Einführung in die Kryptologie

Johannes Köbler

Institut für Informatik
Humboldt-Universität zu Berlin

SS 2022

Asymmetrische Kryptosysteme

- Diffie und Hellman hatten 1976 die Idee, dass ein Kryptosystem selbst dann sicher sein könnte, wenn der Chiffrierschlüssel k veröffentlich wird
- Natürlich darf dann der Dechiffrierschlüssel k' nicht mit vertretbarem Aufwand aus dem Chiffrierschlüssel k berechenbar sein
- Jeder Teilnehmer X kann dann ein Schlüsselpaar k_X, k'_X erzeugen und den Chiffrierschlüssel k_X veröffentlichen, während k'_X geheim bleibt
- Dies hat den großen Vorteil, dass für die Übertragung des Schlüssels k_X nur ein authentisierter (und kein sicherer) Kanal benötigt wird
- Es reicht nämlich aus, dass sich der Empfänger von der Herkunft und Originalität des Schlüssels k_X überzeugen kann
- Ein Kryptosystem heißt symmetrisch, wenn die Kenntnis des Chiffrierschlüssels gleichbedeutend mit der Kenntnis des Dechiffrierschlüssels ist, der eine also leicht aus dem anderen berechnet werden kann
- Bei einem asymmetrischen Kryptosystem darf dagegen der Chiffrierschlüssel veröffentlicht werden, da sich der Kryptotext damit nicht entschlüsseln lässt

Asymmetrische Kryptosysteme

- Symmetrische Kryptosysteme werden auch als konventionell oder als Secret-Key-Kryptosysteme bezeichnet, während man bei asymmetrischen Kryptosystemen auch von Public-Key-Kryptosystemen spricht
- Wie der Name schon sagt, sind bei einem symmetrischen Kryptosystem die Rollen von Sender und Empfänger austauschbar, da sie ein gemeinsames Geheimnis in Form des symmetrischen Schlüssels teilen
- Der Unterschied lässt sich durch folgende Analogie verdeutlichen, in der Geheiminformationen mithilfe eines Bankschließfachs übergeben werden:
  - Symmetrische Verschlüsselung: Alice und Bob sind im Besitz eines Schlüssels k für das Schließfach, welches sich mit k sowohl auf- als auch zuschließen lässt. Alice schließt die Nachricht in den Tresor ein und Bob öffnet danach das Schließfach, um die Nachricht zu lesen
  - Asymmetrische Verschlüsselung: Am Schließfach befindet sich ein Zahlenschloß, dessen Zahlenkombination k'_B nur Bob bekannt ist. Alice kennt nur die Schließfachnummer k_B, legt ihre Nachricht hinein und verdreht anschließend das Schloß. Bob kann das Schließfach mit seinem „privaten“ Schlüssel k'_B öffnen und die Nachricht entnehmen

Asymmetrische Kryptosysteme

- An dieser Analogie wird auch deutlich, warum der öffentliche Schlüssel k_B über einen authentisierten Kanal an Alice übergeben werden muss
- Andernfalls könnte sich nämlich ein Angreifer als Bob ausgeben und Alice seinen eigenen Schlüssel zusenden
- Anschließend könnte er die für Bob bestimmte Nachricht lesen (und ggf. mit k_B verschlüsselt an Bob weiterleiten) ohne dass dies bemerkt wird
- Da Alice nicht im Besitz von Bobs privatem Schlüssel k'_B ist, kann sie keine mit k_B verschlüsselten Nachrichten lesen; insbesondere auch keine, die Bob von anderen Teilnehmern erhält
- Dies hat den Vorteil, dass für jeden Teilnehmer nur ein asymmetrisches Schlüsselpaar generiert werden muss, während für die Kommunikation zwischen n Teilnehmern bis zu $\binom{n}{2}$ symmetrische Schlüssel nötig wären
- Zu beachten ist auch, dass mit Bobs Schlüsselpaar (k_B, k'_B) nur eine Nachrichtenübermittlung von Alice (oder anderen Teilnehmern) an Bob möglich ist, und für die Übermittlung von Nachrichten an Alice das Schlüsselpaar (k_A, k'_A) von Alice benutzt werden muss

