Computersystemsicherheit – Übungsblatt Nr. 1 – Lösung

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.

> **Lösung.**
> Confidentialty (Vertraulichkeit), Integrity (Integrität), Availability (Verfügbarkeit)

b) Was besagt Kerckhoffs-Prinzip?

> **Lösung.**
> Die Sicherheit eines kryptographischen Systems beruht nicht auf der Geheimhaltung des Systems, sondern nur auf der des Schlüssels.

c) Was besagt die funktionale Korrektheit eines symmetrischen Verschlüsselungsverfahren?

> **Lösung.**
> Für alle Nachrichten m und alle Schlüssel k gilt: $Dec(k, Enc(k, m)) = m$.

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 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.

   Lösung.

   Security: Vertraulichkeit ist nicht gewährleistet, wenn das Abhören von sensiblen Daten möglich ist.

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.

   Lösung.

   Beeinträchtigung der *Safety*, da die Verlässlichkeit des Betriebsablaufs gestört ist. Sogar Menschen könnten in Gefahr sein.
   Security: Die Verfügbarkeit kann ebenfalls beeinträchtigt werden, wenn es die einzige Bahn ist und der U-Bahn-Betrieb komplett ausser Betrieb dadurch ist.

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.

   Lösung.

   Security: Die Eigenschaft Verbindlichkeit/Nicht-Abstreitbarkeit wird dadurch verletzt. Der Mitarbeiter, der eigentlich die Buchung durchgeführt hat, löscht die Transaktionen aus dem Buchungsprotokoll.

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

   Lösung.

   Security:

   - Authentizität: Die Web Applikation überprüft nicht, ob die Nutzer berechtigt sind Änderungen durchzuführen.
   - Integrität: Änderungen können durchgeführt werden ohne, dass das Subjekt autorisiert ist.
   - Verbindlichkeit: Könnte gewährleistet sein/bleiben, wenn die Änderungen mit eindeutigen Merkmalen gesichert werden, z.b. IP/Zeit.

Aufgabe 3 (Teilertheorie und Modulare Arithmetik).

a) Berechnen Sie:

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

Lösung.

i) $7 \mod 2 = 1$
ii) $3^5 \mod 7 \equiv 243 \mod 7 = 5$
iii) $4^3 \mod 3 \equiv 64 \mod 3 = 1$
iv) $12 \mod 4 = 0$

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

Lösung.

$429 = 3 \cdot 11 \cdot 13$ und $595 = 5 \cdot 7 \cdot 17$. Da sie keine gemeinsamen Primfaktoren besitzen, sind sie teilerfremd (alternativ mit dem Euklidschen Algorithmus lösbar).

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.

Lösung.

Seien $a, b \in \mathbb{Z}$ beliebig. Aus der Vorlesung ist bekannt, dass $a \equiv b \mod n$ bedeutet, dass $n|(a-b)$. Nach Vorraussetzung gilt $p|n$ und somit auch $p|(a-b)$, woraus $a \equiv b \mod p$ folgt.
Als Gegenbeispiel für die Rückrichtung geht z.B. $n = 6, p = 2, a = 4, b = 2$.

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.

Lösung.

Für die Verschlüsselung gilt: $c := m \oplus k$.
Für die Entschlüsselung gilt: $c \oplus k = m \oplus k \oplus k = m$.

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

Lösung.

$c = 1010\ 1111 \oplus 1111\ 0000 = 0101\ 1111$.

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

Lösung.

Perfekte Sicherheit bedeutet informell, dass das Auftreten eines bestimmten Schlüssels k stochastisch unabhängig davon ist, dass ein bestimmter Klartext vorliegt. D.h. falls ein Verschlüsselungsverfahren perfekt sicher ist dann ist es für einen Angreifer, welcher ein Chiffrat abgefangen hat, nicht möglich irgendwelche statistischen Auffälligkeiten des Klartextraums auszuwerten. Etwas formaler bedeutet dies, dass für alle Klartexte m und Chiffrate c die Gleichung $P[M = m|C = c] = P[M = m]$ gilt.

Das Chiffrat im OTP wird durch bitweises XOR von m und k berechnet, d.h. $c = m \oplus k$. Im Chiffrat kann ein einzelnes Bit c_i den Wert 1 annehmen falls $m_i = 0$ und $k_i = 1$ *oder* falls $m_i = 1$ und $k_i = 0$. Die Bitfolge des Schlüssels ist nach Voraussetzung zufällig und gleichverteilt sind, sind auch die Werte 0 und 1 in m für den Angreifer gleichwahrscheinlich.

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

Lösung.

Mehrfache Anwendung des gleichen Schlüssels führt dazu, dass das OTP unsicher wird. D.h. zwei verschiedene Nachrichten m und m' werden mit dem gleichen Schlüssel verschlüsselt. Wenn wir jetzt die resultierende Chiffrate mit XOR verknüpfen ergibt sich $c \oplus c' = m \oplus k \oplus m' \oplus k = m \oplus m'$. Der Angreifer kann jetzt die Differenz der Klartexte analysieren. Diese zeigen im Gegensatz zu zufälligen Strings deutliche Auffälligkeiten, welche statistisch ausgewertet werden können und somit zur Entschlüsselung beitragen.

