Wolfgang K. Seiler
Tel. 2515

A5, C201

25. September 2007

3. Übungsblatt Kryptologie

Aufgabe 1: (*5 Punkte*)
Geben Sie für die Operationsmodi CBC, CFB, OFB und CTR jeweils einen konkreten Algorithmus an, wie der Empfänger aus der Folge $c_1c_2\dots c_r$ der Chiffretextblöcke die Folge $m_1m_2\dots m_r$ der Nachrichtenblöcke rekonstruiert! Über welche Informationen muß er jeweils verfügen?

Aufgabe 2: (*5 Punkte*)
Sie verschlüsseln eine Datei via Triple-DES (oder einer anderen Blockchiffre) im OFB-Modus mit einem Schlüssel und Anfangsblock, den Sie vorher mit Ihren Kollegen vereinbart haben; danach stellen Sie die verschlüsselte Datei ins Netz. Plötzlich bemerkt Ihre Sekretärin, daß der Name des Generaldirektors falsch geschrieben ist: Herrmann statt Hermann. In der Hoffnung, daß erst wenige Kollegen den Text heruntergeladen haben, verbessern Sie den Fehler, verschlüsseln das Ergebnis mit den vereinbarten Parametern und ersetzen die fehlerhafte Datei durch die neue. Welche Informationen kann ein Gegner gewinnen, der sich beide Versionen verschafft hat, und wie geht er vor?

Aufgabe 3: (*5 Punkte*)

a) Finden Sie die Umkehrabbildung zu $\varphi\colon \begin{cases} \mathbb{F}_p \to \mathbb{F}_p \\ x \mapsto x^e \end{cases}$ für die Primzahl $p = 123\,456\,791$ und den Exponenten $e = 3$!

b) Zeigen Sie, daß es für $e = 2$ keine Umkehrabbildung gibt!

c) Bestimmen Sie alle $e \leq 100$, für die φ keine Umkehrabbildung hat!

Aufgabe 4: (*5 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 **ohne** Computerhilfe!

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! *(Spätestens hierzu sollten sie definitiv einen Computer benutzen!)*

Abgabe bis zum Dienstag, dem 2. Oktober 2007, um 12.00 Uhr