WOLFGANG K. SEILER
Tel. 2515

A5, C201

9. Februar 2005

14. Übungsblatt Kryptologie

Aufgabe 1: (*7 Punkte*)

a) Der teuerste Schritt bei der Erzeugung einer elektronischen Unterschrift nach DSA besteht in der Berechnung von $r = (a^k \bmod p) \bmod q$. Da dieser Teil der Unterschrift nicht von der zu unterschreibenden Nachricht abhängt, bietet sich an, jedes Mal dasselbe k und damit auch dasselbe r zu verwenden. Zeigen Sie durch eine „differentielle Kryptanalyse", daß auch diese Sparmaßnahme wie so viele andere in der Kryptographie katastrophale Folgen hat!

b) Was ändert sich, wenn man als privaten Schlüssel s statt einer Zahl $x < q$ eine beliebige Zahl zwischen 1 und $p - 1$ wählt?

c) 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. 0902051200 für dieses Übungsblatt):

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.) $k = \text{SHA-1}(\textit{vorigem}\ k)$
6.) $k = \text{SHA-1}(\Delta)$

Aufgabe 2: (*4 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: (*6 Punkte*)

a) p, q seien Primzahlen und $p \equiv 1 \bmod q$. Wie groß ist die Wahrscheinlichkeit dafür, daß für eine zufällig gewählte Zahl a zwischen 1 und $p-1$ das Element $a^{(p-1)/q}$ keine Untergruppe der Ordnung q erzeugt?

b) Auf dem Maple *worksheet* blatt14.mws finden Sie eine 192-Bit-Primzahl q sowie eine 2048-Bit-Primzahl $p \equiv 1 \bmod q$. Finden Sie ein Element $a \in \mathbb{F}_p^\times$ der Ordnung q !

c) Erzeugen Sie bezüglich des gewählten a eine DSA-Unterschrift unter die Nachricht 2^{128} zum privaten Schlüssel $x = 2^{190} + 2^{150} + 2^{110} + 2^{70} + 2^{30} + 1$!

d) Berechnen Sie den öffentlichen Schlüssel y zu x und überprüfen Sie damit die Unterschrift!

Aufgabe 4: (*3 Punkte*)

Schätzen Sie, um welchen Faktor der Aufwand steigt, wenn man bei der Suche nach einer Primzahl $p \equiv 1 \bmod q$ für eine gegebene Primzahl q die Bitlänge von p verdoppelt!

Abgabe bis zum Dienstag, dem 15. Februar 2005, um 12.00 Uhr