OTP wird auch unsicher wenn Sender und Empfänger den Einmalschlüssel nicht geheim austauschen. Ein weiteres Problem tritt auf wenn der Schlüssel nicht zufällig gewählt wird sondern beispielsweise einer bekannten Textpassage entspricht.

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

Lösung.

Erinnern wir uns zuerst an die Wertetabellen für XOR und ODER

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

x	y	$x \vee y$
0	0	0
0	1	1
1	0	1
1	1	1

Betrachten wir nochmals das Bespiel aus Aufgabenteil b) mit $m = 1010\ 1111$ und $k = 1111\ 0000$. Wir berechnen jetzt $c = m \vee k = 1010\ 1111 \vee 1111\ 0000 = 1111\ 1111$. Falls

wir das Chiffrat jetzt entschlüsseln wollen, und wir beim OTP nur das XOR durch ein ODER ersetzen, erhalten wir $c \vee k = 1111\ 1111 \vee 1111\ 0000 = 1111\ 1111 \neq m$. Auf diese Weise funktioniert die Entschlüsselung nicht mehr. Allgemein sehen wir aber auch, dass es insgesamt (solange $k \neq 00000000$) mehrere Klartexte gibt, die auf den selben Chiffretext abbilden und somit eine eindeutige Entschlüsselung unmöglich wird.

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 $c = (0010)$.

Lösung.

Um ein Chiffrat c zu entschlüsseln gilt es den zugehörigen Vektor v zu bestimmen um schließlich den unterliegenden Klartext per $m = M^{-1} \cdot v$ zu berechnen.

Aus dem ersten Klartext und Chiffrat Paar lassen sich die benötigten Funktionswerte bestimmen. Da $m = 0000$ folgt in (I) das $v = 0000$. Damit folgt in (II), dass für jede Komponente gilt: $c_i = v_i \oplus f_i(k) = 0 \oplus f_i(k) = f_i(k)$ für $i = 1, 2, 3, 4$. Einsetzen der Chiffratkomponenten liefert

$$c_1 = f_1(k) = 1 \qquad c_2 = f_2(k) = 0$$
$$c_3 = f_3(k) = 1 \qquad c_4 = f_4(k) = 0$$

Wir berechnen jetzt sukzessive für jedes Klartext und Chiffrat Paar den zugehörigen Vektor v mithilfe der eben bestimmten Funktionswerten. Umstellen der Formel in (II) ergibt $v_i =$

$c_i \oplus f_i(k)$. Wir beginnen mit dem zweiten Chiffrat. Einsetzen der Chiffratkomponenten und Funktionswerte liefert

$$v_1 = c_1 \oplus f_1(k) = 1 \oplus 1 = 0 \qquad v_2 = c_2 \oplus f_2(k) = 1 \oplus 0 = 1$$
$$v_3 = c_3 \oplus f_3(k) = 1 \oplus 1 = 0 \qquad v_4 = c_4 \oplus f_4(k) = 1 \oplus 0 = 1$$

Also haben wir hier $v_{(2)} = 0101$. Analoges rechnen liefert: $v_{(3)} = 1001$, $v_{(4)} = 1110$ und $v_{(5)} = 0100$.
Jetzt gilt es die (4×4) Matrix M zu bestimmen und dafür stellen wir das folgende lineare Gleichungssystem nach (I) auf.

$$\begin{aligned}
a_{11} \cdot m_1 + a_{12} \cdot m_2 + a_{13} \cdot m_3 + a_{14} \cdot m_4 &= v_1 \\
a_{21} \cdot m_1 + a_{22} \cdot m_2 + a_{23} \cdot m_3 + a_{24} \cdot m_4 &= v_2 \\
a_{31} \cdot m_1 + a_{32} \cdot m_2 + a_{33} \cdot m_3 + a_{34} \cdot m_4 &= v_3 \\
a_{41} \cdot m_1 + a_{42} \cdot m_2 + a_{43} \cdot m_3 + a_{44} \cdot m_4 &= v_4
\end{aligned}$$

Wir beginnen mit dem zweiten Klartext $m_{(2)}$ und $v_{(2)}$ erhalten damit das lineare Gleichungssystem:

$$\begin{aligned}
a_{11} \cdot 0 + a_{12} \cdot 0 + a_{13} \cdot 0 + a_{14} \cdot 1 &= 0 \\
a_{21} \cdot 0 + a_{22} \cdot 0 + a_{23} \cdot 0 + a_{24} \cdot 1 &= 1 \\
a_{31} \cdot 0 + a_{32} \cdot 0 + a_{33} \cdot 0 + a_{34} \cdot 1 &= 0 \\
a_{41} \cdot 0 + a_{42} \cdot 0 + a_{43} \cdot 0 + a_{44} \cdot 1 &= 1
\end{aligned}$$

