im Beispiel ist dies eine ziemlich langwierige Angelegenheit. Wenn ein Angreifer A allerdings in der Lage ist, aus dem öffentlichen Schlüssel (n, e) den geheimen Schlüssel d zu berechnen, kann er den Code knacken.

Wie hängt d mit dem öffentlichen Zahlenpaar (n, e) zusammen? Kann man eventuell auf einfache Weise aus den bekannten Zahlen das unbekannte d herleiten?

Wir halten fest:

– Verschlüsseln bedeutet $c = (e \cdot m) \bmod n \iff me = \alpha n + c \iff c \equiv_n me$

– Entschlüsseln bedeutet $m = (c \cdot d) \bmod n \iff cd = \beta n + m \iff m \equiv_n cd$

$\Rightarrow\ m \equiv_n (me)d \iff 1 \equiv_n ed.$

Fazit: Man kann entschlüsseln, falls man $d \in \mathbb{Z}$ kennt mit $ed \equiv_n 1$.

Als nächstes geben wir ein Verfahren zur Berechnung von d an. Hierzu benötigt man den euklidischen Algorithmus und das Lemma von Bézout.

Satz 4.2.1 (Lemma von Bézout, siehe auch Beutelspacher 5.3.3, Seite 69)
Seien $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}\,(a, b) = t \quad \Rightarrow \quad \exists\, a', b' \in \mathbb{Z}$ mit $a'a + b'b = t$.

Beweisidee: Berechne zunächst $\mathrm{ggT}\,(a, b) = t$ mit Hilfe des euklidischen Algorithmus und bestimme dann „rückwärts“ a' und b'.

Wir verzichten auf die Durchführung des Beweises und machen uns seine Vorgehensweise lediglich an unserem Zahlenbeispiel klar.

Beispiel: Sei $a = 343$ und $b = 109$. Der euklidische Algorithmus liefert

$$\begin{aligned} 343 &= 3 \cdot 109 + 16 \\ 109 &= 6 \cdot 16 + 13 \\ 16 &= 1 \cdot 13 + 3 \\ 13 &= 4 \cdot 3 + 1 \end{aligned}$$

$$\begin{aligned} \text{Berechnung von } a' \text{ und } b'\text{:}\quad 1 &= 13 - 4 \cdot 3 \;=\; 13 - 4 \cdot (16 - 1 \cdot 13) \\ &= -4 \cdot 16 + 5 \cdot 13 \;=\; -4 \cdot 16 + 5 \cdot (109 - 6 \cdot 16) \\ &= 5 \cdot 109 - 34 \cdot 16 \;=\; 5 \cdot 109 - 34 \cdot (343 - 3 \cdot 109) \\ &= -34 \cdot 343 + 107 \cdot 109 \;=\; a'a + b'b \end{aligned}$$

Aus der letzten Gleichung folgt $107 \cdot 109 = 34 \cdot 343 + 1 \iff 107 \cdot 109 \equiv_{343} 1$.

Fazit: Zur Anwendung dieses Algorithmus besorge man sich zwei nicht zu kleine teilerfremde Zahlen n und e, bestimme d wie oben und hoffe, dass keiner der Beteiligten das Lemma von Bézout kennt.

Ein sichereres Verfahren, der sogenannte *RSA–Algorithmus*, benutzt statt $m \mapsto (me) \bmod n$ die Rechnung $m \mapsto m^e \bmod n$. Um seine Arbeitsweise zu verstehen, beginnen wir mit einigen vorbereitenden Aussagen.

Def 4.2.1 Die Abbildung $\varphi : \mathbb{N} \to \mathbb{N}$ mit $\varphi(n) := |\{1 \le k \le n \mid \mathrm{ggT}\,(k, n) = 1\}|$ heißt *Eulersche φ – Funktion*.

$\varphi(n)$ zählt alle natürliche Zahlen kleiner als n, die teilerfremd zu n sind.

Beispiel: $\varphi(1) = 1 = \varphi(2), \quad \varphi(10) = |\{1, 3, 7, 9\}| = 4, \quad \varphi(243) = 162.$

Einige Eigenschaften dieser Funktion fasst der nächste Satz zusammen.

