Institut für Betriebssysteme und Rechnerverbund

Übungen zur Vorlesung "Sicherheit in Netzen und Verteilten Systemen"

M. Gutbrod, S. Schmidt
<gutbrod|schmidt@ibr.cs.tu-bs.de>

Übung 8 WS 02/03 9. Januar 2003

Die Übungsblätter sowie aktuelle Informationen zu den Übungsterminen finden Sie stets auf der Web-Seite der Vorlesung unter `http://www.ibr.cs.tu-bs.de/lehre/ws0203/sec/`. Die Übungsblätter sind in der Regel eine Woche vor den Übungsterminen erhältlich.

ACHTUNG: Zur Beantwortung einiger Fragen auf diesem Aufgabenblatt ist es evtl. notwendig sich im Internet etc. über den Sachverhalt zu informieren!

Aufgabe 8.1: Bitweise XOR Verschlüsselung

Welches Problem tritt bei bitweiser Verschlüsselung, die lediglich eine XOR-Verknüpfung des Schlüssels mit dem Klartext vornimmt, auf, wenn einem Kryptanalytiker die gleiche Nachricht im Klartext und im Geheimtext vorliegt?

Aufgabe 8.2: Authentifizierung mittels symmetrischer Schlüssel

a) Alice und Bob wollen über ein unsicheres Medium kommunizieren. Dazu haben sie bei einem Treffen den symmetrischen Schlüssel K_{AB} ausgetauscht. Erstellen Sie auf dieser Basis ein Protokoll, das den beiden erlaubt sich im Netz zu authentifizieren! Wie schätzen Sie die Sicherheit Ihrer Lösung ein?

b) Wie sieht das Szenario aus, wenn Alice und Bob keinen symmetrischen Schlüssel ausgetauscht haben aber ein Schlüsselserver existiert, mit dem beide jeweils einen geheimen symmetrischen Schlüssel (K_{AS} und K_{BS}) teilen?

c) Welches Problem ergibt sich bei der Authentifizierung über symmetrische Schlüssel?

Aufgabe 8.3: Steganographie

a) In welchen Situationen würden Sie Kryptographie, Steganographie oder beides verwenden?

b) Laden Sie sich die beiden Bilder kirschblueten.bmp und kirschblueten_geheim.bmp von der Webseite herunter. Sehen Sie irgendwelche Unterschiede in dem Bildern oder der Größe der Dateien?

   Benutzen Sie sich nun S-Tools 4.0[1] um die versteckte Datei in kirschblueten_geheim.bmp zu extrahieren. Das Passwort lautet "sec". Was war in der Datei versteckt?

c) Wie funktioniert Steganographie auf Bitebene und warum eignen sich besonders Bilder und Audiodaten für Steganographie?

Aufgabe 8.4: Feistel-Netzwerk

Eine heute zentrale Komponente gängiger Kryptoverfahren ist das Anfang der 70er Jahre bei IBM entstandene Feistel-Netzwerk.

[1] Freeware für Windows – http://www.webattack.com/download/dlstools.shtml

a) Welche einfachen Prinzipien liegen dem Verfahren zugrunde?

b) Welche Verschlüsselungsverfahren basieren auf Feistel?

c) Wieviele Runden werden mindestens zur vollständigen Verschlüsselung benötigt?

d) Chiffrieren Sie die Zahl 2899 mittels des Feistel-Netzwerks und der Verschlüsselungsfunktion $f_{(x)} = (x-1)k$; $k = 1$.

e) Machen Sie die die Probe indem Sie den Wert wieder entschlüsseln.