Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikationssysteme und Systemprogrammierung
Prof. Dr. Helmut Reiser

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2021/2022
Übungsblatt 7

Besprechung: Di, 14.12.2021

Achtung: Zur Bearbeitung einiger Ãbungsaufgaben ist es notwendig sich Ã¼ber den Vorlesungsinhalt hinaus, durch Internet- und Literaturrecherche mit dem Thema zu beschÃ¤ftigen.

Aufgabe 28: (T) Einfache Chiffriermethoden & One Time Pads

Eines der zentralen Themen in der Informationssicherheit ist die Kryptographie. Neben den bekannten symmetrischen und asymmetrischen Verfahren gibt es zahlreiche, auch sehr einfache und dennoch effektive Methoden, die Vertraulichkeit von Informationen sicher zu stellen.

a. 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.

b. 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 fälllt Ihnen bei dieser Substitution auf? Wie sollten Sie den Parameter k wählen, damit der beobachtete Effekt nicht auftritt?

c. One-Time-Pad gilt derzeit als eine der sichersten Verschlüsselungsmethoden. Geben Sie das Chiffrat, d.h. nach Anwendung des One-Time-Pads MISTGABEL für die Eingabe HALLOWELT an.

Aufgabe 29: (H) Grundlagen Kryptographische Systeme & DES

a. Wie definiert man allgemein ein kryptographisches System bzw. Kryptosystem? Welche Unterschiede bestehen hierbei zwischen einem symmetrischen und einem asymmetrischen Verfahren?

b. Erklären Sie die Begriffe bzw. Verfahren *Substitution* und *Permutation*? Welche der beiden Verahren setzt z.B. der bekannte symmetrische Verschlüsselungsalgorithmus DES ein? Falls Permutationen verwendet werden, würden Sie sagen, dass sich dadurch die Stärke des DES-Verfahrens erhöht?

c. In der Vorlesung wurde der Ablauf der Algorithmen DES als auch 3DES erläutert, wobei bei 3DES grundsätzliche eine Hintereinanderausführung von Verschlüsselungs- und Entschlüsselungsschritten erfolgt. Für die dabei verwendeten Schlüssel gibt es mehrere Möglichkeiten, die auch als *Keying options* bezeichnet werden. Nennen und erläutern Sie diese kurz.

d. Nennen und erläutern Sie noch je zwei Vor- bzw. Nachteile, die das DES-Verschlüsselungsverfahren aufweist.

Aufgabe 30: (H) Steganographie

a. Betten Sie die Nachricht "*Dies ist eine versteckte Botschaft*" in die Bilder `rot.jpg`, `bunt.jpg` und `kariert.jpg`, welche Sie auf der Webseite herunterladen können ein. Verwenden Sie hierzu das Werkzeug *steghide*.

b. Extrahieren Sie die versteckten Nachrichten wieder aus den Bildern.

c. Vergleichen Sie die Histogramme der Bilder mit und ohne versteckter Nachricht. Was fällt auf?

d. Welche Techniken existieren, um Nachrichten in Bildern zu verstecken?

e. Wie robust sind die eingebetteten Nachrichten gegenüber nachträglichen Veränderungen am Bild?