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

Security

Sommersemester 2021
(LV 4121 und 4241)

1. Aufgabenblatt

Ziel dieser Übung ist es, die potenzielle Gefährdungslage im IT-Umfeld zu diskutieren sowie das grundsätzliche Anliegen nach Informationssicherheit herauszustellen. Im Hinblick auf Gefährdungslage wird insbesondere zwischen den Begrifflichkeiten Angriff, Bedrohung, Schwachstelle, Sicherheitslücke und dem daraus ableitbaren Risiko unterschieden.

Aufgabe 1.1

a) Recherchieren Sie den Anteil der von Sicherheitsverstößen betroffener Unternehmen sowie die am stärksten betroffenen Branchen.

1. Finanzdienstleistungen
2. Logistik
3. Gesundheitswesen
4. Regierungsbehörden
5. Energiesektor

b) Versetzen Sie sich kurz in die Rolle eines Angreifers und beschreiben Sie generisch einen potenziellen Angriffsversuch. Welche prinzipiellen Schritte sind für einen IT-Angriff erforderlich? Welche Aktionen sind seitens des Angegriffenen zu erwarten? Wann ergibt sich aus einem Angriff eine Gefährdung?

1. Ziel wählen
2. Informationsgewinnung
3. Social Engineering
4. Angriff

Schutz durch Schulungen der Mitarbeiter, Softwareupdates durchführen,
Sicherheitslevel der Mitarbeiter, Rechner verschlüsseln, Netzwerk sichern, Firewall

Aufgabe 1.2

Ein Online-Banking Kunde erhält von seiner Bank eine E-Mail mit der Aufforderung, seine persönlichen Bankdaten zu aktualisieren. Gleichzeitig wird der Kunde darüber informiert, dass ein System-Update seitens der Bank erfolgt ist und er nunmehr seine Online-Daten auf Korrektheit prüfen solle. In der E-Mail ist ein Hyperlink enthalten, der offensichtlich ohne großen Aufwand ein Kunden-Login auf dem Portal der Bank ermöglicht. Diesen Link klickt der Kunde an. Über den Browser erscheint ein Login-Formular, in welches der Kunde seine persönliche Online-Daten eingibt und welches er abschließend mit dem Login-Button abschließt. Im Anschluss an diese Aktion erscheint eine Fehlermeldung mit dem Hinweis, dass der Login-Versuch fehlgeschlagen sei und wiederholt werden müsse. Der Kunde folgt dieser Aufforderung. Einige Sekunden später wird der Browser automatisch auf das Bankportal geleitet, wonach der Kunde den Login-Vorgang erneut durchführt. Diesmal allerdings mit Erfolg!

a) Welcher Art des Angriffs ist der Kunde mit hoher Wahrscheinlichkeit zum Opfer gefallen?

Phishing => Passwort fischen

b) Was sind die Schwachstellen eines solchen Online-Anmeldeformulars, mit dessen Hilfe der Kunde seine Benutzer-Authentifikation durch Eintippen von Benutzername und Kennwort in aller Regel mittels eines Standard-Browser bewerkstelligt?

fehlende gegenseitige Authentifizierung

c) Benennen und beschreiben Sie zwei Gegenmaßnahmen, die den Kunden vor dieser Art von Angriffsszenarium schützen.

keinen dubiosen Aufforderungen aus Mails folgen, HTTPS nutzen, Adressleiste überprüfen

d) Auf welche möglichen Motive der Angreifer lässt dieses Beispiel schließen? Nennen Sie mindestens vier.

1. Daten stehlen
2. Zugriff auf Account bekommen
3. Einpflanzen eines Virus
4. Verbreitung um Daten von weiteren Nutzern zu bekommen

Aufgabe 1.3

Warum sollen Passwörter auch dann nicht für Benutzer zugänglich abgespeichert sein, wenn die Passwörter beispielsweise durch eine Einwegfunktion verschlüsselt sind?

Brute Force Attack → Beliebte Passwörter hashen um zu sehen ob der gleiche Hash rauskommt. (Wörterbuchattacke)

Aufgabe 1.4

a) Erklären Sie kurz folgende 5 Begriffe aus der IT-Security Vorlesung:

Funktionssicherheit, asymmetrische Verschlüsselung, Spoofing, HMAC und Verfügbarkeit.

Funktionssicherheit = Safety zielt auf Übereinstimmung der Ist-Funktionalität der

Komponenten mit der spezifizierten Soll-Funktionalität ab
asymmetrische Verschlüsselung = privat key/public key
Spoofing = Authentifikations-, Authentifizierungs- und Identifikationsmechanismus
HMAC = Signaturen für Nachrichten. Zusätzlich zur Nachricht wird auch ein private key vom Ersteller mit gehasht
Verfügbarkeit = Schutz gegen unautorisierte Vorenthaltung/Verweigerung.
Wahrscheinlichkeit, den Betrachtungsgegenstand zu einem festen Zeitpunkt in einem intakten, funktionsfähigen Zustand anzutreffen.

b) Kreuzen Sie bitte an, welche Sicherheitsmaßnahmen beim Erreichen welcher Schutzziele sinnvoll sind:

	Redundanz	Firewall	Kryptographie	Virenschutz
Integrität	X		X	X
Vertraulichkeit			X	(x)
Verfügbarkeit	X	X		X
Zurechenbarkeit			X	
Verbindlichkeit			X	

c) Kreuzen Sie in der folgenden Tabelle ferner an, welche Themen eher mit Safety und welche eher mit Security zu tun haben:

	Safety	Security
Höhere Gewalt	X	X
Sniffing		X
Malware		X
HW-Defekt	X	
DDoS		X

DDoS = Distributed Denial of Service

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

Security

Sommersemester 2021
(LV 4121 und 4241)

2. Aufgabenblatt

Ziel dieser Übung ist es, einen Einblick in die Abgründe von Sicherheitslöchern zu geben. Die Sammlung von teils kuriosen, in der Regel aber recht schwerwiegenden Vorkommnissen soll Beispiele für typische Motive von Angreifern, die eingesetzten Angriffsmethoden und die dabei ausgenutzten Schwachstellen informationstechnischer Systeme zeigen. Durch das aufgezeigte breite Spektrum der Motive und Methoden soll insbesondere das Bewußtsein für die Notwendigkeit einer strukturierten Risikoanalyse geschaffen werden.

Aufgabe 2.1

Ihr Studentenwohnheim bietet vernetze Rauchmelder an, welche über WLAN und die Cloud im Bedarfsfall einen Alarm auf Ihr Handy auslösen. Wie hoch ist die System-Verfügbarkeit der Alarmierung, wenn in Ihrer Ein-Zimmer-Studentenwohnung zwei redundante Rauchmelder angebracht sind, die eine Verfügbarkeit von 90 % besitzen, und sowohl WLAN als auch die Cloud eine Verfügbarkeit von 98 % bzw. 96 % aufweisen?

