Wolfgang K. Seiler
Tel. 2515

A5, C201

30. September 2010

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 $c_1 c_2 \dots c_r$ der Chiffretextblöcke die Folge $m_1 m_2 \dots m_r$ 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)*
Zeigen Sie:

a) Wenn bei DES alle sechzehn Rundenschlüssel identisch sind, ist die Entschlüsselung gleichbedeutend mit der Verschlüsselung.

b) Die ist insbesondere dann der Fall, wenn jeder der beiden anfangs aus dem Schlüssel extrahierten Teilschlüssel entweder nur aus Nullen oder nur aus Einsen besteht.

c) Finden Sie vier Schlüssel, bei denen dies der Fall ist! (*Hinweis:* Betrachten Sie die Bitpositionen, die in die beiden Teilschlüssel gehen, modulo acht!)

Aufgabe 4: *(5 Punkte)*
Um die Vigenère-Chiffre aus dem 19. ins 21. Jahrhundert zu transportieren, macht sie der Geheimdienst von Exotistan wie folgt zu einer Blockchiffre: Die Blocklänge beträgt 128 Bit, die Schlüssellänge 512 Bit. Jeder Block wird aufgeteilt in vier Teilblöcke u, v, w, x zu je 32 Bit; der Schlüssel S wird aufgeteilt in 16 Teilschlüssel $s_1, \dots, s_{16}$ von ebenfalls jeweils 32 Bit. Die Verschlüsselung eines Blocks (u_0, v_0, w_0, x_0) geschieht in sechzehn Runden. Dabei wird in der i-ten Runde im Block $(u_{i-1}, v_{i-1}, w_{i-1}, x_{i-1})$ zunächst der Rundenschlüssel s_i zu jedem der vier Teilblöcke addiert; der dabei entstehende Block sei $(u'_{i-1}, v'_{i-1}, w'_{i-1}, x'_{i-1})$. Danach werden die vier Teilblöcke

$$u''_{i-1} = u'_{i-1}, \quad v''_{i-1} = v'_{i-1} \oplus u''_{i-1}, \quad w''_{i-1} = w'_{i-1} \oplus v''_{i-1} \quad \text{und} \quad x''_{i-1} = x'_{i-1} \oplus w''_{i-1}$$

gebildet. Eine zyklische Verschiebung macht daraus das Rundenergebnis

$$(u_i, v_i, w_i, x_i) = (x''_{i-1}, u''_{i-1}, v''_{i-1}, w''_{i-1}) .$$

a) Wie kann man bei Kenntnis von S entschlüsseln?

b) Beurteilen sie die Sicherheit dieser Chiffre!

Abgabe bis zum Donnerstag, dem 7. Oktober 2010, um 15.30 Uhr