

21. November 2007

## 11. Übungsblatt Kryptologie

### Aufgabe 1: (5 Punkte)

Bei der Erzeugung einer elektronischen Unterschrift nach DSA muß für jede zu unterschreibende Nachricht eine Zufallszahl  $k$  gewählt werden. Welche der folgenden Strategien zur Wahl von  $k$  sind sicher, und welche Attacken gibt es gegen die anderen? Dabei sei jeweils  $k_0$  eine ein für allemal fest gewählte Zufallszahl und  $\Delta$  sei das Datum in der Form Tag:Monat:Jahr:Stunde:Minute, aufgefaßt als zehnstellige Zahl (also z.B. 2711071200 für das Abgabedatum dieses Übungsblatts):

- |  |                                      |
|--|--------------------------------------|
| 1.) $k = k_0 + 3i$ für die $i$ -te Nachricht               | 2.) $k = k_0 + \Delta$               |
| 3.) $k = \text{SHA-1}(k_0 + 3i)$ für die $i$ -te Nachricht | 4.) $k = \text{SHA-1}(k_0 + \Delta)$ |
| 5.) $k = \text{SHA-1}(\text{vorigem } k)$                  | 6.) $k = \text{SHA-1}(\Delta)$       |

### Aufgabe 2: (5 Punkte)

- a) Sie wählen bei DSA mit 160-Bit-Unterschriften die Werte von  $k$  jeweils zufällig. Nach wie vielen Unterschriften ist die Wahrscheinlichkeit, daß Sie zweimal denselben Schlüssel gewählt haben, in der Größenordnung der Wahrscheinlichkeit für sechs Richtige im Lotto?
- b) Nach wie vielen Unterschriften entspricht sie der Wahrscheinlichkeit für sechs Richtige im Lotto in zwei aufeinanderfolgenden Wochen?

### Aufgabe 3: (5 Punkte)

Beim Münzwurf per Telephon wählt A die beiden Primzahlen  $p = 44483$  und  $q = 77783$ , schickt deren Produkt  $N = 3460021189$  an B und erhält von diesem die Zahl  $y = 1831904234$ , die B als Quadrat modulo  $N$  von  $x = 12345678$  konstruiert hat. Welche Zahlen kann A nun an B schicken, und bei welchen Wahlen hat er gewonnen?

### Aufgabe 4: (5 Punkte)

Auch die Prüfziffern des Europäischen Artikelnummernsystems EAN sowie der Internationalen Standardbuchnummern ISBN können als eine Art Hashwert angesehen werden. Dieser soll allerdings nicht vor absichtlichen Verfälschungen schützen, sondern vor zufälligen. Die häufigsten davon sind in der folgenden Tabelle zusammengefaßt:

Falsche Ziffer	$2 \rightarrow 3$	79,1%
Vertauschung benachbarter Ziffern	$45 \rightarrow 54$	10,2%
Vertauschung nichtbenachbarter Ziffern	$273 \rightarrow 372$	0,8%
Benachbarte gleiche Ziffern beide falsch	$66 \rightarrow 99$	0,5%
Verwechslung von -zehn und -zig	$14 \rightarrow 40$	0,5%
Nichtbenachbarte gleiche Ziffern beide falsch	$636 \rightarrow 939$	0,3%

Eine EAN besteht aus 13 Ziffern  $a_1, \dots, a_{13}$ , wobei  $a_{13}$  so gewählt wird, daß

$$a_1 + a_3 + a_5 + a_7 + a_9 + a_{11} + a_{13} + 3(a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12}) \equiv 0 \pmod{10}$$

ist; eine ISBN besteht aus zehn Ziffern  $a_1, \dots, a_{10}$  mit

$$10a_1 + 9a_2 + 8a_3 + 7a_4 + 6a_5 + 5a_6 + 4a_7 + 3a_8 + 2a_9 + a_{10} \equiv 0 \pmod{11}.$$

- a) Gegen welche Arten zufälliger Fehler schützen diese Systeme?
- b) Ersetzen Sie in der ISBN 3-406-42918-1 die Verlagsnummer 406 durch eine andere dreistellige Zahl derart, daß wieder eine korrekte ISBN entsteht!

Abgabe bis zum Dienstag, dem 27. November 2007, um 12.00 Uhr