Wolfgang K. Seiler
Tel. 2515

A5, C201

8. Dezember 2004

7. Übungsblatt Kryptologie

Aufgabe 1: (*5 Punkte*)
Sie verschlüsseln eine Datei via AES im OFB-Modus mit einem Schlüssel und Anfangsblock, den Sie vorher mit Ihren Partnern vereinbart haben; danach stellen Sie die verschlüsselte Datei ins Netz. Plötzlich bemerkt Ihre Sekretärin, daß der Name des Generaldirektors falsch geschrieben ist: Dickmann statt Dickman. In der Hoffnung, daß erst wenige Partner den Text heruntergeladen haben, verbessern Sie den Fehler, kodieren das Ergebnis mit den vereinbarten Parametern und ersetzen die fehlerhafte Datei durch die neue. Welche Informationen kann ein Gegner, der sich beide Versionen verschafft hat, gewinnen, und wie geht er vor?

Aufgabe 2: (*5 Punkte*)

a) Berechnen Sie das Ergebnis der Byte-Substitution, angewandt auf das Byte `FF`!

b) Hat auch AES wie DES die Eigenschaft, daß für alle Schlüssel s und alle Blöcke x gilt

$$\mathrm{AES}(\overline{s}, \overline{x}) = \overline{\mathrm{AES}(s, x)}\,,$$

wobei $\overline{x}$ das 1-Komplement von x bezeichnet?

Aufgabe 3: (*4 Punkte*)
Leider haben Sie nur eine alte RSA-Implementierung, die nicht mit den heute wünschenswerten Modullängen zurechtkommt. Um trotzdem ein sicheres System zu bekommen, entwickeln Sie in Anlehnung an Triple-DES das folgende Triple-RSA-System: Sie wählen sich einen Modul N und zwei öffentliche Exponenten e_1, e_2; ein Block b wird dann verschlüsselt als

$$\mathrm{RSA}_{N,e_1}\Big(\mathrm{RSA}_{N,e_2}\big(\mathrm{RSA}_{N,e_1}(b)\big)\Big)\,.$$

a) Warum wird in der Mitte nicht, analog zu Triple-DES, $\mathrm{RSA}^{-1}_{N,e_2}$ verwendet?

b) Ist die Sicherheit von Triple-RSA vergleichbar mit der von einfachem RSA mit doppelter Blocklänge?

Aufgabe 4: (*6 Punkte*)

a) Zeigen Sie: $N = 2^{2n} - 1$ ist genau dann eine Primzahl, wenn $n = 1$ ist.

b) Zeigen Sie: $2^n - 1$ ist genau dann durch drei teilbar, wenn n gerade ist.

c) Die Zahl $N = \frac{1}{3}(2^{122} - 1)$ ist Produkt zweier Primzahlen. Finden Sie diese!

d) Finden Sie den kleinsten öffentlichen Exponenten e, den man in einem RSA-System mit Modul N benutzen kann!

e) Bestimmen Sie den privaten Exponenten dazu!

Abgabe bis zum Dienstag, dem 14. Dezember 2004, um 12.00 Uhr