

IT-Sicherheit im Wintersemester 2012/2013

Übungsblatt 5

Abgabetermin: 12.12.2012 bis 14:00 Uhr

Achtung: Zur Bearbeitung einiger Übungsaufgaben ist es notwendig sich über den Vorlesungsinhalt hinaus, durch Internet- und Literaturrecherche mit dem Thema zu beschäftigen.

Die schriftlichen Lösungen aller mit **H** gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben (per Email an die Adresse uebung-itsec_AT_lrz.de oder schriftlich vor der Übung). Während des Semesters werden vier Übungsblätter korrigiert. Bei vier richtigen Lösungen erfolgt ein Bonus von zwei Drittel Notenstufen auf die Klausurnote, bei nur drei oder zwei richtigen Lösungen erhalten Sie einen Notenbonus von einer Drittel Notenstufe.

Aufgabe 11: (H) Steganographie & einfache Chiffren

Steganographie wird verwendet, um geheim zu haltende Nachrichten durch Verstecken in frei zugänglichen Texten und Medien auszutauschen.

- Auf der Vorlesungs-Webseite finden Sie im Übungsabschnitt ein Bild in das eine geheime Nachricht mit dem Werkzeug *steghide* eingebettet wurde. Laden Sie sich das Programm *steghide* aus dem Internet herunter und extrahieren Sie damit die entsprechende Nachricht. Das hierzu notwendige Passwort ist der entschlüsselte Plaintext (ohne Leerzeichen, nur Grossbuchstaben) in Teilaufgabe b).
- Ein sehr altes kryptographisches Verfahren ist *Skytale*, welches auch als Spaltentransformation bezeichnet wird. Der Geheimtext nach Anwendung der Transposition lautet FNABAIHUESNAFNSDUGKEESAL. Entschlüsseln Sie diesen und verwenden Sie hierbei eine Skytale mit einem Umfang $U=5$.
- Neben additiven Chiffren (Caesar-Chiffre) existieren auch multiplikative Chiffren. Hierbei wird einem Buchstaben erst eine Zahl zugeordnet und anschließend mit einem Schlüsselwert k multipliziert. Das Ergebnis gibt die entsprechende Position im Alphabet (A-Z) an. Verwenden Sie den Wert $k = 2$. Der Buchstabe O soll dabei auf den Buchstaben D abgebildet werden. Geben Sie die Berechnungsvorschrift an und berechnen Sie die passenden Werte für alle Buchstaben.
- Was fällt Ihnen bei der in Teilaufgabe c) berechneten Substitution auf?
- Wie müssten Sie den Wert k wählen, damit der in Teilaufgabe d) genannte Effekt nicht auftritt?

Aufgabe 12: (H) Advanced Encryption Standard (AES)

Leiten Sie den Wert für das 1. Byte (1. Zeile, 1. Spalte) der Ausgabe des Rijndael-Algorithmus (Block-/Schlüsselgröße 128 Bit) am Ende der 1. Runde für die nachfolgenden Werte her. Beachten Sie, dass die Multiplikationen in $GF(2^8)$ durchzuführen sind. Das zugehörige, irreduzible Polynom lautet $x^8 + x^4 + x^3 + x + 1$. **Benennen Sie die jeweilige Phase des AES-Algorithmus**, berechnen Sie die Werte und geben Sie die **alle** relevanten Zwischenergebnissen an, damit Ihr Rechenweg nachvollziehbar ist!

$$\text{Klartext: } \begin{pmatrix} 17 & 21 & 03 & 06 \\ 08 & 43 & 24 & 16 \\ 33 & 12 & 41 & 23 \\ 51 & 37 & 11 & 35 \end{pmatrix} \quad \text{Schlüssel: } \begin{pmatrix} 11 & 22 & 33 & 44 \\ 2A & 33 & 44 & 11 \\ 32 & 44 & 11 & 22 \\ 44 & 11 & 22 & 33 \end{pmatrix}$$

$$\text{Spaltenmixmatrix: } \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$$

S-BOX:

	0	1	2	3	4	5	6	7	8
0	0x00	0x10	0x20	0x01	0x18	0x19	0xB4	0x45	0x2C
1	0x01	0x25	0xE1	0xCB	0x10	0x13	0xA7	0x3B	0x1A
2	0x2D	0xA1	0x40	0x89	0x9D	0x34	0x12	0x5E	0x2D
3	0x38	0x40	0x2C	0x29	0x02	0x27	0xF1	0x01	0x89
4	0x43	0xF2	0x20	0x30	0x40	0x02	0xD8	0x7B	0x6A
5	0xC4	0xA1	0x28	0x34	0xA2	0x09	0x7F	0x4D	0xC2
6	0x32	0x27	0x98	0x45	0x51	0x02	0xE4	0x89	0x2E
7	0xA6	0x2A	0x16	0x46	0x18	0x27	0xB3	0x1D	0xC8

In der ersten Key Expansion wurde folgender erster Rundenschlüssel berechnet:

$$\text{1. Rundenschlüssel: } \begin{pmatrix} 1A & 5A & EE & 18 \\ B7 & 87 & 26 & B4 \\ 41 & 51 & 43 & 45 \\ 19 & 39 & CA & 18 \end{pmatrix}$$