1

Einleitung

Visuelle Kryptographie ist ein 1994 von NAOR und SHAMIR [26] erfundenes Verschlüsselungsverfahren, bei dem die Entschlüsselung ohne Computerhilfe vorgenommen werden kann. Um ein Gefühl dafür zu bekommen, worum es dabei geht, drucken Sie die Folien 1 und 2, die Sie auf der Homepage des Buches finden aus. Bei beiden Folien erkennt man nur eine einheitlich graue Fläche (Abbildung 1.1 a, b). Legt man aber beide Folien übereinander so ist deutlich ein Bild (Abbildung 1.1 c) zu sehen.

1, 2

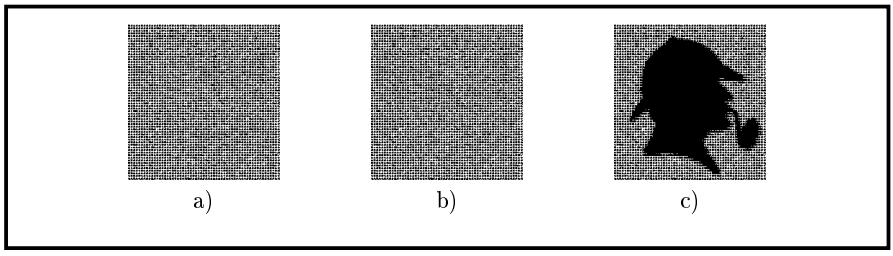


Abb. 1.1: Beispiel für visuelle Kryptographie

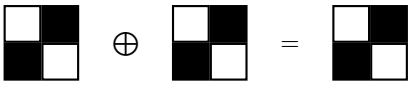
Die Erklärung für diesen Effekt ist überraschend einfach (siehe Konstruktion 1.1 auf der nächsten Seite).

Konstruktion 1.1 liefert uns ein einfaches aber sicheres Verschlüsselungssystem. Im Gegensatz zu „normalen“ Verschlüsselungsverfahren brauchen wir keine komplizierten Berechnungen mit Computern durchführen und müssen auch keine höhere Mathematik wie endliche Körper, elliptische Kurven etc., beherrschen, um das Verfahren zu verstehen. Hier liegt einer der Hauptvorteile der visuellen Kryptographie: Die Verfahren sind leicht einsichtig und man kann große Teile der Kryptographie an ihnen erklären ohne die sonst notwendigen schwierigen Techniken.

Konstruktion 1.1

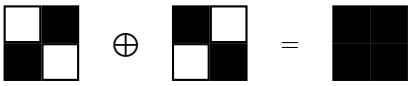
Jeder Bildpunkt des ursprünglichen Bildes wird auf den Folien durch eine Kombination von vier Teilpunkten dargestellt. Dabei wird eine der beiden folgenden Kombinationen benutzt.

Die Kombinationen auf der ersten Folie werden zufällig ausgesucht. Die zweite Folie wird nach den folgenden Regeln gebildet. Soll ein heller Bildpunkt codiert werden, so müssen die Kombinationen auf beiden Folien übereinstimmen. Also etwa:



Beim Übereinanderlegen der Folien entsteht eine Region, in der die Hälfte aller Teilpunkte weiß ist. Dies wird als grau wahrgenommen.

Bei einem dunklen Bildpunkt stimmen die Kombinationen nicht überein.

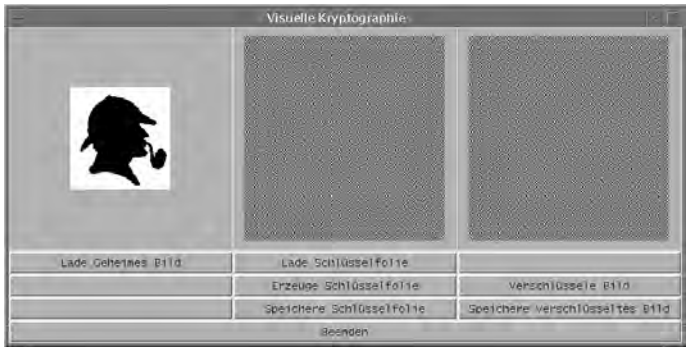


Legt man beide Folien übereinander so werden alle vier Teilpunkte abgedeckt, d.h. man sieht eine schwarze Fläche.

