

Computersystemsicherheit

Lösungsblatt Nr. 1

von Patrick Elsen

Marc Fischlin, Jacqueline Brendel, Christian Janson

Wintersemester 2018-2019

Technische Universität Darmstadt

Gruppenübung

Die Übungsaufgaben in diesem Bereich sind Gegenstand der Übungen in der Woche vom 29.10.2018–02.11.2018.

Aufgabe 1 (Verständnisaufgaben).

In dieser Aufgabe prüfen wir unser Verständnis über den Inhalt der Vorlesung.

Benennen Sie die drei Schutzziele aus der Vorlesung.

Das erste Schutzziel ist *Vertraulichkeit*: die Eigenschaft, dass Informationen nicht Unberechtigten zur Verfügung gestellt wird). *Integrität* bedeutet, dass Informationen akkurat, komplett und unversehrt ist. *Verfügbarkeit* bedeutet, dass auf Informationen zugegriffen werden kann.

Was besagt Kerckhoffs-Prinzip?

Das Kerckhoffs-Prinzip sagt, dass die Sicherheit eines kryptographischen Systems nicht auf der Geheimhaltung des Systems, sondern auf der des Schlüssels beruht.

Will man ein sicheres System bauen, muss man davon ausgehen, dass der Angreifer das System kennt. Die Sicherheit darf also nicht darauf beruhen, dass der Angreifer das System nicht versteht. Ein sicheres System muss auch dann sicher sein, wenn es bekannt ist.

Was besagt die funktionale Korrektheit eines symmetrischen Verschlüsselungsverfahrens?

Die funktionale Korrektheit (auch *Vollständigkeit*) besagt, dass man mit allen Schlüsseln jede Nachricht erfolgreich ver- und entschlüsseln kann. Man schreibt also:

$$\forall m \in M, k \in K : \text{dec}(k, \text{enc}(k, m)) = m$$

Aufgabe 2: Schutzziele.

Wie Sie in der Vorlesung gelernt haben, bietet die deutsche Sprache keine eigenen Worte für *Safety* und *Security*. Beide Worte werden in der Regel mit Sicherheit übersetzt. *Safety* bezieht sich auf die Verlässlichkeit von IT-Systemen in Bezug auf Ablauf- und Ausfallsicherheit. Häufig übersetzt mit Betriebssicherheit. *Security* wird oft mit Angriffssicherheit übersetzt und spaltet sich dabei in die Teilaspekte *Authenzität*, *Integrität*, *Vertraulichkeit*, *Verfügbarkeit* und *Verbindlichkeit*.

Im Folgenden sind einige Szenarien gegeben, die eine Verletzung bestimmter Eigenschaften aufzeigen. Bitte nennen Sie die verletzte Schutz Eigenschaft und ggf. den Teilaspekt.

SZENARIO	SCHUTZEIGENSCHAFT
Durch Abhören eines Firmennetzwerkes ist es möglich, Passwörter von Mitarbeitern abzufangen.	Security (Vertraulichkeit)
Durch einen Programmierfehler in der Software des U-Bahn-Betriebs kommt es in letzter Zeit häufiger zu Abstürzen und einzelne Bahnen bleiben dabei auch unvorhergesehen in Tunneln stehen.	Safety
Ein Vorgesetzter beauftragt seinen Mitarbeiter eine Reise für ihn im internen Buchungssystem zu buchen. Der Mitarbeiter möchte aber nicht mit der Buchung in Verbindung stehen und beauftragt den Datenbankbeauftragten seinen Namen zu entfernen.	Security (Verbindlichkeit)
Durch eine Schwachstelle in einer Web Applikation ist es beliebigen (auch nicht registrierten) Nutzern möglich Gästebuch-einträge zu verändern.	Security (Integrität)

Aufgabe 3: Teilertheorie und Modulare Arithmetik

Berechnen Sie L

$$\begin{array}{ll} \text{i)} & 7 \equiv 1 \pmod{2} \\ \text{ii)} & 3^5 = 243 \equiv 5 \pmod{7} \\ \text{iii)} & 4^3 \equiv 1^3 = 1 \pmod{3} \\ \text{iv)} & 12 \equiv 0 \pmod{4} \end{array}$$

Zeigen Sie, dass 429 und 595 teilerfremd sind.

