Der Bote

Anmerkungen

- erhöhtes Anforderungsniveau
- vorgesehene Bearbeitungszeit: 150 min

Aufgabe

Im Zeitalter des Absolutismus (17. Jahrhundert) herrscht Ludwig XIV. in Frankreich. Die Kommunikation des Königs mit den Befehlshabern des Militärs und innerhalb des Militärs soll stärker abgesichert werden. Bislang werden wichtige Mitteilungen von einem als vertrauenswürdig geltenden Boten übermittelt, entweder *mündlich* oder mit dem Caesar-Verfahren *verschlüsselt in schriftlicher* Form.

Eine Übermittlung von Ludwig XIV. zum militärischen Oberbefehlshaber läuft wie folgt ab:

Der König lässt von seinem Schreiber eine Mitteilung notieren. Der Schreiber verschlüsselt die Mitteilung nach dem Caesar-Verfahren. Der Berater des Königs wählt unter den Boten einen aus, der dem Oberbefehlshaber bekannt ist. Der Bote nimmt die verschlüsselte Mitteilung und eilt zum Oberbefehlshaber. Nachdem sich der Oberbefehlshaber davon überzeugt hat, dass ihm der Bote bekannt ist, nimmt er die Botschaft entgegen und entschlüsselt sie.

1. Geben Sie eine Definition der grundlegenden Begriffe Vertraulichkeit, Integrität und Authentizität an und erläutern Sie diese Begriffe anhand des Beispiels.
2. Protokolle sollen den geordneten Ablauf einer Kommunikation ermöglichen.

   Arbeiten Sie heraus, inwieweit beim bisherigen Ablauf der Kommunikation der geordnete Ablauf sichergestellt wird.
3. Beschreiben Sie, wie man einen mit dem Caesar-Verfahren verschlüsselten Text ohne Kenntnis des Schlüssels entschlüsseln kann.
4. Bereits im 16. Jahrhundert entwickelte Blaise de Vigenère das nach ihm benannte Verfahren.

   Stellen Sie das Vigenère-Verfahren an einem selbst gewählten Beispiel dar.

   Erklären Sie, wovon die Sicherheit des Verfahrens abhängt.
5. In der Anlage ist der Quelltext für eine Vigenère-Verschlüsselung abgedruckt.

   Erläutern Sie die Funktionsweise der Funktion `vigenere` sowie der zugehörigen Hilfsfunktion anhand der ersten beiden Buchstaben für den Beispielaufruf

   (vigenere '(I N F O R M A T I K) '(H O L Z)) .

   Erklären Sie darüber hinausgehend, wie die wiederholte Anwendung des Schlüsselwortes realisiert worden ist.
6. Es gibt sogenannte schwache Schlüssel, die einen Angriff auf einen damit erstellten Geheimtext vereinfachen. Beim Vigenère-Verfahren sollte der Schlüssel deshalb möglichst keine Buchstabenwiederholungen enthalten.

   Entwickeln und implementieren Sie eine Funktion (ggf. mit weiteren Unterfunktionen), die den Schlüssel entsprechend überprüft.
7. Es gibt mehrere Gründe, das bisherige Verfahren zu verändern. Dazu gibt es eine Reihe von Vorschlägen:

1. Die Boten erhalten einen Dienstausweis.
2. Es werden in Zukunft Mitteilungen nur noch schriftlich übergeben.
3. Der verwendete Schlüssel wird jeden Monat geändert.
4. Als Verschlüsselungsverfahren wird das Vigenère-Verfahren eingeführt.

Bewerten Sie jeden dieser Vorschläge.

Begründen Sie, welcher oder welche Vorschläge umgesetzt werden sollten.

