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 2019/2020
Übungsblatt 7

Abgabetermin: 17.12.2019 um 12:00 Uhr

Aufgabe 14: (K) 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 15: (K) 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. Erläutern Sie kurz den Ablauf von DES. Geben Sie hier die wichtigen Phasen an, gehen Sie insbesondere auf die Funktion f ein.

d. 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.

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