TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik Institut für Systemarchitektur, Professur für Betriebssysteme

Betriebssysteme und Sicherheit, WS 2017/18

5. Aufgabenblatt – Kryptographie

Geplante Bearbeitungszeit: eine Woche

Aufgabe 5.1

(a) Welches sind die drei Haupt-Schutzziele in der Datensicherheit?

(b) Welche Aufgaben haben kryptographische Systeme?

(c) Nach welchem Grundprinzip arbeiten solche Systeme? Was versteht man unter symmetrischen, asymmetrischen und hybriden kryptographischen Systemen?

Aufgabe 5.2 Der RSA-Algorithmus (Algorithmus von RIVEST/SHAMIR/ADLEMAN, 1977) hat folgende Struktur:

(I) Wähle zufällig zwei Primzahlen $p \neq q$ mit annähernd gleicher Stellenzahl.

(II) Bilde $n = p \cdot q$. In diesem Fall gilt für die EULERsche Funktion φ: $\varphi(n) = (p-1) \cdot (q-1)$.

(III) Wähle c mit $2 < c < \varphi(n)$, so dass $\text{ggT}\left(c, \varphi(n)\right) = 1$.

(IV) Berechne d mit $c \cdot d \equiv 1 \bmod \varphi(n)$ und $1 < d < \varphi(n)$.

(V) Verteile den Modul n sowie c als öffentlichen Schlüssel und nutze d als privaten Schlüssel.

Eine Nachricht x wird durch $x^c \equiv y \bmod n$ verschlüsselt und entschlüsselt durch $y^d \equiv x \bmod n$, wobei $0 \leq x, y < n$.

(a) Auf welcher Annahme basiert die Sicherheit dieses Algorithmus?

(b) Begründen Sie die einzelnen Restriktionen in (I) und (III). Welche Aussage trifft die EULERsche Funktion? Welche Bedeutung hat Schritt (IV) für das Vorgehen?

(c) Demonstrieren Sie den RSA-Algorithmus an 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 und b mit (o.B.d.A.) $a > b$ sowie der Summendarstellung nach dem Erweiterten EUKLIDischen Algorithmus eine Tabelle folgender Form:

	a	b	
a	1	0	
b	0	1	
x_i	s_i	t_i	y_i

mit

$$y_i = -\left(x_{i-1} \operatorname{div} x_i\right)$$
$$x_{i+1} = x_{i-1} \bmod x_i$$
$$s_{i+1} = s_i \cdot y_i + s_{i-1}$$
$$t_{i+1} = t_i \cdot y_i + t_{i-1}$$

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: $x_{i-1} = \text{ggT}(a,b) = s_{i-1} \cdot a + t_{i-1} \cdot b$.

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

- Benutzen Sie zur Entschlüsselung der Nachricht binäre Exponentiation, auch bekannt als „Square and Multiply". Zur einfachen Notation bietet sich dabei das folgende Schema zur Berechnung von a^b an:

b	a
x_i	y_i

mit

$$x_{i+1} = \lfloor x_i \div 2 \rfloor \quad x_0 = b$$
$$y_{i+1} = y_i^2 \quad y_0 = a$$

Der Algorithmus bricht ab bei $x_i = 1$. Abschließend werden alle diejenigen y_i zum Endergebnis aufmultipliziert, deren zugehöriges x_i ungerade ist.

Aufgabe 5.3 Um die Faktoren p,q eines RSA-Schlüsselpaars 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: $n_a = 73.684.837$ und $n_b = 63.546.229$. Überprüfen Sie, ob beide Moduln sich einen Faktor teilen! Faktorisieren Sie n_a und n_b!