Anlage

Hinweis: statt der Funktion `first` kann `car` benutzt werden.
statt der Funktion `rest` kann `cdr` benutzt werden.

```
1  (define alphabet '(A B C D E F G H I J K L M N O P Q R S T U V W X Y Z))
2
3  ;pos-symbol liefert die Position eines Symbols (Buchstabe) in einer Liste.
4  ;Die Nummerierung beginnt mit 0.
5  ;Ist das Symbol nicht Element der Liste,
6  ;liefert die Funktion als Wert die Länge der Liste + 1.
7  ;Beispielaufruf: (pos-symbol 'C alphabet) --> 2, aber (pos-symbol 'c alphabet) --> 27
8  ;
9  (define (pos-symbol symbol liste)
10   (cond ((null? liste) 1)
11         ((equal? (first liste) symbol) 0)
12         (else (+ 1 (pos-symbol symbol (rest liste))))))
13
14 ;symbol-pos liefert das Symbol, das sich an der n-ten Stelle einer Liste befindet.
15 ;Beispielaufruf: (symbol-pos 4 alphabet) --> E
16 ;Liegt ein Index außerhalb der Liste, wird eine leere Liste zurückgeliefert.
17 (define (symbol-pos index liste)
18   (cond ((null? liste) '())
19         ((= index 0) (first liste))
20         (else (symbol-pos (- index 1) (rest liste)))))
21
22 ;Beispielaufruf (caesar 'A 5) --> F
23 (define (caesar klarzeichen schluessel)
24   (symbol-pos
25    (modulo (+ (pos-symbol klarzeichen alphabet) schluessel) (length alphabet))
26    alphabet))
27
28 ;vigenere-hilf (Hilfsfunktion), da für den Aufruf nicht benutzerfreundlich.
29 ;Beispielaufruf:
30 ;(vigenere-hilf '(I N F O R M A T I K) '(H O L Z) '(H O L Z)) -->
31 ;(P B Q N Y A L S P Y)
32 (define (vigenere-hilf klartextliste schluessel schluesselwort)
33   (cond ((null? klartextliste) '())
34         ((null? schluessel)
35          (vigenere-hilf klartextliste schluesselwort schluesselwort))
36         (else (cons (caesar   (first klartextliste)
37                               (pos-symbol (first schluessel) alphabet))
38                     (vigenere-hilf
39               (rest klartextliste) (rest schluessel) schluesselwort)))))
40
41 ;vigenere erhält einen Klartext als Liste von Symbolen sowie das Schlüsselwort,
42 ;ebenfalls als Liste.
43 ;Beispielaufruf (vigenere '(I N F O R M A T I K) '(H O L Z)) --> (P B Q N Y A L S P Y)
44 (define (vigenere klartextliste schluesselwortliste)
45   (vigenere-hilf klartextliste schluesselwortliste schluesselwortliste))
```

Lösungshinweise

Aufg.	erwartete Leistungen
1	Vertraulichkeit: Nur ausgewählte befugte Personen können die Nachricht lesen. Integrität: Die Nachricht kann während der Übertragung nicht verändert werden. Authentizität: Die Identität des Absenders bzw. die genaue Zuordnung der Absenderadresse ist sichergestellt. Vertraulichkeit wird mit Hilfe des Caesar-Verfahrens hergestellt. (unsicher, siehe 3.) Integrität wird dadurch hergestellt, dass der Bote die Nachricht transportiert und damit schützt. Authentizität wird dadurch hergestellt, dass der Absender und der Empfänger den Boten kennen.
2	Das „Protokoll“ legt zwar den Ablauf der Ver- und Entschlüsselung sowie die Übertragung fest, sieht aber keinerlei Regelungen für den Fall etwaiger Fehler oder Probleme vor. Die Liste der möglichen Fehler ist lang: unbekannter Bote, Bote kommt nicht an, Bote kommt ohne Nachricht an, … Von den oben aufgeführten Aspekten ist nur der Fall geregelt, dass ein unbekannter Bote beim Empfänger ankommt; aber auch in diesem Fall bleibt offen, ob der Sender von dem Ereignis erfährt.
3	Mit der Häufigkeitsanalyse wird der häufigste Buchstabe im Geheimtext bestimmt. Dieser entspricht vermutlich dem häufigsten Buchstaben im Klartext (im Deutschen das ‚E‘), daraus kann die Verschiebung (= Schlüsselbuchstabe) bestimmt werden. Mit Hilfe der Verschiebung kann der Geheimtext entschlüsselt werden. Der Prüfling darf auch die Brute-Force-Methode beschreiben. Er könnte gemeinsam mit 25 weiteren Mitschülerinnen und Mitschüler auf die Idee kommen, dass jeder eine Verschiebung ausprobiert. Des Weiteren könnte er auch allein mit Hilfe der ersten n Buchstaben 26 Verschiebungen ausprobieren, bis etwas Sinnvolles entsteht.
4	Nach der Festlegung des Schlüsselwortes wird der Klartext zyklisch verschlüsselt. Der Klartext wird in Blöcke von der Länge des Schlüsselwortes unterteilt, der erste (zweite, dritte, …) Buchstabe eines Klartextblocks wird mit dem ersten (zweiten, dritten, …) Buchstaben des Schlüsselwortes nach Caesar verschlüsselt. Beispiel: INFORMATIK - HOLZ → PBQNYALSPY Die Sicherheit hängt in erster Linie von dem Verhältnis Klartextlänge zu Schlüsselwortlänge ab. Erstens wird die Bestimmung der Schlüsselwortlänge mit zunehmender Schlüsselwortlänge tendenziell aufwendiger und zweitens liefert die Häufigkeitsanalyse der gleich verschlüsselten Buchstaben mit zunehmender Schlüsselwortlänge immer schlechtere Ergebnisse.

