WS 2014/15

Diskrete Strukturen

Kapitel 5: Algebraische Strukturen (RSA-Verfahren)

Hans-Joachim Bungartz

Lehrstuhl für wissenschaftliches Rechnen
Fakultät für Informatik
Technische Universität München

http://www5.in.tum.de/wiki/index.php/Diskrete_Strukturen_-_Winter_14

- Das RSA-Kryptosystem:
  - Kryptosystem: Verfahren zur Verschlüsselung und Entschlüsselung von Nachrichten.
  - Schlüssel: Objekte (Zahlen, Bitstrings), die für die Verschlüsselung und Entschlüsselung verwendet werden.

- Symmetrische Kryptosysteme (secret key):
  - Sender und Empfänger verwenden zum Ver- und Entschlüsseln einen einzigen, nur ihnen bekannten geheimen Schlüssel.
  - Die Sicherheit der Kommunikation hängt von der sicheren Aufbewahrung der geheimen Schlüssel ab.
  - Problem: Man braucht einen Schlüssel, um zu kommunizieren, aber man muss kommunizieren, um sich auf einen Schlüssel zu einigen…

- Asymmetrische Kryptosysteme (public key):
  - Jeder Teilnehmer hat zwei Schlüssel: Einen geheimen Schlüssel (private key) und einen öffentlichen Schlüssel (public key).
  - Die öffentlichen Schlüssel werden in einem öffentlichen „Schlüsselverzeichnis“ veröffentlicht (vgl. Telefonbuch).
  - Eine Nachricht von A an B wird von A mit Hilfe des öffentlichen Schlüssels von B verschlüsselt.
  - Die Entschlüsselung einer chiffrierten Nachricht erfolgt mit dem privaten Schlüssel von B.

- Das RSA-Kryptosystem:
  - Das populärste asymmetrische Kryptosystem.
  - Benannt nach Rivest, Shamir, und Adleman (ähnliche Methode von Cocks wurde geheim gehalten).
  - Die Schlüssel sind (sehr) große Zahlen.
  - Die Verfahren für Ver- und Entschlüsselung basieren auf Zahlentheorie.

- Das RSA Kryptosystem – Schlüssel:
  - Jeder Teilnehmer erzeugt zwei große Primzahlen p und q und setzt $n = pq$.
  - Sei $\phi := |\mathbb{Z}_n^*| = (p-1)(q-1)$.
  - Die Teilnehmer wählen $c \in \mathbb{Z}_\phi^*$ und berechnen $d := c^{-1}$, das inverse Element von c in $\langle \mathbb{Z}_\phi^*, *_\phi \rangle$.

    (d kann mit dem erweiterten Euklidischen Algorithmus berechnet werden).
  - Öffentlicher Schlüssel: (n, c)
  - Privater Schlüssel: d

- Das RSA Kryptosystem – Verschlüsseln: (Vereinfacht!)

  Um eine chiffrierte Nachricht an einen Teilnehmer B mit öffentlichem Schlüssel (n, c) zu senden:

  1. Zerlege die Nachricht so in Blöcke, dass jeder Block durch eine Zahl $m < n$ dargestellt werden kann (z.B. ASCII codes).
  2. Berechne für jeden Block das Element $x = m^c$ in der Gruppe $\mathbb{Z}_n^*$. Die Chiffrierung des Blocks ist die Zahl x.
  3. Schicke die Chiffrierungen $x_1, x_2, x_3 \ldots$ der Blöcke an B.

- Das RSA Kryptosystem – Entschlüsseln:

  Um eine chiffrierte Nachricht, die an einen Teilnehmer B mit öffentlichem Schlüssel (n, c) und privatem Schlüssel d geschickt wurde, zu entschlüsseln:

  1. Berechne die Elemente x^d von $\mathbb{Z}_n^*$ für $x = x_1, x_2, x_3, \ldots.$
  2. Diese Zahlen sind garantiert die Darstellungen m der Blöcke. Gewinne aus ihnen die Nachricht zurück.

- Das RSA-Kryptosystem:
  Beispiel (aus Wikipedia):
  - $p = 61,\ q = 53;$
  - $n = 61 \cdot 53 = 3233;$
  - $\phi = 60 \cdot 52 = 3120.$
  - Wähle $c = 17,\ d = 2753.$
    - Es gilt $cd = 46801 = 1 + 15 \cdot 3120 = 1 + k\,\phi.$
  - Öffentlicher Schlüssel: $(3233, 17).$
  - Privater Schlüssel: $2753.$

- Das RSA-Kryptosystem:
  Beispiel (aus Wikipedia):
  - Sei $m = 123$.
  - $x = 12317 \bmod 3233 = 55$.
  - $m = 8552753 \bmod 3233 = 123$.

- Das RSA-Kryptosystem: Warum funktioniert es?

  Lemma (Euler). Seien p und q Primzahlen, $n = pq$ und $\phi = (p-1)(q-1)$.

  Für alle $m \in \mathbb{Z}_n^*$ gilt: $m^{\phi} \equiv 1 \bmod n$.

  Beweis: Die Gruppe $\langle \mathbb{Z}_n^*, *_n \rangle$ hat ϕ Elemente. Es folgt: $\mathrm{ord}(m)$ teilt ϕ (Lagrange) und daher gibt es k mit

$$m^{\phi} = m^{k\,\mathrm{ord}(m)} = \left(m^{\mathrm{ord}(m)}\right)^k \equiv 1 \bmod n.$$

- Das RSA Kryptosystem: Warum funktioniert es?
  - Wir haben $x^d = (m^c)^d = m^{cd}$.
  - Wegen $cd \equiv 1 \bmod \phi$ gibt es k mit
    $$cd = 1 + k\phi.$$
  - Es folgt $m^{cd} = m^{1+k\phi} = m(m^\phi)^k$ und mit dem Lemma von Euler ergibt sich
    $$x^d = m^{cd} = m(m^\phi)^k \equiv m \bmod n.$$
    (Bemerkung: Der Satz von Euler beweist Korrektheit von RSA nur für $m \in \mathbb{Z}_n^*$. Ein anderes, ähnliches Argument zeigt sie auch für $m \equiv 0 \bmod p$ und $m \equiv 0 \bmod q$.)

- Das RSA Kryptosystem: Ist es sicher?
  - Keine Garantie!
  - Bisher kein effizientes Verfahren bekannt, welches aus dem öffentlichen Schlüssel (n, c) den privaten Schlüssel d berechnet.
  - Wenn man p und q kennt, dann kann d effizient berechnet werden. Für die Faktorisierung der Zahl n ist jedoch kein effizientes Verfahren bekannt. (Es existiert jedoch ein polynomielles Verfahren für hypothetische Quantenrechner.)