Das geht am einfachsten mit dem Euklidischen Algorithmus, der den größten gemeinsamen Teiler von zwei beliebigen Zahlen bestimmen kann. **TODO**.

Sei $n \in \mathbb{N}$ und sei $p \in \mathbb{N}$ ein Teiler von n , d. h. $p \mid n$. Zeigen Sie:

TODO.

Aufgabe 4: One-Time-Pad (Vernam Chiffre). In der Vorlesung haben Sie das One-Time-Pad (Vernam Chiffre) kennengelernt.

- a) Erinnern Sie sich an die Definition des OTP und notieren Sie wie die Verschlüsselung einer Nachricht m und Entschlüsselung des resultierenden Chiffrats c funktioniert.

Bei einer One-Time-Pad-Verschlüsselung benutzt man die bitweise Exclusive-OR (XOR) Funktion, um die Nachricht zu verschlüsseln und um das Chiffrat zu entschlüsseln.

$$c = m \oplus k \qquad m = c \oplus k \qquad k = m \oplus c$$

- b) Gegeben sind folgende Nachricht $m = 1010\ 1111$ und der Schlüssel $k = 1111\ 0000$. Berechnen Sie das OTP Chiffrat.

$$\begin{array}{r} 1010\ 1111 \\ \oplus\ 1111\ 0000 \\ \hline 0101\ 1111 \end{array}$$

- c) Was ist perfekte Sicherheit? Und warum erfüllt das OTP diese?

Perfekte Sicherheit ist die Eigenschaft einer Verschlüsselung, dass das Chiffrat keine Informationen über die Nachricht besitzt. Es können aus diesem also keine Schlüsse über die Nachricht gezogen werden. OTP besitzt perfekte Sicherheit, wenn der Schlüssel geheim ist und zufällig generiert wurde.

Da der Schlüssel zufällig gewählt wurde, ist jedes Bit zu 50% 1 und zu 50% 0. Durch den XOR-Operator wird damit jedes Bit der Nachricht zu 50% geflippt. Damit besitzt das Chiffrat keine Informationen mehr über die Nachricht: jedes Bit ist zu 50% ein Bit der Nachricht oder zu 50% ein geflipptes Bit.

- d) Diskutieren Sie warum das OTP unsicher wird sobald man den Schlüssel mehrmals verwendet. Unter welchen Umständen wird das OTP auch unsicher?

- e) Diskutieren Sie was passiert wenn Sie XOR (\oplus) durch die Operation ODER (\vee) im OTP ersetzen.

Mit der Operation ODER kann der OTP nicht funktionieren. Die Funktionsweise des OTP hängt von der Eigenschaft der XOR-Operation, dass eine wiederholte Anwendung zurück zum Klartext führt. Mathematisch braucht man also einen Operator \circ , so dass gilt:

$$m = (m \circ k) \circ k$$

Diese Eigenschaft ist mit dem ODER-Operator nicht gegeben, was an folgenden Beispiel illustriert werden kann:

$$0 \neq (0 \vee 1) \vee 1$$

Aufgabe 5: Angriff auf eine Chiffre (Known-Plaintext-Attack). Im Folgenden wollen wir einen Angriff auf eine Chiffre betrachten. Die zu verschlüsselende Nachricht m und das resultierende Chiffre c sind Bitstrings der Länge n (d.h. $m, c \in \{0, 1\}^n$). Der für die Verschlüsselung notwendige Schlüssel ist folgendermaßen definiert:

- einem Bitstring $k \in \{0, 1\}^n$.
- einer quadratischen invertierbaren Matrix $M \in \{0, 1\}^{n \times m}$.
- Funktionen $f_i : \{0, 1\}^n \rightarrow \{0, 1\}$ für $i = 1, \dots, n$.