Aufg.	erwartete Leistungen
5	In der Funktion `vigenere-hilf` werden Klartext und Schlüssel zeichenweise abgearbeitet. Dazu wird die Funktion `caesar` aufgerufen, die ein Symbol (ein Klartextzeichen) nach dem Caesar-Verfahren verschlüsselt. Klartext- und Schlüsselbuchstabe (I und H bzw. N und O) werden mit der Funktion `pos-symbol` in Zahlen (8 und 7 bzw. 13 und 14) umgewandelt, addiert und durch die Länge des Alphabets modular geteilt. Die dabei ermittelte Zahl (15 bzw. 1) wird mit der Funktion `symbol-pos` in einen Buchstaben (P bzw. B) umgewandelt. Wenn das Schlüsselwort einmal abgearbeitet worden ist (`null? schluessel`), erfolgt der nächste Aufruf der Funktion `vigenere-hilf` mit dem vollständigen Schlüsselwort als zweitem Parameter. Dies geschieht solange, bis die Bedingung (`null? klartextliste`) erfüllt ist, also der Klartext vollständig abgearbeitet wurde. Der Geheimtext wird zeichenweise aufgebaut. Er entsteht beim Aufstieg aus der Rekursionstiefe, bei dem von unten nach oben zunächst das letzte, dann das vorletzte, usw. und schließlich das erste Geheimzeichen in die anfangs leere Liste mit `cons` vorn eingefügt wird.

6	Der Schlüssel wird zeichenweise abgearbeitet. Jedes Zeichen wird in einer Hilfsfunktion daraufhin überprüft, ob es in dem noch folgenden Teil des Schlüssels enthalten ist. Die Funktion wird beendet, wenn ein Buchstabe doppelt im Schlüssel vorkommt oder das Ende bzw. der letzte Buchstabe des Schlüssels erreicht ist.
	Andere Ansätze sind ebenfalls möglich, hängen von den jeweiligen Vorkenntnissen der Prüflinge ab.
	Mustercode
	
	`1 (define (vorhanden? buchst liste)`
	`2 (cond ((null? liste) #f)`
	`3 ((equal? buchst (first liste)) #t)`
	`4 (else (vorhanden? buchst (rest liste)))))`
	`5`
	`6 (define (test schluessel)`
	`7 (cond ((null? schluessel) #t)`
	`8 ((vorhanden? (first schluessel) (rest schluessel)) #f)`
	`9 (else (test (rest schluessel)))))`
	`10`
	`11 (test '(H O L Z)) ergibt true`
	`12 (test '(H O H L)) ergibt false`

7	1: sinnvoll, dadurch müssen die einzelnen Personen sich nicht vorher schon einmal kennengelernt haben, auch sinnvoll bei Krankheit, aber Fälschungssicherheit ist schwer herzustellen 2: sinnvoll, da ein Bote nicht unter Druck die Information preisgeben kann 3: sinnvoll, um die Folgen etwaiger erfolgreicher Angriffe zeitlich zu begrenzen. Die regelmäßige Änderung eines Schlüssels könnte mithilfe eines Schlüsselwortbuches erfolgen. Das ist relativ aufwändig und anfällig, weil das Schlüsselwortbuch gestohlen werden könnte. Alternativ könnte der Schlüssel auch monatlich durch einen Boten übermittelt werden. Dabei besteht jedoch die Gefahr, dass der Schlüssel abgefangen wird. 4: sinnvoll, da polyalphabetische Verfahren nicht so einfach anzugreifen sind wie monoalphabetische. Alle Aspekte müssen gegeneinander abgewogen werden (insbesondere 1 und 3 erscheinen als umständlich oder schwierig unter den damaligen Verhältnissen). Eine mögliche Entscheidung würde also in erster Linie die Vorschläge 2 und 4 berücksichtigen. Vorschlag 3 könnte in Form eines Schlüsselwortbuches für einen bestimmten Zeitraum berücksichtigt werden.

Aufg.	erwartete Leistungen
	Anmerkung: Darüber hinaus können Einzelaspekte konkretisiert und/oder ergänzt werden wie Länge und andere Eigenschaften des Schlüsselwortes, Versiegelung der Nachricht, …

Quelle: Freie und Hansestadt Hamburg, Behörde für Schule und Berufsbildung, Abituraufgaben Informatik 2014

Zuordnung zu den Prozess-, Inhalts- und Anforderungsbereichen

Aufg.	Prozessbereiche					Inhaltsbereiche					Bewertungseinheiten in Anforderungsbereichen		
	MI	BB	SV	KK	DI	ID	AL	SA	IS	IMG	I	II	III
1				X						X	3	3	
2		X		X						X	4	2	
3				X			X			X	4	3	
4				X			X			X		4	3
5			X	X	X		X				2	5	
6	X					X	X					5	6
7		X								X		3	3
										Summe 50	13	25	12