0,9 * 0,9 * 0,98 * 0,96 + 0,1 * 0,9 * 0,98 * 0,96 * 2 = 0,931392 = **93,13 %**

Aufgabe 2.2

Eine Firma führt eine Datenbank mit den Gehältern ihrer Angestellten. Der Zugriff hierauf ist lediglich privilegierten Personen der Gehaltsbuchhaltung möglich. Allerdings existieren auf dieser Datenbank Zugriffsmöglichkeiten, die es den (unprivilegierten) Mitarbeitern der Abteilung für Unternehmensstatistik erlauben, das Durchschnittsgehalt einer Gruppe von mindestens zehn benennbaren Personen auszulesen.

a) Ist es einem Mitarbeiter dieser Abteilung unter dieser Sicherheitsstrategie möglich, die individuellen Gehälter einzelner Mitarbeiter zu extrahieren?

ja

b) Wenn ja, auf welche Weise? Wenn nein, welche zusätzlichen Rechte bräuchte er?

Gehalt_gruppe_von_10 = 75,000
Gehalt_gruppe_von_11 = 77,272
Gehalt_von_person_11 = 100,000

Gehalt_von_person_11 = Gehalt_gruppe_von_11 * 11 - Gehalt_gruppe_von_10 * 10

= 77,272 * 11 - 75,000 * 10 = 100,000

c) Auf welche möglichen Motive der Angreifer lässt dieses Beispiel schließen? Nennen Sie mindestens vier?

Datenverkauf an Konkurrenten
Wikileaks
Industrie Spionage
Neid
Reputationsschaden

d) Welche der abstrakten Werte der Informationssicherheit wurden durch den Angriff bedroht?

Integrität und Vertraulichkeit

Aufgabe 2.3

a) Was versteht man unter Steganographie?

Nachrichtenaustausch durch versteckte Nachrichten

b) Welche Prinzipien und Verfahren werden in der Steganographie angewandt.

- Bilddaten
- Audiodaten
- Textdaten
- im Dateisystem als Fragment

c) Was sind die beiden Hauptziele der Steganographie?

Vertraulichkeit
Dass man die Verschlüsselung nicht direkt erkennt

d) Was verbirgt sich hinter den folgenden drei Chiffren?

i) DSSGHISCE AITEEMAH
ii) SCHS! PUHCLESL RSUE
iii) RASEAC SUILUJ SUIAG

i) = DAS IST GEHEIMSACHE → abwechselt die Buchstaben aus den Wörtern lesen
ii) = SPRUCHSCHLUESSEL! →
iii) = GAIUS JULIUS CAESAR → rückwärts lesen

Aufgabe 2.4

a) Beschreiben Sie anhand eines Schaubildes oder mittels mathematischer Gleichungen die Arbeitsweise einer synchronen XOR-Stromchiffre! Nennen Sie je einen Vor- und einen Nachteil!

b) Was ist bezüglich des Schlüssels speziell bei Verwendung einer XOR-Stromchiffre immer zu beachten, außer dass der Schlüssel hinreichend lang und geheim sein muss? Begründung anhand eines Beispiels.

One Time Pad

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

Security

Sommersemester 2021
(LV 4121 und 4241)

3. Aufgabenblatt

Ziel dieser Übung ist es, die grundsätzlichen Aspekte der Informationssicherheit 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 die häufigsten Formen des Computermissbrauchs.

Aufgabe 3.1

a) Was versteht man unter "Sicherheit eines IT-Systems"?

IT Sicherheit besteht aus dem Verhältnis zwischen Risiko Wahrscheinlichkeit auf Angriff und gewichteter möglicher Schaden

b) Nennen und erläutern Sie fünf grundsätzliche Aspekte der Informationssicherheit.

Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität

c) Welches sind die häufigsten Formen des Missbrauchs informationstechnischer Systeme?

Diebstahl, Betrug, Spionage, Sabotage, Urkundenfälschung

d) Wie schätzen Sie die prozentuale Verteilung der verschiedenen Missbrauchsformen bzgl. statistisch erfasster Schadensereignisse ein?

1. Diebstahl
2. Betrug
3. Spionage
4. Sabotage
5. Urkundenfälschung

e) Informieren Sie sich über die häufigsten Missbrauchsdelikte und stellen Sie das Resultat graphisch dar.

Urkundenfälschung, Sabotage

Aufgabe 3.2

a) Welche Mindestanforderungen werden grundsätzlich an einen Verschlüsselungsalgorithmus gestellt?

Entschlüsselungsresistent, Konfusion, Diffusion, geringe Chiffrelänge bei notwendiger Sicherheit, einfach zu implementieren, Vielseitigkeit, nicht Vorhersagbar

b) Durch welchen Parameter sollte die Sicherheit eines Verschlüsselungsalgorithmus in der Praxis bestimmt sein?

Schlüssellänge, Vielfalt, Inhalt

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

Allgemein sicher: Nicht knackbar mit vertretbarem Ressourcen- und Zeitaufwand
Uneingeschränkt sicher: Klartext auch dann nicht ermittelbar, wenn Chiffretext in beliebigen Umfang vorhanden ist ⇒ starke Kryptographie

d) Was besagt das Prinzip von A. Kerckhoffs?

Sicherheit eines Kryptosystems darf nicht von dessen Geheimhaltung, sondern nur von der Schlüssellänge abhängen

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

Im Hinblick auf die Unterschiede entstehen beim Symmetrischen Verfahren ganz n*(n-1)/2 Schlüssel, wenn man eine Anzahl von n Nutzern hat, bei asymmetrisch n Schlüssel

Aufgabe 3.3

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

Verwendung findet bei der Signaturerstellung der geheime Schlüssel des Teilnehmers T
Bei der Signaturprüfung wird der zugehörige öffentliche Schlüssel des Teilnehmers T benötigt

Verifikationsalgorithmus, Signaturwert des Urhebers

b) Schildern Sie schematisch den Vorgang einer Signaturerstellung.

Ausgangspunkt: zu signierendes Dokument
Datensatz SigT der zusätzlich zu einem Dokument M erzeugt wird und die beiden das signierte Dokument eindeutig an Teilnehmer T zuordnet
SIGT = sig(H, SkT) → H = Hash-Message

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

1. Signatur-Ergebnis aus der empfangenen Nachricht des Urhebers und öffentlichem Schlüssel des Urhebers stimmen mit übertragenem Signaturwert des Urhebers überein
2. Nachricht des Urhebers muss integer sein
3. öffentlicher Schlüssel muss der öffentliche Schlüssel des Urhebers sein

Ist eine dieser Bedingungen nicht erfüllt, ist das Prüfergebnis negativ

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

Eine qualifizierte Signatur basiert auf einem qualifizierten Zertifikat und wurde mit einer sicheren Signaturerstellung (SSEE) erstellt.
Sie ist so konzipiert, dass man eine nachträgliche Veränderung der Daten in der Signatur erkennen kann.
Gültigkeitsbereich, Zertifikationsersteller, verwendete Hashfunktion, öffentliche Schlüssel das Zertifikat muss den Inhaber eindeutig identifizieren

Aufgabe 3.4

a) Wie funktioniert ein hybrides Verschlüsselungsverfahren?

