Wolfgang K. Seiler
Tel. 2515

A5, C201

10. Mai 2013

11. Übungsblatt Kryptologie

Aufgabe 1: *(6 Punkte)*

Wir betrachten einen Mini-SHA, der nicht mit Wörtern der Länge 32 oder 64 arbeitet, sondern mit solchen der Länge acht. Berechnen Sie für die (hexadezimal dargestellten) Wörter $x = AB, y = C2$ und $z = 17$ die Ergebnisse der folgenden SHA-Operationen:

a) $ROTR^3(x)$ und $SHR^3(x)$

b) $x \oplus y$ und $x + y$

c) $Maj(x, y, z)$

d) $Ch(x, y, z)$

Aufgabe 2: *(9 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 Δ sei das Datum in der Form Tag:Monat:Jahr:Stunde:Minute, aufgefaßt als zehnstellige Zahl (also z.B. 1705131155 für das Abgabedatum dieses Übungsblatts):

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

Mit SHA ist hier jeweils einer der beiden Algorithmen SHA-256 oder SHA-512/256 gemeint.

Aufgabe 3: *(5 Punkte)*

a) Sie wählen bei DSA mit 256-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?

Abgabe bis zum Freitag, dem 17. Mai 2013, um 11.55 Uhr