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

Security

Sommersemester 2022
(LV 4120 und 7240)

11. Aufgabenblatt

Das folgende Aufgabenblatt beschäftigt sich zunächst mit der Implementierung einer affinen Tauschchiffre. Ziel ist es dabei, die zur Verschlüsselung und Entschlüsselung verwendete Chiffrier- bzw. Dechiffrierfunktion in einer höheren Programmiersprache zu implementieren und darüber hinaus die mathematischen Methoden anzuwenden, die zur Ermittlung der Schlüsselparameter heranzuziehen sind. Des Weiteren setzen wir uns mit den Grundlagen und Anwendung einer ElGamal-Verschlüsselung auseinander.

Aufgabe 11.1

Wir betrachten eine (monoalphabetische) affine Tauschchiffre über dem Alphabet **A** = { 0, 1, ..., 9, a, b, ..., z, A, B, ..., Z } mit der folgenden Chiffrierfunktion:

$$\mathbf{E}: \quad z' = (z \cdot t + k) \bmod n$$

wobei

$$t = 13 \quad \text{und} \quad k = 57.$$

a) Wie lautet die entsprechende Dechiffrierfunktion **D** in allgemeiner Form?

b) Handelt es sich bei der Parameterwahl t = 13 und k = 57 um eine geeignete Vorgabe? Begründen Sie Ihre Antwort!

c) Berechnen Sie die Schlüsselparameter der Dechiffrierfunktion **D**.

d) Welchem Klartext-Zeichen entspricht das Chiffre-Zeichen „ h “?

Aufgabe 11.2

a) Wie viele verschiedene affine Tauschchiffren gibt es auf dem Alphabet **A** = {a, b, ..., z}?

b) Entscheiden Sie, ob n = 437 eine RSA-Zahl ist. Falls ja, bestimmen Sie die Anzahl aller möglicher öffentlicher Exponenten e.

Aufgabe 11.3

Wir betrachten das ElGamal-Verschlüsselungsverfahren über der Gruppe $\mathbf{G} = \mathbf{Z}_{29}^*$ mit dem Erzeuger g = 2.

a) Verschlüsseln Sie die beiden Klartexte $M_1 = 7$ und $M_2 = 10$ mit dem öffentlichen Schlüssel $P_K = 5$. Verwenden Sie hierzu die Zufallszahlen $r_1 = 5$ bzw. $r_2 = 8$.

Wir betrachten nunmehr das ElGamal-Verschlüsselungsverfahren über der Gruppe $\mathbf{G} = \mathbf{Z}_{13}^*$ mit dem Erzeuger g = 2.

b) Wie lautet der zugehörige öffentlichen Schlüssel P_K zum geheimen Schlüssel $S_K = 5$?

c) Entschlüsseln Sie des Weiteren mit dem geheimen Schlüssel $S_K = 5$ die beiden Chiffrate $C_1 = (4, 1)$ und $C_2 = (11, 2)$.

d) Wie viel Bit Nutzinformation kann ein einzelnes ElGamal-Chiffrat über $\mathbf{G} = \mathbf{Z}_p^*$ (p prim) haben?

e) Wie ist das Verhältnis von Nutzinformation und Chiffratlänge?

Aufgabe 11.4

Erläutern Sie die Begriffe Diffusion und Konfusion am Beispiel eines symmetrischen Verschlüsselungsalgorithmus.

Aufgabe 11.5

Ein Texteditor zeige Ihnen ein in einer Passwortdatei verschlüsselt abgelegtes Passwort wie folgt am Bildschirm an:

┴S 8≤f SΓö u┴

Bekannt sei, dass jedes dieser Zeichen gemäß dem 8-Bit-ASCII-Zeichensatz (erweiterte ASCII-Tabelle) durch ein 8 Bit langes Datenwort repräsentiert wird. Demnach wurden die einzelnen Chiffrezeichen wie folgt kodiert:

ASCII-Zeichen	┴	S	8	≤	f	Γ	ö	u
Hexadezimalzahl	BD	53	38	F3	66	E2	94	75

Weiterhin sei bekannt, dass zum Chiffrieren des ursprünglich im Klartext eingegebenen Passwortes das RSA-Verschlüsselungsverfahren mit einer Blocklänge von 2 Zeichen (16 Bit Wortlänge) verwendet wurde.

a) Welchen Wert hat der die Passwortdatei verschlüsselnde und sogenannte Verschlüsselungsschlüssel, wenn der geheime (private) Schlüssel des angewandten RSA-Verschlüsselungsverfahrens den Wert ($S_k = 27917$, $n = 67519$) aufweist?

b) Wie lautet die dazugehörige Dechiffrierfunktion?

c) Verwenden Sie nun die in Ihrer kryptographischen Library bereits vorhandene Funktion `encRSA()` und dechiffrieren Sie die verschlüsselte Passwortdatei unter Anwendung des entsprechenden Schlüssels.

d) Wie lautet demnach das vollständige Klartext-Passwort?

Aufgabe 11.6

a) Ermittlung der ersten 1.000.000 Primzahlen > 2 und tabellarische Ausgabe der Primzahlen. Ermitteln Sie eine zufällige Primzahl im Intervall [10, 100] sowie im Intervall [375, 20000].

b) Überprüfen Sie mit `IsPrime(n)`, ob es sich bei den Zahlen n = 1.999.121, 2.482.553 und 2.617.259 um Primzahlen handelt.

c) Wie viele Primzahlen liegen im Intervall [2.400.000, 2.500.000]?

d) Bestimmen Sie für die folgenden Zahlen die Primteiler und deren Vielfaches: n = 56735, 445 und 94567.