Satz 4.2.2 Seien p und q verschiedene Primzahlen. Dann gelten
(1) $\varphi(p) = p-1$ (2) $\varphi(p^2) = p(p-1)$ (3) $\varphi(pq) = (p-1)(q-1)$

Beweis (1) $\varphi(p) = |\{1,2,\ldots,p-1\}| = p-1$
(2) Sämtliche Teiler von p^2 sind außer 1 die Zahlen $p, 2p, 3p, \ldots, p\cdot p$. Damit ist $\varphi(p^2) = p^2 - p = p(p-1)$.
(3) Für jedes $x \in \{1,2,\ldots,pq\}$ mit $\mathrm{ggT}\,(x,pq) = a \neq 1$ gilt $a \mid x$ und $a \mid pq$. Weil p und q Primzahlen sind, gilt $a \mid pq \;\Rightarrow\; a \mid p \vee a \mid q \;\Rightarrow\; a \in \{p,q\}$, also ist x ein Vielfaches von p oder von q, d.h., $x \in \{p, 2p, \ldots, qp, q, 2q, \ldots (p-1)q\}$, einer Menge mit $q+p-1$ vielen Elementen.
$\Rightarrow\; \varphi(pq) = pq - (q+p-1) \;=\; pq - q - p + 1 \;=\; (p-1)(q-1) \;=\; \varphi(p)\varphi(q)$.

Satz 4.2.3 (Kleiner Satz von Fermat)
Für jede Primzahl p und jedes $m \in \mathbb{N}$ gilt $m^p \bmod p = m \bmod p$ bzw. $p \mid (m^p - m)$.

Beweis: Wir führen eine Induktion nach m durch, wobei der *Induktionsanfang* $m = 1$ trivialerweise gilt.
Induktionsannahme: Für ein $m \in \mathbb{N}$ sei $m^p = \alpha \cdot p + m$.
Induktionsbehauptung: Für $m+1$ gilt $(m+1)^p = \beta \cdot p + (m+1)$. *Beweis*: Es ist

$$(m+1)^p = \sum_{\nu=0}^{p} \binom{p}{\nu} m^{p-\nu} \;=\; m^p + \sum_{\nu=1}^{p-1} \binom{p}{\nu} m^{p-\nu} + 1$$

Wir untersuchen die Binomialkoeffizienten $\binom{p}{\nu}$ für $\nu \in \{1,\ldots,p-1\}$.

Beh.: $p \mid \binom{p}{\nu}$ *Bew.*: $\binom{p}{\nu} = \frac{p!}{\nu!(p-\nu)!} =: n \iff p! = n \cdot \nu! \cdot (p-\nu)!$

Weil p eine Primzahl ist, teilt p weder $\nu!$ noch $(p-\nu)!$, also gilt $p \mid n = \binom{p}{\nu}$ für jedes dieser ν, und damit ist $\sum_{\nu=1}^{p-1} \binom{p}{\nu} m^{p-\nu}$ ein Vielfaches von p.

Insgesamt folgt mit Hilfe der Induktionsannahme

$$(m+1)^p = m^p + x \cdot p + 1 = \alpha \cdot p + m + x \cdot p + 1 \;=\; (\alpha + x) \cdot p + (m+1)\;.$$

Der nächste Hilfssatz beschäftigt sich mit Modulorechnung.

Hilfssatz Für alle $m, r, n \in \mathbb{N}$ gilt $m^r \bmod n = (m \bmod n)^r \bmod n$

Beweis: Wir setzen $x = m \bmod n$, es gilt also $m = \alpha n + x$ mit $\alpha \in \mathbb{N}$. Es folgt
$m^r = (\alpha n + x)^r = \sum_{\nu=0}^{r} \binom{r}{\nu} (\alpha n)^{r-\nu} x^\nu \;=\; (\cdots)\, n + x^r$ (In $\sum_{\nu=0}^{r-1} \cdots$ wurde n ausgeklammert.)

$$\Rightarrow \quad m^r \bmod n = (\alpha n + x)^r \bmod n = [(\cdots)n + x^r] \bmod n = x^r \bmod n = (m \bmod n)^r \bmod n$$

Analog gelten $(a \cdot b) \bmod n = ((a \bmod n) \cdot (b \bmod n)) \bmod n$, $(a \pm b) \bmod n = ((a \bmod n) \pm (b \bmod n)) \bmod n$.

Ausführliches *Beispiel*:

$$\begin{aligned} 7^{10} \bmod 11 &= (7^2)^5 \bmod 11 \;=\; (7^2 \bmod 11)^5 \bmod 11 \;=\; (49 \bmod 11)^5 \bmod 11 \\ &= 5^5 \bmod 11 \;=\; (5^2 \cdot 5^3) \bmod 11 \;=\; ((5^2 \bmod 11) \cdot (5^3 \bmod 11)) \bmod 11 \\ &= ((25 \bmod 11) \cdot (125 \bmod 11)) \bmod 11 \;=\; (3 \cdot 4) \bmod 11 \;=\; 1 \end{aligned}$$

Wir beschäftigen uns mit Spezialfällen des kleinen Fermat.