Hybride Verschlüsselungsverfahren setzen ein asymmetrisches Verfahren für den Schlüsselaustausch ein und verschlüsseln Datenübertragung mit einem symmetrischen Verfahren

1. symmetrischer Schlüssel wird erzeugt
2. dieser wird mit einem asymmetrischen Schlüssel verschlüsselt
3. und an den Empfänger gesendet

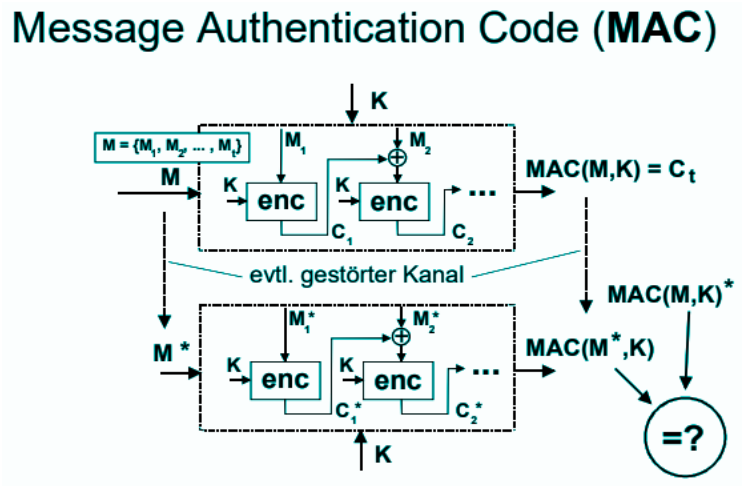
b) Welchen Schlüssel benutzt man für die Entschlüsselung einer Nachricht bei einer asymmetrischen Verschlüsselung?

private key

Aufgabe 3.5

a) Zeichnen Sie das Prinzip der Berechnung eines Message Authentication Codes (MAC).

Message Authentication Code (**MAC**)



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

Digitale Signatur

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

Security

Sommersemester 2021
(LV 4121 und 4241)

4. Aufgabenblatt

Ziel dieser Übung ist es, den Umgang mit algebraischen Strukturen wie Gruppen, Ringe oder Körper und hierbei insbesondere die Anwendung von mathematischen Operationen als Teil eines Kryptosystems kennen zu lernen. Bereits bei der mathematischen Formulierung einer einfachen Vigenère-Chiffre haben wir Modulo-Operationen (mod m) als Wertzuweisung benutzt und uns dabei auf den Restklassenring $\mathbf{Z}_m = \{0, 1, ..., m - 1\}$ bezogen. Von nun an werden wir dieses Konzept auch auf den Bereich von Kongruenzen anwenden. Die Berechnung und Lösung entsprechender Ausdrücke bzw. Gleichungen ist dann immer so zu verstehen, dass der zugewiesene Wert der kleinste nichtnegative Repräsentant der Restklasse ist.

Aufgabe 4.1

Bei der Definition von Gruppen wurde die Existenz eines neutralen Elements gefordert. Zeigen Sie, dass es in jeder Gruppe nur genau ein neutrales Element gibt.

Aufgabe 4.2

Angenommen, Sie wissen:

i) $7^a \bmod 31 = 10$ mit $a \in \mathbf{Z}_{31}$

ii) $6^x \equiv 1 \pmod{11}$ mit $x \in \mathbf{Z}_{11}$

wobei $\mathbf{Z}_m$:= Ring mod m = {0, 1, 2, ..., m – 1} ist. Ermitteln Sie mittels Raten und Einsetzen die ganzen Zahlen a und x.

Aufgabe 4.3

Wir betrachten die algebraische Struktur $<\mathbf{Z}_n, +, \cdot>$, bei der die Addition und die Multiplikation von a und b definiert sind als:

$$(a + b) \bmod n \quad \text{bzw.} \quad (a \cdot b) \bmod n$$

a) Um welche Struktur handelt es sich bei $<\mathbf{Z}_n, +, \cdot>$?

b) Ermitteln Sie für die beiden Elemente a = 1 und b = 2 in $<\mathbf{Z}_4, +, \cdot>$ die Elemente $-a$ und $-b$, sofern sie existieren.

c) Ermitteln Sie für die beiden Elemente a = 1 und b = 2 in $<\mathbf{Z}_4, +, \cdot>$ die Elemente a^{-1} und b^{-1} – sofern sie existieren.

Aufgabe 4.4

Zeigen Sie, dass für a, b, c $\in$ **Z** (Menge der ganzen Zahlen) gelten:

a) Aus $b \mid a$ und $c \mid b \Rightarrow c \mid a$.

b) Aus $c \mid a$ und $c \mid b \Rightarrow c \mid (a \pm b)$.

c) Zeigen Sie ferner, dass zwei ganze Zahlen a und b bei der Division durch n genau dann restgleich sind, wenn ihre Differenz ein Vielfaches des Moduls n ist. Für a, b $\in$ **Z** also gilt:

$$a \equiv b \pmod{n} \quad \Leftrightarrow \quad n \mid (a - b)$$

Aufgabe 4.5

a) Bestimmen Sie alle natürlichen Zahlen n, für die $n^3 - 1$ eine Primzahl ist.

b) Bestimmen Sie alle Primzahlen p, für die $11 \cdot p + 1$ eine Quadratzahl ist (d. h., dass $11 \cdot p + 1 = n^2$ für ein n $\in$ **N** ist).

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

Security

Sommersemester 2021
(LV 4121 und 4241)

5. Aufgabenblatt

Ganze Zahlen spielen eine fundamentale Rolle in der angewandten Kryptologie. Daher stellen wir in dieser Übungsserie grundlegende Eigenschaften der ganzen Zahlen heraus, die wir anschließend nutzen, um grundlegende kryptographische Basisalgorithmen effizient formulieren zu können. Ferner lösen wir Kongruenzgleichungen und beschäftigen uns mit einer Anwendung der Eulerschen Phi-Funktion.

Aufgabe 5.1

Es sei g := ggT(a, b) der größte gemeinsame Teiler der Zahlen a und b. Eine Vielfachsummendarstellung von g bei bekannten a und b ist gegeben durch die Form:

$$g = x \cdot a + y \cdot b$$

a) Ermitteln Sie zunächst mit Hilfe des Euklidischen Algorithmus den größten gemeinsamen Teiler der Zahlen a = 792 und b = 75.

b) Berechnen Sie anschließend durch sukzessives Einsetzen der Euklidischen Gleichungskette die ganzen Zahlen x und y mit der Eigenschaft:

$$ggT(792, 75) = 792 \cdot x + 75 \cdot y$$

Aufgabe 5.2

Es seien $a \in \mathbf{N}$ (Menge der natürlichen Zahlen) sowie $p, q \in \mathbf{P}$ (Primzahlen). Die Zahl a sei ferner kongruent 1 modulo p und kongruent 0 modulo q, d. h.

$$a \equiv 1 \pmod 5 \quad \text{und} \quad a \equiv 0 \pmod{17}$$

Wie lautet die Zahl a? (Bitte den Berechnungsweg vollständig angeben!)

Aufgabe 5.3

a) Berechnen Sie mit Hilfe eines Taschenrechners die Zahl $z = 257^{887} \bmod 31$.

b) Berechnen Sie die modulare Inverse der Zahl 15 im Ring $\mathbf{Z}_{1276}$!

Formal: $15^{-1} \bmod 1276 = ?$

Aufgabe 5.4

Bezüglich der Zahl 53461 seien zwei Dinge bekannt geworden:

i) Die Zahl 53461 ist das Produkt von genau zwei Primzahlen.

ii) $\phi(53461) = 52992$, wobei ϕ die Eulersche ϕ-Funktion bezeichne.

a) Können Sie mit Hilfe dieser Informationen die Zahl 53461 faktorisieren? Wenn ja, wie lauten die Primfaktoren?

b) Welche Konsequenzen hätte die Möglichkeit einer solchen Faktorisierung im Hinblick auf die Erzeugung kryptographischer Schlüssel?