Jemand, der nur eine Folie kennt, sieht lediglich eine zufällige Verteilung von Mustern der Form  bzw.  , aus der er nicht auf das geheime Bild schließen kann. In Kapitel 2 werden wir dies auch formal nachweisen.

Damit Sie die in diesem Buch besprochenen Verfahren bequem selbst ausprobieren können, habe ich für alle Verfahren Beispielprogramme erstellt. Sie können sich von der Homepage des Buches vorgefertigte Pakte für Windows, Mac OS X und Linux herunterladen.

Das Programm **vis-crypt** kann dazu benutzt werden, um ein Paar Folien für visuelle Kryptographie zu erzeugen.



Laden Sie zunächst das geheime Bild. Danach können Sie die Schlüsselfolie erzeugen und das Bild verschlüsseln (die Reihenfolge ist wichtig). Alternativ können Sie statt eine neue Schlüsselfolie zu erzeugen, eine bereits erzeugte laden. Wir werden in Kapitel 3 davon Gebrauch machen.

Sind Sie mit den erzeugten Folien zufrieden, speichern Sie sie ab und bearbeiten sie mit einem Bildbearbeitungsprogramm Ihrer Wahl. (Auf der CD stehen mehrere gute Bildbearbeitungsprogramme zur Auswahl.)

Visuelle Kryptographie kann auch ganz praktische Anwendungen haben, allerdings nur in relativ extremen Fällen. Eine notwendige Voraussetzung für eine Anwendung von visueller Kryptographie ist, dass man die Sicherheit eines modernen Verschlüsselungsverfahren wünscht, aber aus irgendwelchen Gründen gerade keinen Computer zur Verfügung hat, der die Verschlüsselung berechnet. Denn falls man einen Computer zur Hand hat, ist es bequemer ein konventionelles Verschlüsselungsverfahren mit vielen Rechenoperationen zu benutzen. PDAs und Handys zählen in diesem Sinn ebenfalls zu Computern, da sie programmierbare Teile enthalten.

In ihrer ursprünglichen Arbeit schlagen Naor und Shamir ein verschlüsseltes Fax als Beispiel vor (für den Fall, dass wir ein Faxgerät, aber keinen Laptop mit E-Mail-Anschluss besitzen). Im Prinzip könnte man auch ein Fax-Gerät mit einem speziellen Verschlüsselungschip ausstatten. Dies erfordert aber Modifikationen an der Hardware und ist daher teuer und (für seltene Anwendung) weniger praktisch als visuelle Kryptographie.

Es gibt jedoch noch andere Anwendungen.

Man stelle sich die folgende Situation vor. Nach einigen Einkäufen mit der Geldkarte stellt man überrascht fest, dass mehrere Hundert Euro zu viel von der Karte abgebucht wurden. Eine genauere Überprüfung zeigt, dass der Zigarettenautomat um die Ecke statt jeweils 5€ immer 50€ für eine Schachtel verlangt haben muss. Dummerweise ist die Zahlung mit einer Geldkarte anonym und da der Automatenbetreiber schlau genug war den manipulierten Automaten auszutauschen, bevor der Betrug entdeckt wurde, kann der Betrug im Nachhinein nicht mehr nachgewiesen werden. Der Betrogene bleibt auf seinem Schaden sitzen. Obwohl ein solcher Betrug bisher noch nicht vorgekommen ist, wäre er durchaus möglich. (Einer der Hauptgründe für das bisherige Ausbleiben dieses Betrugs dürfte der relativ hohe Aufwand für den Betrug sein. Bisher haben die Betrüger immer noch leichtere Varianten gefunden.) Das Problem liegt darin, dass die Bezahlung mit einer Geldkarte am Automaten ähnlich ist, als würde man dem Verkäufer an einer Kasse seinen Geldbeutel geben, damit er sich den fälligen Betrag selbst nimmt ohne ihn dabei zu kontrollieren. Die Unsicherheit dieses Vorgehens ist augenfällig. Was kann man also tun, um das Bezahlsystem sicherer zu gestalten?

Eine mögliche Lösung wäre statt anonymer Geldkarten Kreditkarten zu verwenden, bei denen alle Transaktionen protokolliert werden. Die Möglichkeiten den Kunden zu betrügen wären bei diesem Vorgehen für unseriöse Automatenhersteller stark eingeschränkt. Allerdings ist aus Datenschutzgründen

ein solches Vorgehen, das einen „gläsernen Kunden“ schafft, nicht wünschenswert.

