Hochschule Darmstadt
Department of Computer Science
Bachelor of Computer Science
Christian Rathgeb, Ulrich Scherhag, Jannis Priesnitz

SS 2020
11. Mai 2020

IT-Sicherheit, Praktikum 2

Aufgabe 1 (Verschlüsselungsverfahren)

(a) Mit Hilfe eines Brute-Force Angriffs soll ein symmetrisches Verschlüsselungsverfahren mit einem Schlüsselraum von 2^n Schlüsseln gebrochen werden (d.h. das Sicherheitsniveau ist n Bit). Sowohl Angreifer als auch Nutzer des Kryptosystems wählen die Schlüssel gleichverteilt aus. Wie viele Versuche werden statistisch benötigt, um den richtigen Schlüssel zu erhalten? Begründen Sie Ihre Antwort.

(b) Nehmen Sie an, ein Angreifer kann 2^{24} Schlüssel pro Sekunde testen. Wie lange dauert ein Brute-Force-Angriff auf DES bzw. AES-128?

(c) Zwei wesentliche Grundprinzipien von Kryptosystemen sind Konfusion und Diffusion. Konfusion wird mit Hilfe einer Substitution erreicht, Diffusion mittels Permutation. Führen Sie die zwei Operationen beispielhaft auf den unten angegeben Text aus. Was soll innerhalb eines Kryptosystems mit diesen beiden Operationen erreicht werden? Erläutern Sie die Unterschiede.

G	E	H	E	I	M

Substitution

G	E	H	E	I	M

Permutation

Aufgabe 2 (Symmetrische Verschlüsselung mit OpenSSL)
OpenSSL[1] ist eine Bibliothek zur Nutzung kryptographischer Funktionen. Machen Sie sich mit der Kommandozeilen-Umgebung von OpenSSL vertraut. Sie können die `openssl`-Implementierung von Kali Linux verwenden.

(a) Die beiden Optionen „`aes-128-ctr`“ und „`des-ede-cbc`“ realisieren symmetrische Verschlüsselungsalgorithmen. Geben Sie für beide jeweils an, um welche Chiffre es sich handelt, welche Schlüssel- und Blocklänge und welcher Verschlüsselungsmodus eingesetzt wird. Erläutern Sie dabei, wie CTR und CBC funktionieren. Sind die Verschlüsselungsverfahren kryptographisch sicher? Begründen Sie Ihre Antwort.

(b) Erstellen Sie in Ihrer Kali-VM mit Hilfe eines Texteditors Ihrer Wahl eine Textdatei, in der Sie vier mal untereinander `IT-Sicherheit19` einfügen (d.h. die Textdatei besteht aus vier Zeilen mit jeweils dem angegebenen Wort). Verschlüsseln Sie anschließend die Datei jeweils mit Hilfe des Data Encryption Standard (im OFB Modus) und Advanced Encryption Standard (Schlüssellänge 256 Bit im ECB Modus).

Hinweis: Nutzen Sie bei beiden OpenSSL-Befehlen zusätzlich die Option `-nosalt`.

Im Anschluss sollen Sie sich beide verschlüsselte Dateien in einem Hexeditor betrachten (beispielsweise `xxd`). Was fällt Ihnen dabei auf? Beurteilen Sie die Sicherheit der verwendeten Verfahren.

[1] `www.openssl.org`