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

Security

Sommersemester 2021
(LV 4121 und 4241)

6. Aufgabenblatt

Ziel des folgenden Aufgabenblatts ist es, den erforderlichen Rechenaufwand bei anspruchsvollen kryptographischen Berechnungen abschätzen zu können. Dazu beschäftigen wir uns zunächst mit der simultanen Lösung von Kongruenzgleichungen sowie der Berechnung der modularen Quadratwurzel. Anschließend entziffern wir eine Blockchiffre der Länge 2, deren Chiffretext bekannt ist.

Aufgabe 6.1

Es sei $x \in \mathbf{N}$ (Menge der natürlichen Zahlen).

a) Die Zahl x sei kongruent 1 modulo 3 und kongruent 2 modulo 5, d. h.

$$x \equiv 1 \pmod 3 \quad \text{und} \quad x \equiv 2 \pmod 5$$

Wie lautet die Zahl x? (Bitte den Berechnungsweg vollständig angeben!)

b) Gesucht ist die simultane Lösung der beiden Kongruenzen

$$2 \equiv x \pmod 3 \quad \text{und} \quad 1 \equiv x \pmod 5$$

Wie lautet die positive ganze Zahl x? (Bitte den Berechnungsweg vollständig angeben!)

c) Wann hat die Kongruenz

$$a \cdot x \equiv c \pmod m$$

eine Lösung x? (Die Frage ist nur zu beantworten!)

Aufgabe 6.2

Eine Lösung x der quadratischen Gleichung

$$x^2 = a$$

in der Ringstruktur $\mathbf{Z}_n$ nennen wir eine modulare Quadratwurzel und bezeichnen sie mit

$$x = a^{1/2} \bmod n.$$

Zahlen, welche eine modulare Quadratwurzel besitzen, nennen wir auch quadratische Reste (sonst quadratische Nichtreste).

a) Ermitteln Sie die beiden modularen Quadratwurzeln der Gleichung

$$x = 19^{1/2} \bmod 67.$$

b) Wieso treten die Lösungen von modularen Wurzelgleichungen immer paarweise auf?

c) Wann besitzt eine modulare Wurzelgleichung keine Quadratwurzeln?

Aufgabe 6.3

Bei der folgenden Blockchiffre der Länge 2 werde jeder Klartextblock **M** in einen entsprechenden Chiffreblock **C** gemäß der Vorschrift:

$$\mathbf{C} = \mathbf{K} \cdot \mathbf{M} \bmod n$$

transformiert, wobei der Schlüssel **K** aus einer 2x2-Matrix der Gestalt:

$$\mathbf{K} = \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix}$$

besteht. Für die Codierung der Zeichen a, b, c, ..., z und | des zugrunde liegenden Alphabets werden die Nummern 0, 1, 2, ..., 26 benutzt. Alle, sich bei der Transformation ergebenden Additionen und Multiplikationen werden modulo 27 berechnet.

a) Finden Sie die Schlüsselmatrix **K**, wenn sich als Chiffretext zu „`turing`“ die Zeichenfolge „`UBIXGT`“ ergibt.

b) Entschlüsseln Sie den restlichen Geheimtext „`ENERHLNHAHRM`“.

c) Warum wurde hier das Alphabet künstlich um das Zeichen „|“ erweitert, so dass es 27 statt 26 Buchstaben umfasst?

d) Warum ist 27 auch keine optimale Wahl? Geben Sie einen besseren Wert an.

Aufgabe 6.4

Berechnen Sie die modulare Exponentiation $2^{19487190} \bmod 19487191$ im Restklassenring $\mathbf{Z}_{19487191}$.

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

Security

Sommersemester 2021
(LV 4121 und 4241)

7. Aufgabenblatt

Mit den folgenden Aufgaben realisieren wir eine Krypto-Programmbibliothek, die uns für die wichtigsten kryptographischen Grundoperationen entsprechende Grundfunktionen zur Verfügung stellt. Neben der Generierung von Zufallszahlen, der Berechnung von Primzahlen sowie der Bestimmung der modularen Inversion und Exponentiation sind es auch die Basisalgorithmen zur Realisierung von unterschiedlichen Substitutionschiffren. Standardverfahren wie RSA, Diffie-Hellman oder ElGamal lassen sich auf diese Weise sehr effizient realisieren.

Aufgabe 7.1

Benutzen Sie die in der Vorlesung behandelten kryptographischen Grundfunktionen, um folgende Aufgabenstellungen zu lösen:

a) ggT(44243, 39713)

b) $\phi(78817)$

c) eEA(37486, 26319)

d) $136^{33} \bmod 257$

e) $3196^{-1} \bmod 83461$

Aufgabe 7.2

Es seien m = 259200, a = 7141 und b = 54773 die Parameter eines linearen Kongruenzengenerators.

a) Bestimmen Sie die durch $x_{n+1} = (a \cdot x_n + b) \bmod m$ definierte Pseudozufallsfolge $x_1, x_2, ..., x_{10}$ für die Startwerte: $x_0 = 0$ und $x_0 = 4711$.

b) Wie groß ist die Periodizität des Generators?

Aufgabe 7.3

a) Ermitteln Sie die Anzahl $\pi'(a, b)$ der Primzahlen im Intervall [a, b] mit $a = 10^6$ und $b = 10^9$.

Formal: $\pi'(a, b) = \#p_k$, $p_k \in \mathbf{P}$ wobei $a \leq p_k \leq b$ für $k = 1, 2, ..., \pi'(a, b)$

b) Ermitteln Sie die Anzahl der Primzahlen $\pi(n)$ kleiner gleich n und stellen Sie das Ergebnis graphisch dar.

c) Bestimmen Sie die Primzahlendichte $\pi(n) / n$ kleiner gleich n und stellen Sie auch dieses Ergebnis in einem Schaubild dar.

d) Ermitteln Sie alle Primzahlenpaare (p, q) für die gilt: $q = p + 2$ und $q < 200$. Beispiele für Primzahlenpaare sind: (3, 5), (5, 7), (11, 13) und (17, 19).

Aufgabe 7.4

Seien $k \geq 1$ und $p \in \mathbf{P}$. Zeigen Sie, dass dann für die Eulersche Phifunktion Φ gilt:

$$\Phi(p^k) = p^{k-1} (p - 1)$$

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

Security

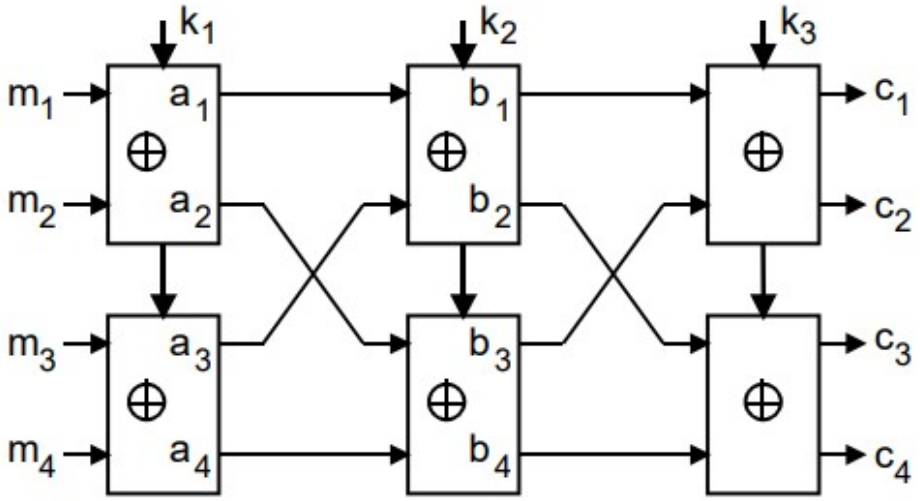
Sommersemester 2021
(LV 4121 und 4241)

8. Aufgabenblatt

Analyse und Entzifferung von einfachen Block- und Stromchiffren (Ver- und Entschlüsselung). Diskussion der Schlüsselwahl und -reihenfolge.

