Klausur Datensicherheit

Semester:	AI7	**Sommersemester 02**,	8.7..2002
Bearbeitungszeit:	90 Minuten	Hilfsmittel:	nicht prog. Taschenrechner

Aufgabe 1 (Punkte)

Gegeben sei eine 64-Bit-Blockchiffre, die bei festem Schlüssel k die beiden Klartextvektoren

$$M_1 = 00000000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000$$
$$M_2 = 10000000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000$$

abbildet auf die Chiffretextvektoren

$$C_1 = 01101000\ 01011100\ 10110010\ 11001110\ 10010100\ 01010011\ 00010101\ 11110100$$
$$C_2 = 01100101\ 10010100\ 00110110\ 10001010\ 10011000\ 11001011\ 10110011\ 01010000$$

a) Welches Problem stellen Sie hier fest?
b) Angenommen dieses Problem tritt für viele Klartexte auf. Warum handelt es sich hier um eine unsichere Chiffre?
c) Welcher Angriff wird dadurch erleichtert?

Lösung zu Aufgabe 1

a) C_1 und C_2 unterscheiden sich nur an 22 Stellen.
b) Der Lawineneffekt funktioniert hier nicht gut genug.
c) Die differentielle Kryptanalyse.

Aufgabe 2 (Punkte)

a) Welches der heute bekannten Verfahren zur Speicherung des geheimen Schlüssels eines Public-Key-Paares bietet die höchste Sicherheit. (kurze Begründung)
b) Geben Sie den Grund an für die Einführung einer Public Key Infrastruktur.
c) Warum ist die Chipkarte im Vergleich zur EC-Karte viel sicherer? (nennen Sie einen Angriff!)

Lösung zu Aufgabe 2

a) Chipkarte, denn der geheime Schlüssel kann nicht ausgelesen werden. Entschlüsseln und Signieren erfolgen auf der Karte.
b) Man-in-the-middle-Problem beim Austausch öffentlicher Schlüssel.
c) Trojaner am Bankautomaten kann bei der EC-Karte den Magnetstreifen auslesen und die PIN speichern. Das ist bei der Chipkarte nicht möglich.

Aufgabe 3 (Punkte)

Für die Schlüsselerzeugung von RSA seien die Primzahlen $p = 3$ und $q = 11$ gegeben, sowie der öffentliche Exponent $e = 17$.

a) Zeigen Sie, dass $d = 13$ der zugehörige geheime Exponent ist.
b) Verschlüsseln Sie die Zahl 31 mit RSA.

Lösung zu Aufgabe 3

a) $\phi(n) = 2 \cdot 10 = 20, \qquad 13 \cdot 17 \mod 20 = 221 \mod 20 = 1$
b) $31^{17} \mod 33 = 4.$

Aufgabe 4 (Punkte)

a) Zeigen Sie, dass in $\mathbb{Z}_{111}$ gilt: $-34 = 77$.
b) Zeigen Sie, dass in $\mathbb{Z}_{111}$ gilt: $\frac{1}{34} = 49$.
c) Warum gibt es in $\mathbb{Z}_{111}$ zur Zahl 3 keine multiplikative Inverse (d.h. $1/3$ existiert nicht)?

Lösung zu Aufgabe 4

a) $34 + (-34) = 34 + 77 = 111 = 0$
b) $34 \cdot 49 = 1$
c) Weil $\mathrm{ggT}(3, 111) = 3$.

Aufgabe 5 (Punkte)

Berechnen Sie mit dem erweiterten Euklidischen Algorithmus $125^{-1} \mod 512$.

Lösung zu Aufgabe 5

$$\begin{aligned}
512 &= 4 \cdot 125 + 12 \\
125 &= 10 \cdot 12 + 5 \\
12 &= 2 \cdot 5 + 2 \\
5 &= 2 \cdot 2 + 1 \\
2 &= 2 \cdot 1
\end{aligned}$$

$$\begin{aligned}
1 &= 5 - 2 \cdot 2 \\
&= 5 - 2 \cdot (12 - 2 \cdot 5) = -2 \cdot 12 + 5 \cdot 5 \\
&= -2 \cdot 12 + 5 \cdot (125 - 10 \cdot 12) = 5 \cdot 125 - 52 \cdot 12 \\
&= 5 \cdot 125 - 52 \cdot (512 - 4 \cdot 125) = 213 \cdot 125 - 52 \cdot 512
\end{aligned}$$

Da $52 \cdot 512 \mod 512 = 0$ gilt also $231 \cdot 125 \mod 512 = 1$. Also ist 231 invers zu 125 modulo 512.