Hochschule RheinMain
Fachbereich Design Informatik Medien
Studiengang Angewandte Informatik / Informatik Technische Systeme
Prof. Dr. Bernhard Geib

Security

Sommersemester 2022
(LV 4120 und 7240)

3. Aufgabenblatt

Ziel dieser Übung ist es, die grundsätzlichen Anforderungen an ein Kryptosystem herauszustellen. Ferner werden erste Überlegungen hinsichtlich der Sicherheit von kryptographischen Algorithmen und Verschlüsselungsverfahren angestellt. Des Weiteren streift diese Übung kurz die Themenbereiche digitale Signatur sowie Message Authentication Code.

Aufgabe 3.1

a) Welche Mindestanforderungen werden grundsätzlich an einen Verschlüsselungsalgorithmus gestellt?

b) Welcher Schlüsselraum ergibt sich bei einer Schlüssellänge von L = 32 Zeichen und einem Schlüsseltextalphabet A .. Z, a .. z, 0 .. 9? Vergleichen Sie diesen Schlüsselraum mit dem des derzeit bedeutendsten symmetrischen Verschlüsselungsverfahrens AES (192 Bit Schlüssellänge).

c) Unter welchen Voraussetzungen gilt ein Kryptoalgorithmus im Allgemeinen als sicher? Wann ist er uneingeschränkt sicher?

d) Was besagt das Prinzip von A. Kerckhoffs?

e) Welcher Unterschied besteht zwischen symmetrischen und asymmetrischen Verfahren im Hinblick auf die Schlüsselmannigfaltigkeit?

Aufgabe 3.2

a) Welche Komponenten (Algorithmen, Schlüssel, Zertifikate etc.) benötigen Sie, um eine digitale Signatur zu erstellen?

b) Schildern Sie schematisch den Vorgang einer Signaturerstellung.

c) Unter welchen Bedingungen endet die Signaturprüfung mit einem positiven Prüfergebnis?

d) Recherchieren Sie im Internet, was man unter einer *qualifizierten* digitalen Signatur versteht.

Aufgabe 3.3

a) Wie funktioniert ein hybrides Verschlüsselungsverfahren?

b) Welchen Schlüssel benutzt man für die Entschlüsselung einer Nachricht bei einer asymmetrischen Verschlüsselung?

Aufgabe 3.4

a) Zeichnen Sie das Prinzipschaltbild zur Berechnung eines Message Authentication Codes (MAC).

b) Welches Verfahren erhält man, wenn man bei der Berechnung eines Message Authentication Codes (MAC) den symmetrischen Verschlüsselungsalgorithmus gegen einen asymmetrischen Verschlüsselungsalgorithmus austauscht?

Aufgabe 3.5

a) Welche Botschaft verbirgt sich hinter der folgenden chiffrierten Nachricht, von der Sie wissen, dass es sich um eine Caesar-Verschlüsselung mit dem Schlüsselwert k = 3 handelt? Die nachstehende Tabelle verdeutlicht die Anwendung des Schlüssels bei der vorgenommenen Chiffrierung. Das Klartextalphabet besteht aus a .. z und das Cybertextalphabet aus A .. Z.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Caesar-Chiffre (k = 3)

```
FUBSW RORJB LVWKH VFLHQ FHWKD WHPEU DFHVF
UBSWR JUDSK BDQGF UBSWD QDOBV LVEXW WKHWH
UPFUB SWROR JBVRP HWLPH VORRV HOBGH VLJQD
WHVWK HHQWL UHGXD OILHO GRIER WKUHQ GHULQ
JVLJQ DOVVH FXUHD QGHAW UDFWL QJLQI RUPDW
LRQIU RPWKH PWKLV EURDG HUILH OGKDV JURZQ
WRLQF OXGHP DQBQH ZDUHD VLWHQ FRPSD VVHVI
RUHAD PSOHP HDQVW RGHSU LYHWK HHQHP BRILQ
IRUPD WLRQR EWDLQ DEOHE BVWXG BLQJW KHWUD
IILFS DWWHU QVRIU DGLRP HVVDJ HVDQG PHDQV
RIREW DLQLQ JLQIR UPDWL RQIUR PUDGD UHPLV
VLRQV
```

b) Zu welchem Verfahren gelangt man, wenn man den Verschlüsselungsalgorithmus für beliebige Schlüsselwerte $1 \leq k \leq 26$ auslegt?