Die Verschlüsselungsoperation für eine beliebige Nachricht $m \in \{0, 1\}^n$ und Schlüssel ist wie folgt definiert:

1. Setze $v = M * m$, wobei $v = (v_1, \dots, v_n)$.
2. Berechne die i -te Chiffrekomponente $c_i = v_i \oplus f_i(k)$ für $i = 1, \dots, n$.

Dadurch erhalten Sie das Chiffre $c = (c_1, \dots, c_n)$.

Sie haben jetzt folgende Klartext und Chiffre Paare abgefangen:

Diese Informationen genügen, um jedes beliebige Chiffre effizient zu entschlüsseln, obwohl die Funktionen f_i und die Matrix M unbekannt sind. Brechen Sie die obige Chiffre und berechnen Sie den Klartext hinter dem Chiffre $c = (0010)$.

1 Hausübung

Dieser Bereich ist dazu gedacht das Gelernte weiter zu vertiefen. Dazu werden je nach Themen weitere Übungsaufgaben, ergänzende Beweise oder ähnliche Aufgaben gestellt. Die Aufgaben sind freiwillig, können aber, bei erfolgreicher Bearbeitung, zu Bonuspunkten in der Klausur führen. Die Abgabe dieser Übungen erfolgt über *Moodle* und kann in Gruppen mit bis zu vier Studenten (*aus Ihrer eigenen Übungsgruppe*) eingereicht werden. Abgaben werden nur als PDF-Dateien akzeptiert. Denken Sie bitte daran, dass Ihre Lösungen nachvollziehbar und entsprechend ausführlich dargestellt werden sollen.

Für Gruppenabgaben ist folgendes zu beachten: Sie müssen in der Abgabe (.pdf-Datei) deutlich und eindeutig kennzeichnen mit welchen Gruppenpartnern die Aufgaben gelöst wurden.

Der Fachbereich Informatik misst der Einhaltung der Grundregeln der wissenschaftlichen Ethik großen Wert bei. Zu diesen gehört auch die strikte Verfolgung von Plagiarismus. Falls dieser Fall eintritt, behalten wir uns das Recht vor für diese Abgabe den jeweiligen Gruppen keine Punkte gutzuschreiben.

Bitte reichen Sie Ihre Abgabe bis spätestens Freitag 09.11.2018 um 11:40 Uhr ein. Verspätete Abgaben können nicht berücksichtigt werden.

Hausübung 1: PGP (2 Punkte – Einzelabgabe). Sie haben in der Vorlesung das Schutzziel Dreieck (C.I.A.) kennengelernt. Ein Beispiel Angriff auf die Confidentiality ist das Mitlesen der Internetkommunikation, wie z.B. ihrer Emails. Dieses Problem kann man leicht beheben indem man die Emaillkommunikation verschlüsselt. PGP (Pretty Good Privacy) ist ein Programm zum Verschlüsseln (und signieren) von Daten und basiert auf einem Public-key (asymmetrisches) Verfahren. Führen Sie folgende Schritte durch:

- Installieren Sie PGP kostenlos für Ihr bevorzugtes Betriebssystem.
- Generieren Sie für Ihre Emailadresse ein Schlüsselpaar und besorgen Sie sich aus Moodle den öffentlichen Schlüssel Ihres Tutors, sowie die jeweilige Emailadresse.
- Schicken Sie dann eine verschlüsselte Email an ihren Tutor mit dem Betreff *ComSySec - Hausübung 1* und mit folgenden Informationen: Ihr Name, Name des Tutors, Übungstermin (inkl. Gruppennummer) und Raumnummer.

