Computersystemsicherheit – Übungsblatt Nr. 1

Marc Fischlin, Jacqueline Brendel, Christian Janson
TU Darmstadt, 26 Oktober 2018

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.

a) Benennen Sie die drei Schutzziele aus der Vorlesung.

b) Was besagt Kerckhoffs-Prinzip?

c) Was besagt die funktionale Korrektheit eines symmetrischen Verschlüsselungsverfahren?

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 folgende Teilaspekte:
  - Authentizität ("authenticity"): Echtheit und Glaubwürdigkeit des Objektes bzw. Subjekts, die anhand von bestimmten Eigenschaften überprüfbar sind.
  - Integrität ("integrity"): Gewährleistung, dass es Subjekten nicht möglich ist, die zu schützenden Daten unautorisiert und unbemerkt zu manipulieren.
  - Vertraulichkeit ("confidentiality"): Das System sollte keine unautorisierte Informationsgewinnung ermöglichen.
  - Verfügbarkeit ("availability"): Gewährleistung, dass authentifizierte und autorisierte Subjekte nicht in den Funktionen beeinträchtigt werden.
  - Verbindlichkeit ("non repudiation"): Verbindlichkeit und Zuordenbarkeit einer Menge von Aktionen ohne der Möglichkeit der Abstreitbarkeit im Nachhinein.

Teile der Definitionen sind aus dem Buch "IT-Sicherheit von Claudia Eckert, 5. Auflage, Verlag Oldenbourg" entnommen.

Im folgenden sind einige Szenarien gegeben, die eine Verletzung bestimmter Eigenschaften aufzeigen. Bitte nennen Sie die verletze Schutzeigenschaft und ggf. den Teilaspekt.

1. Durch Abhören eines Firmennetzwerkes ist es möglich Passwörter von Mitarbeitern abzufangen.

2. 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.

3. 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.

4. Durch eine Schwachstelle in einer Web Applikation ist es beliebigen (auch nicht registrierten) Nutzern möglich Gästebucheinträge zu verändern.

Aufgabe 3 (Teilertheorie und Modulare Arithmetik).

a) Berechnen Sie:

   i) $7 \mod 2$
   ii) $3^5 \mod 7$
   iii) $4^3 \mod 3$
   iv) $12 \mod 4$

b) Zeigen Sie, dass 429 und 595 teilerfremd sind.

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

$$a \equiv b \mod n \Longrightarrow a \equiv b \mod p \text{ für alle } a, b \in \mathbb{Z}.$$

   Geben Sie ferner ein Beispiel, welches die Gültigkeit der Umkehrung dieser Aussage widerlegt.

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.

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

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

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.

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 Chiffrat c sind Bitstrings der Länge n (d.h. $m, c \in \{0,1\}^n$). Der für die Verschlüsselung notwendige Schlüssel ist folgenermaßen definiert:

- einem Bitstring $k \in \{0,1\}^n$

- einer quadratischen invertierbaren Matrix $M \in \{0,1\}^{n \times n}$
- Funktionen $f_i \colon \{0,1\}^n \to \{0,1\}$ für $i = 1, \ldots, n$

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

(I) Setze $v = M \cdot m$, wobei $v = (v_1, \ldots, v_n)$.

(II) Berechne die i-te Chiffratkomponente $c_i = v_i \oplus f_i(k)$ für $i = 1, \ldots, n$.

Dadurch erhalten Sie das Chiffrat $c = (c_1, \ldots, c_n)$.

Sie haben jetzt folgende Klartext und Chiffrat Paare abgefangen:

m	c
0000	1010
0001	1111
0011	0011
0111	0100
1111	1110

Diese Information genügen um jedes beliebige Chiffrat 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 Chiffrat $c = (0010)$.

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 Schutzziele 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 Emailkommunikation verschlüsselt. PGP (Pretty Good Privacy) ist ein Programm zum Verschlüsseln (und signieren) von Daten und basiert auf einem Public-key (asymetrisches) 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. Gruppennummmer) und Raumnummer.

Bitte beachten Sie, dass es sich bei dieser Aufgabe um eine **Einzelabgabe** handelt und trotz Gruppenabgabe muss jeder individuell diese Nachricht anfertigen und abschicken.

Hausübung 2 (Permutationschiffre und Operationsmodi (1,5 + 1 + 2 Punkte)). In der Vorlesung haben Sie das Konzept der Blockchiffre und verschiedene Operationsmodi (z.B. CBC) kennengelernt.
Wir definieren eine Blockchiffre E, die die Eingabebits permutiert, wobei die Permutation π als Schlüssel fungiert. Die Verschlüsselung sei gegeben durch

$$Enc((b_1, \ldots, b_n), \pi) := (b_{\pi(1)}, \ldots, b_{\pi(n)}),$$

und die Entschlüsselung durch

$$Dec((d_1, \ldots, d_n), \pi) := (d_{\pi^{-1}(1)}, \ldots, d_{\pi^{-1}(n)}).$$

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

b) 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.

c) Gegeben sei eine Sequenz $m_1, m_2, \ldots, m_n$ von Klartexten, die mittels einer beliebigen Blockchiffre im ECB oder CBC-Modus verschlüsselt wird, um eine Sequenz von Chiffraten $c_1, c_2, \ldots, c_n$ 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 $m_1, m_2, \ldots, m_n$ werden durch den Empfänger falsch rekonstruiert, wenn der ECB oder CBC-Modus verwendet wird? Begründen Sie Ihre Antwort.

Hausübung 3 (Kasiski Test (1,5 + 0,5 + 0,5 + 1 Punkte)). Sie haben einen Ciphertext abgefangen und wissen, dass es sich bei der Verschlüsselung um eine Vigenère-Verschlüsselung handelt. Der Ciphertext hat die folgende Form:

```
EckOstgloaUclxatrxmfUclxrvkuikugfqwobxvKdfeywtqxpdbcgkw
CcbomsxxrKdfeywtqxpfhcaxvjclkmubtwafqbgzpdmaafbxvzpjxr
```

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

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

b) Bestimmen Sie die Primfaktorzerlegung für alle gefundenen Differenzen.

c) 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.

d) 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.

Hinweis: Als Hilfsmittel können Sie das unten angegebene Tool verwenden (benötigt Flash um zu funktionieren). Dort können Sie für jeden Buchstaben des Schlüssels getrennt Häufigkeitsanalysen durchführen und sich den Ciphertext für einen Schlüssel entschlüsseln lassen. Sie können auch gerne ein anderes äquivalentes Tool verwenden oder auch die Analyse per Hand durchführen.

http://crypto.interactive-maths.com/kasiski-analysis-breaking-the-code.html