Asymmetrische Kryptosysteme

- Dass bei der Verschlüsselung kein geheimer Schlüssel benutzt wird, hat andererseits den Nachteil, dass ein asymmetrisches Kryptosystem nicht absolut sicher sein kann (siehe Übungen)
- Da der Chiffrierschlüssel k_B öffentlich bekannt ist, kann ein Gegner bei bekanntem Kryptotext nämlich alle Klartexte ausprobieren
- Damit das System dennoch sicher ist, muss E_{k_B} eine Einwegfunktion (engl. one-way function) sein, d.h. E_{k_B} darf ohne Kenntnis des privaten Schlüssels k'_B nicht effizient umkehrbar sein
- Da dies bei Kenntnis von k'_B möglich ist, spricht man von einer Falltürfunktion (engl. trapdoor one-way function)
- Da E_{k_B} zudem bijektiv ist, handelt es sich genauer um eine Falltürpermutation (engl. trapdoor one-way permutation)
- In den Übungen wird gezeigt, dass mit deterministischen Public-Key-Verfahren keine komplexitätstheoretische Sicherheit erreichbar ist
- Hierzu muss der Verzicht auf die Geheimhaltung von k_B durch Verwendung von Zufall bei der Berechnung von E_{k_B} kompensiert werden

Das RSA-System

- Das RSA-Kryptosystem wurde 1978 von Rivest, Shamir und Adleman veröffentlicht
- Während es beim Primzahlproblem nur um die Frage „Ist n prim?“ geht, muss beim Faktorisierungsproblem im Falle einer zusammengesetzten Zahl mindestens ein nicht-trivialer Faktor berechnet werden
- Genauer gesagt beruht das RSA-Verfahren darauf, dass die Primzahleigenschaft zwar effizient getestet werden kann, aber keine effizienten Faktorisierungsalgorithmen bekannt sind

Schlüsselgenerierung

Für jeden Teilnehmer X werden zwei Primzahlen p, q und zwei Exponenten e, d mit $ed \equiv_{\varphi(n)} 1$ generiert, wobei $n = pq$ und $\varphi(n) = (p-1)(q-1)$ ist

- öffentlicher Schlüssel: $k_X = (e, n)$
- privater Schlüssel: $k'_X = (d, n)$

Ver- und Entschlüsselung

- Jede Nachricht x besteht aus einer Folge $x_1, x_2, \ldots$ von Zahlen $x_i \in \mathbb{Z}_n$, die einzeln wie folgt ver- und entschlüsselt werden:
  - $\mathrm{RSA}((e,n),x) = x^e \bmod n$
  - $\mathrm{RSA}^{-1}((d,n),y) = y^d \bmod n$
- Der Schlüsselraum ist also

  $$K = \{(c,n) \mid \text{es gibt Primzahlen } p \text{ und } q \text{ mit } n = pq \text{ und } c \in \mathbb{Z}^*_{\varphi(n)}\}$$

  und

  $$S = \{((e,n),(d,n)) \in K \times K \mid ed \equiv_{\varphi(n)} 1\}$$

  ist die Menge aller zueinander passenden Schlüsselpaare
- Die Chiffrierfunktionen $\mathrm{RSA}_{(e,n)}$ und $\mathrm{RSA}^{-1}_{(d,n)}$ sind durch Wiederholtes Quadrieren und Multiplizieren effizient berechenbar

Der folgende Satz garantiert die Korrektheit des RSA-Systems

Satz

Für jedes Schlüsselpaar $((e,n),(d,n)) \in S$ und alle $x \in \mathbb{Z}_n$ gilt

$$x^{ed} \equiv_n x$$

Beweis.

- Sei $n = pq$ und sei z eine natürliche Zahl mit $ed = z\varphi(n) + 1$
- Wir zeigen $x^{ed} \equiv_p x$ (die Kongruenz $x^{ed} \equiv_q x$ folgt analog und beide Kongruenzen zusammen implizieren $x^{ed} \equiv_n x$)
- Wegen $\varphi(n) = (p-1)(q-1)$ und wegen $x^{p-1} \equiv_p 1$ für $x \not\equiv_p 0$ folgt

$$x^{ed} = x^{z\varphi(n)+1} = x^{z(p-1)(q-1)}x = (x^{p-1})^{z(q-1)}x \equiv_p x$$

□