Lösen des linearen Gleichungssystems liefert: $a_{14} = 0$, $a_{24} = 1$, $a_{34} = 0$ und $a_{44} = 1$.
Analoges rechnen mit dem dritten Klartext $m_{(3)}$, $v_{(3)}$ sowie einsetzen der zuvor berechneten Komponenten liefert $a_{13} = 1$, $a_{23} = 1$, $a_{33} = 0$ und $a_{43} = 0$.
Weiter folgt für die restlichen Komponenten: $a_{12} = 0$, $a_{22} = 1$, $a_{32} = 1$, $a_{42} = 1$, $a_{11} = 1$, $a_{21} = 0$, $a_{31} = 1$ und $a_{41} = 0$. Damit erhalten wir folgende Matrix

$$M = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

Wie zu Beginn erwähnt lässt sich der Klartext durch $m = M^{-1} \cdot v$ berechnen. Deshalb müssen wir die Matrix M invertieren (vgl. Gauß Algorithmus) und erhalten

$$M^{-1} = \begin{pmatrix} 1 & -1 & 0 & 1 \\ -1 & 1 & 1 & -1 \\ 0 & 1 & 0 & -1 \\ 1 & -1 & -1 & 0 \end{pmatrix}$$

Um den Klartext für die Chiffre $c = (0010)$ zu berechnen bestimmen wir zuerst die passenden Komponenten für v durch einsetzen in (II) und erhalten $v_1 = 1$, $v_2 = 0$, $v_3 = 0$ und $v_4 = 0$. Multiplizieren von M^{-1} und v liefert den resultierenden Klartext $m = (1101)$.

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.

Lösung.

Zur vollständigen Beschreibung des Systems gilt es nur noch zu zeigen, dass Ver- und Entschlüsselung kommutieren.
$Dec(Enc(b_1, \ldots, b_n, \pi), \pi) = Dec(b_{\pi(1)}, \ldots, b_{\pi(n)}, \pi) = (b_{\pi^{-1}\pi(1)}, \ldots, b_{\pi^{-1}\pi(n)}) = b_1, \ldots, b_n.$

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.

Lösung.

ECB-Mode: Anwenden der Permutationsfunktion auf Blöcke der Länge 3.
$Enc(101010101010, \pi) = 011100011100$

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.

Lösung.

ECB: Electronic Code Book
Erinnern wir uns kurz daran wie man in diesem Modus verschlüsselt und entschlüsselt.

$$\textbf{Verschlüsselung}: \quad c_i = f_k(m_i)$$
$$\textbf{Entschlüsselung}: \quad m_i = f_k^{-1}(c_i)$$

Beim Übertragen von c_1 ist ein Fehler aufgetreten. Diesen Ciphertext bezeichnen wir mit c_1'. Jetzt betrachten wir die Entschlüsselungsoperation um zu bestimmen wie viele Blöcke durch den Empfänger falsch rekonstruiert werden. Es folgt:

$$f_k^{-1}(c_1') = m_1'$$
$$f_k^{-1}(c_2) = m_2$$

Es folgt, dass der Fehler nur m_1 betrifft und der Übertragungsfehler pflanzt sich nicht weiter fort.

CBC: Cipher Block Chaining

Erinnern wir uns kurz daran wie man in diesem Modus verschlüsselt und entschlüsselt.

$$\textbf{Verschlüsselung}: \quad c_i = f_k(m_i \oplus c_{i-1})$$
$$\textbf{Entschlüsselung}: \quad m_i = f_k^{-1}(c_i) \oplus c_{i-1}$$

Beim Übertragen von c_1 ist ein Fehler aufgetreten. Diesen Ciphertext bezeichnen wir mit c_1'. Jetzt betrachten wir die Entschlüsselungsoperation um zu bestimmen wie viele Blöcke durch den Empfänger falsch rekonstruiert werden. Es folgt:

$$f_k^{-1}(c_1') \oplus c_0 = m_1'$$
$$f_k^{-1}(c_2) \oplus c_1' = m_2'$$
$$f_k^{-1}(c_3) \oplus c_2 = m_3$$

Es folgt, dass der Fehler noch den nächsten Block betrifft aber ab dem übernächsten Block keinen Einfluss mehr hat.

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.

Lösung.

Für den Fall, dass bei einer Vigenère-Verschlüsselung im Klartext identische Buchstabenfolgen um ein Vielfaches der Schlüssellänge verschoben sind, werden sie auf identischen Buchstabenfolgen im Ciphertext abgebildet.

Doppeltes 4-Gramm durch doppeltes Vorkommen von "Test" im Klartext:

- UCLX an Stelle 21 und 11, Abstand ist 10.

Doppeltes 10-Gramm durch doppeltes Vorkommen von "Schluessel" im Klartext:

- KDFEYWTQXP an Stelle 65 und 40, Abstand ist 25.

b) Bestimmen Sie die Primfaktorzerlegung für alle gefundenen Differenzen.

Lösung.

Vorkommende Differenzen: $25 = 5 \cdot 5$ und $10 = 2 \cdot 5$.

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.

Lösung.

Der Schlüssel hat wahrscheinlich die Länge 5.

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

Lösung.

Schlüssel: BYTES
Klartext: DerKasiskiTestisteinTestzumbestimmenderSchluessellaengeBeikurzen Schluesselngehtdiesgutdasiesichoftwiederholen