Korollar 1 Sei p eine Primzahl und $1 \leq m < p$. Dann gilt $m^{p-1} \equiv_p 1$.

Beweis: Der kleine Fermat besagt $p \mid (m^p - m)$ mit $m^p - m = m(m^{p-1} - 1)$. Es gilt
$1 \leq m < p \;\Rightarrow\; p \nmid m \;\Rightarrow\; p \mid \left(m^{p-1} - 1\right) \;\Rightarrow\; m^{p-1} - 1 = \alpha \cdot p \;\Rightarrow\; m^{p-1} = \alpha \cdot p + 1 \;\Rightarrow\; m^{p-1} \equiv_p 1.$

Beispiel: $14^{16} = 14^{17-1} \equiv_{17} 1$, also $14^{16} = \alpha \cdot 17 + 1$

Korollar 2 Seien m, p wie oben, $k \in \mathbb{N}$. Dann gilt $m^{k(p-1)} \equiv_p 1$.

Beweis: Wir benutzen zuerst den Hilfssatz und dann Korollar 1:
$m^{k(p-1)} \bmod p \;=\; \left(m^{p-1} \bmod p\right)^k \bmod p \;=\; 1^k \bmod p \;=\; 1$

Beispiel: $6^{18} \bmod 7 \;=\; 6^{3(7-1)} \bmod 7 \;=\; 1$

Ab jetzt seien p, q verschiedene Primzahlen.

Korollar 3 Seien $m, k \in \mathbb{N}$ mit $\mathrm{ggT}\,(m, p) = \mathrm{ggT}\,(m, q) = 1$. Dann gilt $m^{k(p-1)(q-1)} \equiv_x 1$ für $x \in \{p, q\}$.

Beweis: Für $x = p$ wenden wir Korollar 2 auf $k' = k(q-1)$ an, für $x = q$ analog auf $k' = k(p-1)$.

Beispiel: Für $p = 3,\ q = 7,\ m = 16,\ k = 4$ gilt $\left(16^{4 \cdot 2 \cdot 6} = 16^{48}\right) \bmod 7 \;=\; 1$

Korollar 4 Seien p, q, m, k wie in Korollar 3. Dann gilt $m^{k(p-1)(q-1)} \equiv_{pq} 1$.

Beweis: Nach Korollar 3 ist $m^{k(p-1)(q-1)} = \alpha \cdot p + 1 = \beta \cdot q + 1 \;\Rightarrow\; \alpha p = \beta q \;\Rightarrow\; q \mid \alpha$
$\Rightarrow\quad \alpha p = (\alpha' q)p = \alpha' pq \quad\Rightarrow\quad m^{k(p-1)(q-1)} = \alpha' pq + 1$

Beispiel: $16^{48} \bmod 21 \;=\; 1$

Im nächsten Satz kommt die Eulersche φ – Funktion vor, wir erinnern uns an $\varphi(pq) = (p-1)(q-1)$, falls p und q verschiedene Primzahlen sind.

Satz 4.2.4 (Satz von Euler)
Seien p, q verschiedene Primzahlen, $k \in \mathbb{N},\ m \in \{1, 2, \ldots, pq-1\},\ n = pq$. Dann gilt

$$m^{k\varphi(n)+1} \;\equiv_n\; m$$

Beweis: 1. Fall: Sei $\mathrm{ggT}\,(m, p) \;= \mathrm{ggT}\,(m, q) \;=\; 1$. Nach Korollar 4 gilt $m^{k(p-1)(q-1)} \equiv_n 1$, hieraus folgt unmittelbar $m^{k\varphi(n)+1} \equiv_n m$.

2. Fall: Sei oBdA $\mathrm{ggT}\,(m, p) > 1$. Weil p eine Primzahl ist, bedeutet dies $p \mid m$. Ferner ist $\mathrm{ggT}\,(m, q) = 1$, sonst folgt aus $q \mid m$ die Ausssage $m > pq$, ein Widerspruch zur Voraussetzung über die Größenordnung von m.
Wir wenden Korollar 2 auf $m,\ k' = k(p-1)$ und $\mathrm{ggT}\,(m, q) = 1$ an:

$$\left(m^{k\varphi(n)} = m^{k'(q-1)}\right) \equiv_q 1 \quad\Rightarrow\quad q \mid \left(m^{k\varphi(n)} - 1\right)$$
$$\Rightarrow\quad (pq = n) \mid \left(m \cdot \left(m^{k\varphi(n)} - 1\right)\right) \;=\; m^{k\varphi(n)+1} - m\ .$$

Beispiel: Wir berechnen $2^{49} \bmod 65$ auf zwei verschiedene Arten:

a) Aus $(2^6 = 64) \bmod 65 = -1$ folgt $\left(2^{49} = \left(2^6\right)^8 \cdot 2\right) \equiv_{65} (-1)^8 \cdot 2 \;=\; 2$

b) Wir nutzen aus, dass $65 = 5 \cdot 13$ ein Produkt zweier Primzahlen ist:
$2^{49} = 2^{48+1} = 2^{4 \cdot 12+1} = 2^{(5-1)\cdot(13-1)+1} \equiv_{5\cdot 13=65} 2$.