Aufgabe 8.1

In der folgenden Abbildung ist eine einfache Blockschiffre $E_k : \{0, 1\}^{16} \times \{0, 1\}^{24} \rightarrow \{0, 1\}^{16}$ mit $c = (c_1, c_2, c_3, c_4) = E_k(m) = E_k(m_1, m_2, m_3, m_4)$ dargestellt, wobei der Schlüssel $k = (k_1, k_2, k_3)$ 24 Bit lang ist. Die Komponenten m_i und c_i , $1 \leq i \leq 4$, sind jeweils 4 Bit lang. Die einzelnen Schlüsselkomponenten k_1, k_2 und k_3 besitzen jeweils eine Länge von 8 Bit.



Wird durch x II y die Konkatenation der Bitfolgen x und y dargestellt, und sind ein Klartext $m = (m_1, m_2, m_3, m_4)$ und ein Schlüssel $k = (k_1, k_2, k_3)$ gegeben, so ergibt sich der Chiffretext $c = (c_1, c_2, c_3, c_4)$ folgendermaßen:

$a_1 \text{ II } a_2 = k_1 \oplus (m_1 \text{ II } m_2)$ $\quad$ $a_3 \text{ II } a_4 = k_1 \oplus (m_3 \text{ II } m_4)$

$b_1 \text{ II } b_2 = k_2 \oplus (a_1 \text{ II } a_3)$ $\quad$ $b_3 \text{ II } b_4 = k_2 \oplus (a_2 \text{ II } a_4)$

$c_1 \text{ II } c_2 = k_3 \oplus (b_1 \text{ II } b_3)$ $\quad$ $c_3 \text{ II } c_4 = k_3 \oplus (b_2 \text{ II } b_4)$

a) Programmieren Sie für die Blockchiffre eine C/C++ Anwendung, die sowohl den 24 Bit Schlüssel k als auch den 16 Bit Klartext m von einer Eingabetextdatei einliest und den dazugehörigen 16 Bit Chiffretext c in eine Ausgabetextdatei schreibt.

Testen Sie die Funktion der Blockchiffre mit Hilfe folgender Beispieldaten:

Eingabedatei:

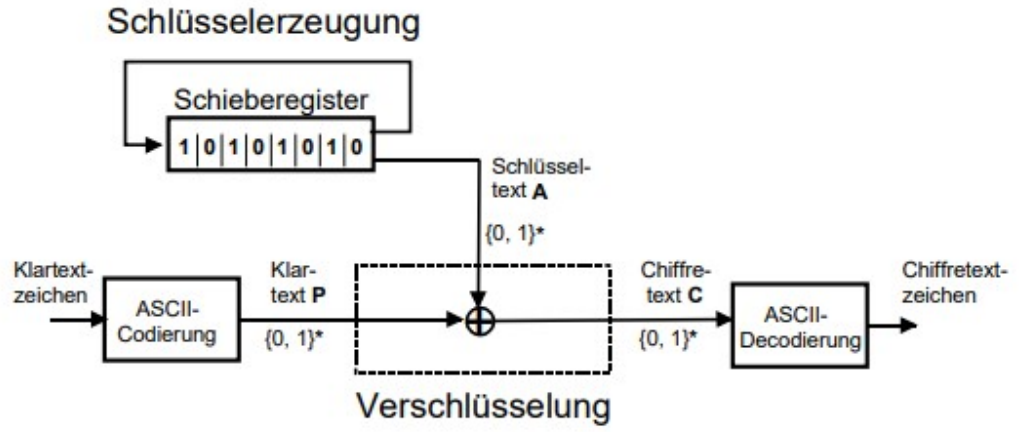
```
k = 10101010  11001100  00110011
m = 1001  0110  1100  0011
```

b) Wie lässt sich mit der angegebenen Blockchiffre aus dem Chiffretext c der Klartext m wieder rekonstruieren?

c) Testen Sie die Korrektheit Ihrer Implementierung, indem Sie den für die aufgeführten Beispieldaten erzielten Chiffretext c wieder in den Klartext m überführen.

Aufgabe 8.2

Wir betrachten die nachfolgend skizzierte binäre Stromchiffre, bei der der Chiffretext **C** aus der bitweisen XOR-Verknüpfung von Klartext **P** und Schlüsseltext **A** generiert wird. Der Einfachheit halber möge der verwendete Schlüsseltext mittels eines einfach rückgekoppelten Schieberegisters erzeugt werden, welches mit dem Cosetmuster 10101010 initialisiert wurde.



Die Codierung sowohl des Klartextes als auch des Chiffretextes erfolge mit Hilfe des 8-Bit ASCII-Zeichensatzes.

Programmieren Sie für die Stromchiffre eine C/C++ Anwendung, die den Klartext P von einer Eingabetextdatei einliest und den dazugehörigen Chiffretext C in eine Ausgabetextdatei schreibt.

Programmieren Sie für die Stromchiffre eine C/C++ Anwendung, die den Klartext P von einer Eingabetextdatei einliest und den dazugehörigen Chiffretext C in eine Ausgabetextdatei schreibt.

a) Testen Sie die Funktion der Stromchiffre mit Hilfe folgender Beispieldaten:

„Jede Sicherheitslücke ist zunächst auf ihre Ausnutzbarkeit hin zu untersuchen."

Wie lautet der dazugehörige Chiffretext?

b) Wie lässt sich aus einem erhaltenen Chiffretext C der dazugehörige Plaintext P ermitteln?

c) Testen Sie auch die Umkehrfunktion. Was verbirgt sich hinter folgender Chiffre?

„ïØÙÞŠÝÏÄÄŠÏÃÄÏŠùÃÉÂÏØÂÏÃÞÙÆVÉÁÏŠËßÙÄßÞÐÈËØŠÃÙÞ†
ÝÃØÎŠÙÃÏŠÐßŠÏÃÄÏÇŠÚÅÞÏÄÞÃÏÆÆÏÄŠøÃÙÃÁÅ„ŠãÄŠÎÃÏÙÏÇ
ìËÆÆŠÙÃÄÎŠùÃÉÂÏØÂÏÃÞÙÜÅØÁÏÂØßÄÍÏÄŠÏØÌÅØÎÏØÆÃÉÂ†
ÎÃÏŠÏÄÞÝÏÎÏØŠÎÃÏŠùÃÉÂÏØÂÏÃÞÙÆVÉÁÏŠÙÉÂÆÃÏuÏÄŠÅÎÏØ
ËÈÏØŠÎËÙŠùÃÉÂÏØÂÏÃÞÙØÃÙÃÁÅŠËßÌŠÏÃÄŠÞÅÆÏØÃÏØÈËØÏÙ
çËuŠÈÏÍØÏÄÐÏÄŠ‡ŠÙÅÍÏÄËÄÄÞÏÙŠøÏÙÞØÃÙÃÁÅ„"

Aufgabe 8.3

Für die Zahl e = 9 ergibt sich in $\mathbf{Z}_{31}$ nach einer Multiplikation mit der Zahl 17 der Wert a = 29. Mit welcher Zahl $z \in \mathbf{Z}_{31}$ müsste man die Zahl a multiplizieren, um wieder in $\mathbf{Z}_{31}$ als Ergebnis der Multiplikation die Zahl e zu erhalten?

