Programmierkurs
Wintersemester 2020/21
Übungsblatt 04 (30.11.2020)

M.Sc. Laslo Hunhold
Dept. Math./Inf., Abt. Informatik
Universität zu Köln

Abgabe für Rückmeldungen bis zum 07.12.2020 (08:00 Uhr), Besprechung ab dem 07.12.2020.

Aufgabe 04-0 (Textverschlüsselung (Monoalphabetische Substitution))

In dieser Aufgabe beschäftigen wir uns mit einer primitiven Methode der Nachrichtenverschlüsselung. Hierzu betrachtet man bei einer Nachricht (dem „Klartext“) (die der Einfachheit wegen nur aus Kleinbuchstaben besteht, z.B. „hallo welt!“) die einzelnen Buchstaben und überträgt diese vom ursprünglichen Alphabet (dem „Klartextalphabet“) in ein geheimes Alphabet (dem „Geheimalphabet“). Man erhält damit eine verschlüsselte Nachricht (den „Geheimtext“ oder das „Chiffrat“)
Dieses Geheimalphabet sollte möglichst nur denjenigen Personen bekannt sein, die den Inhalt der Nachricht kennen dürfen. Man bezeichnet deshalb das Geheimalphabet auch als „(geheimen) Schlüssel“ dieses Verschlüsselungsverfahrens (monoalphabetische Substitution). Im Folgenden sehen Sie ein Beispiel für ein solches Geheimalphabet.

Klartextalphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
Geheimalphabet	?	!	,	.		9	8	7	6	5	4	3	2	1	0	ü	ö	ä	z	y	x	w

Klartextalphabet	w	x	y	z	ä	ö	ü	0	1	2	3	4	5	6	7	8	9		.	,	!	?
Geheimalphabet	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f	e	d	c	b	a

Auf unsere Nachricht „hallo welt!“ angewendet erhalten wir den Geheimtext „7?330ev 3yb“, und weil die Zuordnung (Klartextalphabet $\leftrightarrow$ Geheimalphabet) eindeutig (bijektiv) ist, können wir den Geheimtext auch wieder eindeutig in den Klartext übertragen, sofern uns das Geheimalphabet bekannt ist. Der Geheimtext an sich bietet aber kaum Aufschluß über den Inhalt der Nachricht und kann so „abhörsicher“ übertragen werden, obgleich hier wiederum anzumerken ist, daß die Abhörsicherheit von der Stärke eines Verfahrens abhängt.
Schreiben Sie ein Programm, welches eine (als `String`) gegebene Nachricht mit diesem Verschlüsselungsverfahren verschlüsselt und wieder entschlüsselt. Geben Sie die ursprüngliche Nachricht, den Geheimtext und den bei der Entschlüsselung erhaltenen Klartext in der Konsole aus. Nutzen Sie hierzu das oben gegebene Geheimalphabet, welches Sie wie folgt im Code als 2x44-`char`-Array ausdrücken können.

```
1  char[][] schluessel = {
2          {
3                  'a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v',
4                  'w', 'x', 'y', 'z', 'ä', 'ö', 'ü', '0', '1', '2', '3', '4', '5', '6', '7', '8', '9', ' ', '.', ',', '!', '?',
5          },
6          {
7                  '?', '!', ',', '.', ' ', '9', '8', '7', '6', '5', '4', '3', '2', '1', '0', 'ü', 'ö', 'ä', 'z', 'y', 'x', 'w',
8                  'v', 'u', 't', 's', 'r', 'q', 'p', 'o', 'n', 'm', 'l', 'k', 'j', 'i', 'h', 'g', 'f', 'e', 'd', 'c', 'b', 'a',
9          },
10 };
```

Hierbei sind die Arrays `schluessel[0]` das Klartext- und `schluessel[1]` das Geheimalphabet.
Hinweis: Wie schon in der Vorlesung gezeigt kann man einen `String s` als Array von `char` interpretieren. Ein direkter Zugriff (i.e. `s[1]`) ist aber nicht möglich, sondern erfolgt mit `s.charAt(1)`. Analog zu „`.length`“ bei Arrays erhält man die Länge eines `String` mit „`.length()`“. Eine alternative Herangehensweise ist „`.toCharArray()`“, welches einen `String` in einen `char[]` umwandelt.

Aufgabe 04-1 (Binäre Kodierung)

Kodieren Sie binär die Zahl 42 als uint8 und int8 und die Zahl -23 als int8.

Präsenzaufgabe 04-2 (Ziffernarray)

Schreiben Sie ein Programm, welches für eine gegebene positive Zahl vom Typ `int` (z.B. `1099`) die Anzahl der Ziffern `ziffern` bestimmt (hier `4`) und die Ziffern in einem Array `z` der Länge `ziffern` vom Typ `int[]` speichert, wobei `z[0]` die höchstwertige Ziffer (hier `1`) und `z[z.length - 1]` die niedrigstwertige Ziffer (hier `9`) enthalten soll (also insgesamt `{1, 0, 9, 9}`). Geben Sie die gegebene Zahl, die Anzahl der Ziffern und die Ziffern in der Kommandozeile aus.

Präsenzaufgabe 04-3 (Verschlüsselte Kommunikation)

Nehmen Sie Ihren Code aus Aufgabe 04-0 und erstellen Sie zusammen mit ausgewählten Partnern Ihr eigenes Geheimalphabet. Verschlüsseln Sie mit Ihrem Programm eigene Nachrichten und geben Sie den Geheimtext an Ihre Partner weiter. Umgekehrt entschlüsseln Sie mit Ihrem Programm die Geheimtexte Ihrer Partner.
Überlegen Sie sich, warum die monoalphabetische Substitution lediglich eine primitive Verschlüsselungsmethode ist, und welche Schwächen sie hat.