Hausübung 2: Permutationschiffre und Operationsmodi

In der Vorlesung haben Sie das Konzept der Blockchiffre und verschiedene Operationsmodi (u.a. ECB und CBC) kennengelernt. Wir definieren eine Blockchiffre E , die die Eingabebits permutiert, wobei die Permutation π als Schlüssel fungiert. Die Ver- und Entschlüsselung sei gegeben durch

$$\begin{aligned}\text{Enc}((b_1, \dots, b_n), \pi) &:= (b_{\pi(1)}, \dots, b_{\pi(n)}) \\ \text{Dec}((d_1, \dots, d_n), \pi) &:= (d_{\pi^{-1}(1)}, \dots, d_{\pi^{-1}(n)})\end{aligned}$$

Zeigen Sie, dass dies ein Chiffriersystem definiert. Hinweis: Zeigen Sie, dass Ver- und Entschlüsselung kommutieren.

Dieses System definiert genau dann ein Chiffriersystem, wenn jede mögliche Nachricht ver- und entschlüsselt werden kann, und die originale Nachricht daraus resultiert.

$$\text{Dec}(\text{Enc}((m_1, \dots, m_n), \pi), \pi) = (m_1, \dots, m_n)$$

Das ist genau dann wahr, wenn die Applikation der Permutation und die darauffolgende Applikation der Inversen der Permutation die originalen Bits zurückgibt.

$$\forall n \in \mathbb{N} : n = \pi^{-1}(\pi(n))$$

Da eine Permutation eben so definiert ist, ist dieses ein Chiffriersystem.

Betrachten Sie nun speziell im Fall $n = 3$ den Schlüssel $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ und verschlüsseln Sie den String *101010101010* im ECB-Mode.

Hier kann man ein kleines Ruby-Programm schreiben, um das Ganze zu vereinfachen.

```
def encrypt_ecb(permutations, data)
  data.scan(/.{3}/).map do |block|
    permutations
      .sort_by{|_, v|}
      .map{|_, p| block[p-1]}
      .join
  end.join
end

puts encrypt_ecb({1 => 2, 2 => 1, 3 => 3}, "101010101010")
```

Dieses Programm gibt als ECB-Verschlüsselung den String 011100011100 aus.

Gegeben sei eine Sequenz m_1, m_2, \dots, m_n von Klartexten, die mittels einer beliebigen Blockchiffre im ECB oder CBC-Modus verschlüsselt wird, um eine Sequenz von Chiffraten c_1, c_2, \dots, c_n zu erhalten. Nehmen Sie an, dass bei der Übertragung von c_1 ein Fehler passiert (d.h. einige Bits von c_1 werden falsch übermittelt). Wieviele Blöcke der Sequenz m_1, m_2, \dots, m_n werden durch den Empfänger falsch rekonstruiert, wenn der ECB oder CBC-Modus verwendet wird? Begründen Sie Ihre Antwort.

Wenn der ECB-Modus verwendet wird, dann wird nur c_1 falsch entschlüsselt. Die Blocks im ECB-Modus hängen nicht voneinander ab, also werden Übertragungsfehler auch nicht auf sukzessive Blocks weitergegeben. Nur m_1 wird also fehlerhaft sein. Anders sieht das beim CBC-Modus aus. Hier wird ebenso c_1 falsch entschlüsselt, gleichzeitig gibt es aber auch einen Bitfehler in m_2 , da dieser von c_1 abhängt (welches falsch ist). Also sind hier m_1 falsch sein und m_2 wird einige falsche Bits haben (an genau den Stellen, an den c_1 falsche Bits hat). Um das zu demonstrieren, kann man ein kleines Ruby-Programm schreiben, was das ganze austestet.

```
require "openssl"

# data (four blocks big)
data = "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ;"

# encrypt data
cipher = OpenSSL::Cipher::AES.new(128, :CBC)
cipher.encrypt
key = cipher.random_key
iv = cipher.random_iv
encrypted = cipher.update(data) + cipher.final
orig_enc = encrypted.dup

# mutate first block of cipher
12.times do
  char = rand(16)
```

```

    bit = rand(8)
    encrypted[char] = (encrypted[char].bytes.first ^ (1 << bit)).chr
end

# decrypt data
decipher = OpenSSL::Cipher::AES.new(128, :CBC)
decipher.decrypt
decipher.key = key
decipher.iv = iv
plain = decipher.update(encrypted) + decipher.final

# analyze resulting plaintext
plain.bytes.zip(data.bytes).each_slice(16).each_with_index do |block, count|
  diffs = 0
  block.each do |bytepair|
    diffs += (0..8)
      .map{|bit| bit = (1 << bit); (bytepair[0] & bit) ^ (bytepair[1] & bit) != 0}
      .inject(0){|a,b| if b then a + 1 else a end}
  end
  puts "block_#{count}:_#{diffs}"
end