Aufgabe 8.4

Entwerfen und implementieren Sie eine kryptographische Funktion in C, welche im Restklassenring $\mathbf{Z}_n$ die Berechnung der modulare Exponentiation a^b mod n mittels Square and Multiply Algorithmus ermöglicht.

a) Berechnung der modularen Exponentiation `ModExp(a, b, n)` für die natürlichen Zahlen a = 1.234.567.891.234.567, b = 1.234.567 und n = 543.222.266.

b) Vervollständigen Sie die nachstehende Tabelle mit Ihren Rechenergebnissen in der vierten Spalte.

a	b	n		a^b mod n
4294967295	17	2147483647		
4294967292	19	4294967295		
4294967289	31	8589934591		
4611686018427387909	64	4611686018427387903		
9223372036854775813	64	9223372036854775807		
18446744073709551615	64	18446744073709551611		

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

Security

Sommersemester 2021
(LV 4121 und 4241)

9. Aufgabenblatt

Ziel des folgenden Aufgabenblatts ist es, eine Hillchiffre zu implementieren und den zugrundliegenden Algorithmus zu analysieren.

Aufgabe 9.1

a) Entwickeln und implementieren Sie in der Programmiersprache C eine Applikation für eine (3x3)-Matrix Hill-Chiffre in Form einer multiplikativen Tauschchiffre $E : \{0, 1\}^{64} \times \{0, 1\}^{64} \rightarrow \{0, 1\}^{72}$ mit $\mathbf{C} = (\mathbf{K} \cdot \mathbf{P}) \bmod n$ gemäß dem in Vorlesung betrachteten Verfahren. Realisieren Sie sowohl die Verschlüsselungs- als auch die Entschlüsselungsfunktion `hillverH33()` bzw. `hillentH33()`. Für die Invertierbarkeit der Chiffre wird die Bedingung ggT(det **K**, n) = 1 vorausgesetzt. Die Matrizen **C**, **K** und **P** betrachten wir jeweils als 3x3-Matrix mit jeweils 9 Elementen. Jedes Element hat eine Länge von einem Byte.

$$\mathbf{X} = \begin{pmatrix} x_{1,1} & x_{1,2} & x_{1,3} \\ x_{2,1} & x_{2,2} & x_{2,3} \\ x_{3,1} & x_{3,1} & x_{3,3} \end{pmatrix}$$

*Matrix-Form **X** für **C**, **K**, **P***

Das Feldelement $x_{2,2}$ wählen wir sowohl bei der Schlüsseltextmatrix **K** als auch bei der Klartextmatrix **P** als Prüffeld (Addition mod n) zur Absicherung der übrigen Elemente der Matrix gegenüber eventuellen Übertragungs- oder Berechnungsfehler, so dass sich mit diesem Verfahren eine Blocklänge von 8 x 8 Bit = 64 Bit erzielen lässt. Für die Berechnung des Feldelements $x_{2,2}$ biete sich an:

$$x_{2,2} = (x_{1,1} \oplus x_{1,2} \oplus x_{1,3} \oplus x_{2,1} \oplus x_{2,3} \oplus x_{3,1} \oplus x_{3,2} \oplus x_{3,3}) \bmod n;$$

Der verwendete Zeichensatz sei { a..z, |, !, :, -, ? } und alle Berechnungen seien im Restklassenring $\mathbf{Z}_{31}$ auszuführen.

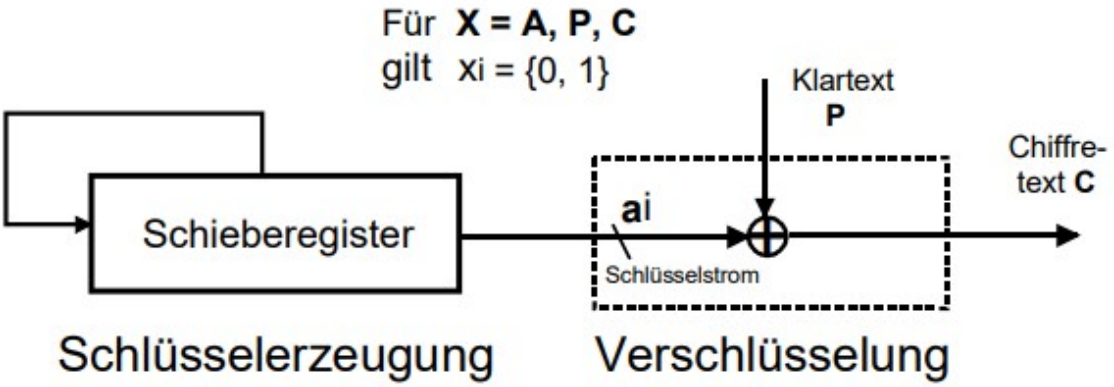
b) Ermitteln Sie unter Verwendung Ihres Programms für das 24 Zeichen lange Klartextpasswort `lestershlestersh:pass-rm` und den 8 Zeichen langen Schlüsseltext `hillkey!` den entsprechenden 24 Zeichen langen Ciphertext.

c) Wie lautet die entsprechende Dechiffrierfunktion und welche Matrizen müssen zum Entschlüsseln verwendet werden?

d) Ist durch die Wahl des Schlüsseltextes die Umkehrbarkeit der Chiffre gewährleistet? Begründen Sie Ihre Antwort.

Aufgabe 9.2

Bei einer binären Strom-Chiffre werden Klartext und Schlüssel modulo 2 addiert, um den Chiffretext zu erhalten. Umgekehrt werden zur Entschlüsselung Chiffretext und Schlüssel modulo 2 addiert. Eine besonders einfache Realisierung dieses Verfahrens (der "heiße Draht" zwischen Washington und Moskau soll auf diesem Prinzip basieren) mit Schieberegisterschaltungen und XOR-Schaltkreisen zeigt das folgende Prinzipschaltbild:



Bei der weiteren Betrachtung nehmen wir an, dass es sich um ein 4stufiges lineares Schieberegister handelt.

a) Welcher Schlüsselstrom ist erforderlich, um die Klartextfolge {1, 0, 1, 1, 0, 1, 1, 1} in die Chiffrefolge {1, 0, 1, 0, 0, 1, 0, 0} abzubilden?

b) Wie lautet der Startvektor des verwendeten Schieberegisters?

c) Ermitteln Sie die zugrundeliegende Rückkopplungsstruktur des Schieberegisters.

d) Skizzieren Sie die vollständige Schaltung des Verschlüsslers sowie des entsprechenden Entschlüsslers.

e) Was gilt es in bezug auf Synchronisation zu beachten?