Jetzt sind wir bereit für den RSA – Algorithmus:

- Wähle (geheim) sehr große Primzahlen p und q
- Berechne $n = pq$ und $\varphi(n) = (p-1)(q-1)$ (und vertraue darauf, dass eine Faktorisierung von n wegen der Größe der Primzahlen nicht möglich ist)
- Wähle $e \in \mathbb{N}$ mit $\mathrm{ggT}\,(e, \varphi(n)) = 1$ (beispielsweise geeignete Primzahl)
- Berechne $d \in \mathbb{N}$ mit $ed \bmod \varphi(n) = 1$ (hier hilft das Lemma von Bézout)
- Veröffentliche (n, e) (und den Algorithmus $m \mapsto c = m^e \bmod n$)
- Halte geheim d (und natürlich p, q und $\varphi(n)$)

Behauptung: Für $m \in \{1, \ldots, n-1\}$ und $c = (m^e \bmod n)$ gilt $c^d \bmod n = m$.
Beweis: Es ist $c^d \bmod n = (m^e \bmod n)^d \bmod n = m^{ed} \bmod n$ mit $ed = k\varphi(n) + 1$, also

$$c^d \bmod n \;=\; m^{k\varphi(n)+1} \bmod n \;=\; m\,.$$

Der RSA – Algorithmus ist sicher, solange n nicht faktorisiert werden kann, weil dann $\varphi(n)$ nicht bestimmt werden kann, die Kenntnis von $\varphi(n)$ aber zur Berechnung des geheimen Schlüssels d benötigt wird.

Beispiel: $p = 3,\ q = 11 \;\Rightarrow\; n = 33,\ \varphi(n) = 2 \cdot 10 = 20$, ferner sei $e = 13$.

Wir bestimmen d: $\quad 20 = 1 \cdot 13 + 7, \quad 13 = 1 \cdot 7 + 6, \quad 7 = 1 \cdot 6 + 1.$

Damit ist $1 = 7 - 1(13 - 1 \cdot 7) = 2 \cdot 7 - 13 = 2(20 - 13) - 13 = 2 \cdot 20 - 3 \cdot 13$

Unsere Rechnung hat $d = -3$ ergeben. Um ein positive Zahl zu erhalten, benutzen wir einen einfachen Trick:

$$1 \;=\; 2 \cdot 20 - 3 \cdot 13 \;=\; 2 \cdot 20 - 3 \cdot 13 + 20 \cdot 13 - 13 \cdot 20 \;=\; -11 \cdot 20 + 17 \cdot 13$$

Damit ist $d = 17$.

Wir veröffentlichen $(n = 33, e = 13)$ und halten geheim $d = 17$.

Die Verschlüsselung von $m = 2$ ergibt

$$c = 2^{13} \bmod 33 \;=\; 2^{5\cdot 2+3} \bmod 33 \;=\; \left[\left(2^5 \bmod 33\right)^2 \cdot 2^3\right] \bmod 33 \;=\; \left[(-1)^2 \cdot 2^3\right] \bmod 33 \;=\; 8$$

Wir entschlüsseln $c = 8$:

$$\begin{aligned} m \;&=\; 8^{17} \bmod 33 \;=\; \left(2^3\right)^{17} \bmod 33 \;=\; 2^{51} \bmod 33 \;=\; \left(2^{40} \cdot 2^{11}\right) \bmod 33 \\ &=\; \left(\left(2^{2\cdot(3-1)(11-1)} \bmod 33\right) \cdot \left(2^{11} \bmod 33\right)\right) \bmod 33 \\ &=\; 1 \cdot \left(\left(2^{10} \bmod 33\right) \cdot (2 \bmod 33)\right) \bmod 33 \;=\; \left(\left(2^5 \bmod 33\right)^2 \bmod 33 \cdot 2\right) \bmod 33 \\ &=\; (-1)^2 \cdot 2 \;=\; 2 \end{aligned}$$