```

Dieses Programm verschlüsselt ein paar Daten mit AES128. Von den resultierenden Chiffreten werden 12 zufällig ausgewählte Bits verändert. Dann werden diese Entschlüsselt. Die entschlüsselten Daten werden nun, Block-für-Block, mit dem originalen Daten verglichen, und es wird ausgegeben, wie viele Bitfehler entstanden sind. Der Output von diesem Programm sieht so aus:

```

block 0: 64
block 1: 12
block 2: 0
block 3: 0

```

Hier sieht man, dass im ersten Block 64 Bitfehler entstanden sind (man erwartet, dass 50% der Bits fehlerhaft sind, das ist also exakt wie erwartet). Im zweiten Block sind nur noch 12 Bitfehler (das macht ebenso Sinn, da hier nur die Bits falsch sind, die im ersten Chiffretenblock falsch waren). Das Experiment bestätigt also diese Antwort.

Hausübung 3: Kasiski-Test

Sie haben einen Ciphertext abgefangen und wissen, dass es sich bei der Verschlüsselung um eine Vigenère-Verschlüsselung handelt. Der Ciphertext hat die folgende Form:

```
Eck0stgloaUclxatrxmfUclxrvkuikugfqwobxvKdfeywtqxpdbcgkw
```

CcbomsxxrKdfeywtqxpfhcaxvjclkmubtwafqbgzpdmaafbxvzpjxr

Wenden Sie den Kasiski-Test an, um die benutzte Schlüssellänge zu ermitteln. Bearbeiten Sie dafür folgende Schritte.

Suchen Sie alle eindeutig doppelt vorkommende N -Gramme (für $N \leq 4$) im Ciphertext und berechnen Sie den Abstand (Position des ersten Auftretens minus die Position des zweiten Auftretens) zwischen beiden gleichen N -Grammen.

Hier kann man ein kleines Ruby-Programm schreiben, um die N -Gramme und deren Abstand zu finden.

```
data = "Eck0stgloaUclxatrxfUclxrvkuikugfqwobxvKdfeywtqxpdcbgkwCcbomsxxrKdfeyw  
tqxpfhcaxvjclkmubtwafqbgzpdmaafbxvzpjxr".split.join
```

```
# find n-grams (4 or longer) and their distance.
```

```
ngrams = []  
(0..data.size).each do |a|  
  (a+1..data.size).each do |b|  
    len = 0  
    while data[a+len] == data[b+len]  
      len += 1  
    end  
  
    if len >= 4  
      ngrams << [b - a, data[a...a+len]]  
    end  
  end  
end
```

```
p ngrams
```

Dieses Programm findet zwei N -Gramme.

Bestimmen Sie die Primfaktorzerlegung für alle gefundenen Differenzen.

Für den Fall, dass die Wiederholung des N -Gramms nicht zufällig, sondern aufgrund einer Wiederholung eines N -Gramms im Klartext aufgetreten ist, enthält die Primfaktorzerlegung dieser Differenz einen Teiler der Schlüssellänge oder die Schlüssellänge selbst. Vermuten Sie die Länge des verwendeten Schlüssels.

Nachdem Sie die Schlüssellänge in Aufgabenteil c) bestimmt haben, versuchen Sie nun den Text zu entschlüsseln. Sie konnten außerdem in Erfahrung bringen, dass der zweite Buchstabe im Schlüssel ein Y und der Vierte ein E ist. Benutzen Sie diese Information um den Schlüssel zu ermitteln und dann den Klartext zu berechnen.