Aufgabe 9.3

Gegeben sei eine Hash-Funktion H, die 10^8 unterschiedliche Hash-Werte erzeugen kann, z. B. Zahlen aus dem Intervall von 0 bis 99 999 999.

a) Weiterhin sei eine Nachricht M mit Hash-Wert H(M) gegeben. Wie viele Nachrichten müssen Sie erzeugen, um mit einer Wahrscheinlichkeit größer als 1/2 eine Nachricht mit demselben Hash-Wert H(M) zu erhalten?

b) Was ist eine Kollision bei Hash-Werten und wieso gibt es überhaupt Kollisionen?

Aufgabe 9.4

a) Entwickeln und implementieren Sie eine C-Funktion `hash(m)`, die zu einer einzulesenden Textdatei bzw. einer beliebig langen Nachricht m einen Fingerabdruck in Form eines Hashwertes h(m) erzeugt, der eine feste Länge von 56 Bit ausweist. Bei der Konstruktion des Hashalgorithmus werden jeweils 8 Zeichen der eingelesenen Nachricht m zu einem Block m_i (i = 0, 1, ..., M) mit der Länge von 8 Byte zusammengefasst und gemäß folgendem Algorithmus verarbeitet:

```
Wiederhole für alle Eingabetextblöcke i mit 0 <= i < M
    mi := block(z0 z1 z2 … z7);
mM := block(z0 z1 z2 … z5 '0' '0');
c0 = (m0)^k mod n ;
Wiederhole für alle Eingabetextblöcke i mit 0 < i <= M
    ci = (mi ⊕ ci-1)^k mod n ;
Output h(m) = cM ;
```

Dabei wird der zuletzt berechnete Block c_M als Hashwert der Nachricht m aufgefasst. Die beiden Sonderzeichen der Textdatei LF (\n) und EOF werden mit dem Wert 10 für \n bzw. 127 für EOF in die Berechnung des Hashwertes miteinbezogen. Falls ein Auffüllen (Pad) des letzten Blockes m_M erforderlich ist, um auf eine Blocklänge von 8 Zeichen zu kommen, erfolgt dies mit dem Zeichen '0' bzw. ASCII-Wert 48 von rechts (LSB) nach links (MSB). Die Parameter dieses Hash-Algorithmus sind n und k. Sie sind für die Kollisionsresistenz von entscheidender Bedeutung.

Wir interpretieren die Zeichen der Textdatei als 7-Bit-ASCII im Wertebereich von 0 bis 127 (dezimal) bzw. 0 bis 7F (hexadezimal) und wenden folgende Zahleninterpretation für den Wert eines Blockes an.

$$Wert(m_i) = z_0 \cdot 2^{49} + z_1 \cdot 2^{42} + \ldots + z_6 \cdot 2^7 + z_7$$

bzw. für $0 \le i < M$

$$Wert(m_i) = z_0 <<<_{49} + z_1 <<<_{42} + \ldots + z_6 <<<_7 + z_7$$

und für den letzten Block m_M:

$$Wert(m_M) = z_0 \cdot 2^{49} + z_1 \cdot 2^{42} + \ldots + \backslash n \cdot 2^{21} + EOF \cdot 2^{14} + '0' \cdot 2^7 + '0'$$

Zwischenräume (Leerzeichen) werden mit dem Wert 32 berücksichtigt.

b) Ermitteln Sie für den Wert der folgenden Eingabetexte im UTF-8-Format den 56 Bit Hashwert als Dezimal- und Hexadezimalwert (einschließlich der beiden Steuerzeichen LF und EOL). Parameter sind k = 17 und n = 72.057.594.037.927.935.

Eingabetext	56 Bit Hashwert (dezimal und hexadezimal)	AZ
12345678		
123456789		
01234567		

AZ: *Anzahl Zeichen (einschließlich \n und EoF)*

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

Security

Sommersemester 2021
(LV 4121 und 4241)

10. Aufgabenblatt

Das folgende Aufgabenblatt beschäftigt sich zunächst mit der Anwendung einer Vigenère-Chiffre. Im Anschluss daran schätzen wir die erforderliche Rechenzeit für einen Brute-Force-Angriff auf einen Blockalgorithmus ab. Schließlich analysieren wir einen One-Time-Pad und stellen dabei einige grundsätzliche Überlegungen an.

Aufgabe 10.1

a) Dechiffrieren Sie die nachfolgenden Geheimtexte von denen Sie wissen, dass eine Verschiebechiffre (Vigenère-Chiffre, 1586) mit dem Schlüssel K = 5 benutzt wurde. Benutzen Sie hierzu ggf. ein selbstentwickeltes Rechnerprogramm!

i) UTQDFQUMFGJYNXHM
ii) FXDRRJYWNXHM
iii) NSAJWYNJWGFW

b) Ist die folgende Aussage „Es ist entscheidend, dass an jeder Stelle des Kryptogramms der Schlüssel eindeutig den Klartextbuchstaben zu jedem Geheimtextbuchstaben festlegt“ richtig?

Aufgabe 10.2

Berechnen Sie die Zeit für das Knacken des 1024-Bit-Schlüssels einer 1024-Bit-Blockchiffre mit einem Brute-Force-Angriff unter der Annahme, das Sie einen Block von 1024 Bit im Klartext und im Chiffretext vorliegen haben. Nehmen Sie ferner an, dass Sie Zugriff auf einen Rechner haben, der pro Sekunde 1 Megabit verschlüsseln kann.

Aufgabe 10.3

Beim One-Time-Pad darf der Schlüsselstrom nicht wiederholt oder für eine andere Nachricht verwendet werden, da sonst durch Korrelation der beiden Chiffretexte eventuell die Chiffre gebrochen werden kann. Diesen Sachverhalt verdeutlichen wir beispielhaft an einer Vernam-Chiffre, die ja bekanntlich einer Vigenère-Chiffre mit einem Klar- und Chiffrealphabet von {0, 1} entspricht. Dabei seien $P = p_1\ p_2 \cdots$ ein Klartext und $K = k_1\ k_2 \cdots$ ein Schlüssel mit $p_i, k_i \in \{0, 1\}$, $i = 1, 2, \cdots$. Dann setzen wir $C = E_K(P) = c_1\ c_2 \cdots$ mit $c_i = p_i \oplus k_i$, $i = 1, 2, \cdots$, wobei $\oplus$ das exklusive Oder ist.

Ein Klartext P werde nun mit dem Schlüssel K chiffriert und ausgesendet. Durch einen Angreifer werde nun dieser Chiffretext mit einem mit dem gleichen Schlüssel erzeugten Chiffrat überlagert.

a) Auf welche Weise (formale Herleitung) lässt sich mit Hilfe des korrelierten Chiffretextes der Klartext P rekonstruieren?

b) Es sei C' = 0111 0101 der korrelierte Chiffretext und P' = 0010 1001 der dem Angreifer bekannte Klartext. Wie lautet der ursprünglich ausgesendete Klartext P?

c) Wie ermittelt der Angreifer hieraus den Schlüssel K?

