

Betriebssysteme und Sicherheit, WS 2014/15

4. Aufgabenblatt – Kryptographie

Geplante Bearbeitungszeit: eine Woche

Aufgabe 4.1

- (a) Welches sind die 3 Haupt-Schutzziele in der Datensicherheit?
- (b) Welche Aufgaben haben kryptographische Systeme?
- (c) Wie funktionieren solche Systeme prinzipiell? Was versteht man unter symmetrischen, asymmetrischen und hybriden kryptographischen Systemen?

Aufgabe 4.2

Der RSA-Algorithmus (Algorithmus von RIVEST/SHAMIR/ADLEMAN, 1977) hat folgende Struktur:

- (I) Wähle zufällig zwei Primzahlen $p \neq q$, annähernd gleiche Stellenzahl.
- (II) Bilde $n = pq$. In diesem Fall gilt für die EULERSche Funktion φ : $\varphi(n) = (p - 1) \cdot (q - 1)$.
- (III) Wähle c mit $2 \leq c < \varphi(n)$, so dass $\text{ggT}(c, \varphi(n)) = 1$.
- (IV) Berechne d mit $cd \equiv 1 \pmod{\varphi(n)}$ und $1 < d < \varphi(n)$.
- (V) Verteile den Modul n sowie c als öffentlichen Schlüssel und d als privaten Schlüssel.

Eine Nachricht $x < n$ wird durch $x^c \equiv y \pmod{n}$ mit $0 \leq y < n$ verschlüsselt und entschlüsselt durch $y^d \equiv x \pmod{n}$.

- (a) Worin liegt das Sicherheitsrisiko dieses Algorithmus?
- (b) Begründen Sie die einzelnen Restriktionen in (I) und (III). Welche Aussage macht die EULERSche Funktion? Welche Bedeutung hat Schritt (IV) für das Vorgehen?
- (c) Demonstrieren Sie den RSA-Algorithmus an dem folgendem Beispiel:

Der Modul sei $n = 55$, der öffentliche Schlüssel sei $c = 7$. Verschlüsseln Sie damit die Nachricht $x = 2$. Berechnen Sie den privaten Schlüssel d , entschlüsseln Sie die verschlüsselte Nachricht und zeigen Sie deren Übereinstimmung mit x .

Hinweise:

- Benutzen Sie zur Berechnung des ggT zweier Zahlen a, b mit (o.B.d.A.) $a > b$ sowie der Summendarstellung nach dem Erweiterten EUKLIDischen Algorithmus eine Tabelle folgender Form:

	a	b		$y_i = -(x_{i-1} \text{ div } x_i)$
a	1	0	mit	$x_{i+1} = x_{i-1} \text{ mod } x_i$
b	0	1		$s_{i+1} = s_i \cdot y_i + s_{i-1}$
x_i	s_i	t_i		$t_{i+1} = t_i \cdot y_i + t_{i-1}$

div bezeichnet die ganzzahlige Division, mod den dabei auftretenden Rest.

In obiger Tabelle beginnt i mit 0, die Formeln gelten ab $i = 1$ (zuerst ist also y_1 in der „ b -Zeile“ zu berechnen). Der Algorithmus bricht ab bei $x_i = 0$, und dann gilt: $x_{i-1} = \text{ggT}(a, b) = s_{i-1}a + t_{i-1}b$.

Die letzte Gleichung gilt auch in jeder Zeile, was zur Rechenkontrolle genutzt werden sollte.

- Zerlegen Sie zum Entschlüsseln die verschlüsselte Nachricht y in Primfaktoren und versuchen Sie dann, in y^d geeignete Potenzen abzuspalten, deren Produkt modulo 55 gleich 1 oder -1 ist.

Aufgabe 4.3

Um die Faktoren p, q eines RSA-Schlüsselpaares zu generieren werden in der Praxis Zufallszahlen benutzt.

- (a) Wie kann man auf einem Computer Zufall (Entropie) erzeugen?
- (b) Einige Endgeräte verwenden schlechte Entropiequellen. Was kann passieren, wenn eine große Anzahl solcher Systeme RSA-Schlüssel generiert?
- (c) Die öffentlichen Schlüssel von Alice und Bob haben folgende Moduln: $n_a = 73684837$ und $n_b = 63546229$. Überprüfen Sie, ob beide Moduln sich einen Faktor teilen! Faktorisieren Sie n_a und n_b !