Aufgabe 10.4

Sender und Empfänger eines Kommunikationskanals stützen den Datenaustausch auf ein Rabin-Kryptosystem ab.

a) Der Sender verschlüsselt den Klartext T = 11 mithilfe des Rabin-Moduls n = 57. Wie lautet der zugehörige Ciphertext G?

b) Der Empfänger erhält eine Ciphertext G = 25. Sein privater Schlüssel sei (3, 19). Entschlüsseln Sie den erhaltenen Ciphertext.

c) Was können Sie über die Eindeutigkeit von T und G bei einem Rabin-Kryptosystem sagen?

d) Beurteilen Sie die Sicherheit eines Rabin-Kryptosystems?

Aufgabe 10.5

Ein Systemadministrator hinterlegt das folgende siebenstellige Passwort verschlüsselt in einem Safe:

eDDlIGT

Als Chiffrierfunktion wurde eine umkehrbare, monoalphabetische und affine Tauschchiffre mit einer Blocklänge von einem Zeichen (8 Bit), den Schlüsselparametern t = 17 und k = 5 sowie dem Modul n = 67 gemäß folgender Funktion verwendet.

$$z' = (t \cdot z + k) \bmod n$$

Dabei symbolisiert das Zeichen z ein Klartextzeichen und das Zeichen z' das dazugehörige Chiffretextzeichen.

Die Zeichenkodierung und -dekodierung erfolgte anhand nachstehender Zuordnung:

Zeichen	**0**	**1**	**...**	**9**	**a**	**b**	**...**	**z**	**A**	**B**	**...**	**Z**	**§**	**%**	**&**	**?**	**#**
zugeordnete Dezimalzahl	0	1	...	9	10	11	...	35	36	37	...	61	62	63	64	65	66

Die Verschlüsselung erfolgte auf einem 64 Bit Windows-Rechner.

a) Entwerfen und implementieren Sie ein C-Programm, welches Ihnen alle die für eine affine Tauschchiffre (Ver- und Entschlüsselung) erforderlichen Berechnungen ermöglicht.

b) Unter welcher Voraussetzung ist die gegebene Chiffrierfunktion umkehrbar?

c) Wie lautet die entsprechende Dechiffrierfunktion und welche Schlüsselparameter weist diese auf?

d) Dechiffrieren Sie nun das hinterlegte Passwort mit Ihrem Programm unter Verwendung der zuvor ermittelten Dechiffrierfunktion und ihrer Schlüsselparameter. Wie lautet das Passwort demnach im Klartext?

Ciphertextzeichen	e	D	D	l	I	G	T
Ciphertextzahlenwert	14	39	39	21	44	42	55
Klartextzahlenwert							
Klartextzeichen							

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

Security

Sommersemester 2021
(LV 4121 und 4241)

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

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

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?

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

Security

Sommersemester 2021
(LV 4121 und 4241)

12. Aufgabenblatt

Im folgenden Aufgabenblatt setzen wir uns mit der Realisierung, der Anwendung und der Analyse des RSA-Verfahrens auseinander. Mit dem RSA-Algorithmus steht das mit Abstand populärste Public-Key-Verfahren zur Verfügung. Der Algorithmus besteht im Wesentlichen aus zwei Teilen. Neben dem eigentlichen Chiffrieralgorithmus ist die Schlüsselerzeugung von großer Wichtigkeit für die Sicherheit des Verfahrens. Diese basiert auf der Schwierigkeit, große Zahlen in ihre Primfaktoren zu zerlegen. Schließlich bewerkstelligen wir mit dem Diffie-Hellman-Verfahren den Schlüsselaustausch innerhalb einer ungesicherten Infrastruktur.

Aufgabe 12.1

Als Public-Key-Verfahren stützt sich der RSA-Algorithmus auf einen öffentlichen Schlüssel (P_K, n) und einen privaten Schlüssel (S_K, n), wobei mit n der Modulus (öffentlich) bezeichnet wird. Dieser sei durch das Produkt zweier Primzahlen $n = p \cdot q$ mit p = 23 und q = 59 vorgegeben. Für die Erzeugung des öffentlichen Schlüssels stehen die folgenden ganzen Zahlen zur Auswahl:

(P_K, n) = (11, 1357) ; (14, 1357) ; (15, 1357) ; (18, 1357) oder (33, 1357)

a) Welcher der fünf Schlüsselwerte kommt als öffentlicher RSA-Schlüssel in Betracht?

b) Begründen Sie Ihre Auswahl!

c) Berechnen Sie den zugehörigen privaten RSA-Schlüssel.

Aufgabe 12.2

Für ein benutztes RSA-Verfahren möge der öffentliche Schlüssel Kp = 3 und n = 33 betragen. Versuchen Sie aus dieser Kenntnis heraus

a) den zugehörigen privaten Schlüssel Ks zu ermitteln und

b) den verschlüsselten Nachrichtenblock C mit dem Wert 180630 bei einer internen Blocklänge von 2 Ziffern zu entschlüsseln.

Aufgabe 12.3

Um einen Diffie-Hellman-Schlüsselaustausch durchzuführen einigen sich die beiden Kommunikationspartner A und B auf g = 3 und p = 17. A wählt als privaten Schlüssel x = 7; B legt für seinen privaten Schlüssel y = 4 fest.

a) Ermitteln Sie die öffentlichen Schlüssel von A und B, die jeweils mit der Gegenseite ausgetauscht werden.

b) Welche Berechnung hat A und B bei der Ermittlung des gewünschten gemeinsamen Schlüssels durchzuführen?

c) Wovon hängt die Sicherheit des DH-Verfahrens ab?

d) Welcher bekannte Angriff besteht beim DH-Schlüsselaustauschprotokoll?

Aufgabe 12.4

a) Erläutern Sie kurz die Grundfunktionen des AES.

b) Welche Bedeutung haben die S-Boxen beim DES?

Aufgabe 12.5

a) Schildern Sie eine Runde des Feistel-Verfahrens in pseudo-algorithmischer Notation. Verwenden Sie hierzu ggf. Zuweisungen, logische Operationen, linkszirkuläres Shiften und arithmetische Funktionen. Als Eingaben haben Sie L0, R0 sowie K0. Ausgaben sind L1 und R1.

b) Auf welchem Konstruktionsprinzip beruht die Sicherheit des Feistel-Verfahrens?

Aufgabe 12.6

Ein Message Authentication Code (MAC) dient dazu, Gewissheit über die Originalität oder den Ursprung von Daten oder Nachrichten zu erhalten und die Unversehrtheit der zu schützenden Daten überprüfen zu können. MAC-Algorithmen erfordern dabei zwei Eingabeparameter: neben dem Hashwert der Daten auch noch einen geheimen Schlüssel. Aus beidem wird dann eine Checksumme – der sogenannte Message Authentication Code – ermittelt.

a) Entwickeln und implementieren Sie ein C-Funktion, mit deren Hilfe Sie für einen gegebenen 32 Bit langen Hashwert h(m) einer Nachricht m und einen ebenso langen (geheimen) Schlüssel k durch die Vorschrift

$$MAC(h(m), k) = h(m) \oplus k$$

den Message Authentication Code MAC(h(m), k) herstellen können.

b) Ermitteln Sie für h(m) = AD778EF0 und den Schlüssel k = 12 34 56 78 den entsprechen MAC-Wert.

c) Welche Eigenschaft besitzt ein auf diese Weise erzeugter MAC? Begründen Sie Ihre Antwort.

d) Ist der auf diese Weise ermittelte MAC-Wert fälschungsresistent? Begründen Sie Ihre Antwort.