Eine andere Lösung setzt visuelle Kryptographie ein. Als Zubehör zur Kreditkarte erhalten wir eine etwa scheckkartengroße Folie, auf der eine zufällige Verteilung der beiden Muster ▚ bzw. ▞ abgedruckt ist. Die Verteilung der beiden Muster auf der Folie ist der Kreditkarte bekannt und muss vor dem Rest der Welt geheimgehalten werden. Wenn der Automat einen Betrag abbuchen möchte, schickt er diesen an die Kreditkarte. Diese berechnet gemäß Konstruktion 1.1 passend zu dem Muster der Folie ein Bild, das der Automat anzeigen soll.

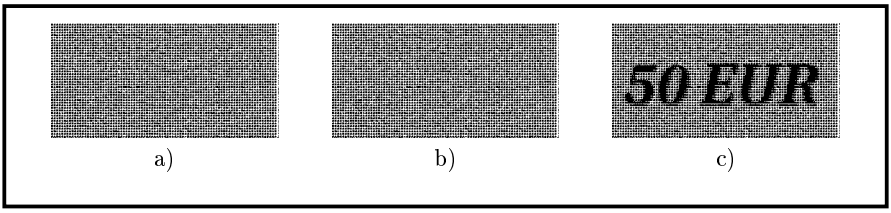


Abb. 1.2: Die Anzeige des Automaten

Zum Beispiel könnte die Folie das Muster aus Abbildung 1.2 a enthalten. Der Automat möchte 50€ abbuchen. Das von unserer Karte berechnete Muster sehen wir in Abbildung 1.2 b und in Abbildung 1.2 c sehen wir die Anzeige, nach dem wir unsere Folie auf das Display des Automaten gelegt haben. Sind wir mit dem angezeigten Betrag einverstanden, bestätigen wir die Transaktion indem wir unsere Kreditkarte tiefer in den Eingabeschlitz des Automaten schieben.

Da der Automat nur ein zufälliges Punktmuster anzeigen soll, weiß er nicht welches Bild wir durch unsere Folie sehen werden. Wir können uns daher darauf verlassen, dass wir genau das Bild sehen, das uns unsere Kreditkarte zeigen möchte. Wir sind also vor einem Betrug durch den Automaten perfekt geschützt. Oder etwa doch nicht? Es stimmt zwar, dass das Punktmuster, das der Automat anzeigen soll, alleine keine Information über das geheime Bild liefert (was wir in Kapitel 2 auch formal zeigen werden). Aber der Automat weiß ja bereits welche Anzeige zu erwarten ist, denn er hat selbst unserer Kreditkarte den Betrag, den sie verschlüsseln soll genannt. Würde die Kreditkarte immer die gleiche Schriftart und immer die gleiche Position im Bild für den Text benutzen, so könnte ein betrügerischer Automat das geheime Bild erraten und seine Anzeige gezielt abändern, um dem Benutzer ein falsches Bild als echt unterzuschieben (siehe Aufgabe 1.1). Um ein sicheres System zu erhalten, muss die Karte den Text auf unvorhersehbare Weise auf dem Bildschirm des Automaten positionieren. In Kapitel 3 werden wir genauer auf die Sicherheit dieses Verfahrens eingehen.

Zugegebenermaßen ist dies ein sehr hoher Aufwand, aber abgesehen von dem Einbau eines kleinen Displays in die Geldkarte ist dies die einzige Möglichkeit, wie man der Anzeige wirklich vertrauen kann. Vermutlich wird man also die bequeme Lösung wählen und das Display des Automaten ohne Sicherung benutzen. In der Regel geht dies gut, da die meisten Leute ehrlich sind. Die Betrugsfälle werden dann als Preis für die Bequemlichkeit verbucht.

Die Möglichkeiten, die in der visuellen Kryptographie liegen, sind mit den oben genannten Beispielen noch lange nicht erschöpft. Dieses Buch soll die verschiedenen Möglichkeiten der visuellen Kryptographie vorstellen. Der Schwerpunkt liegt dabei weniger auf den konkreten Anwendungen, sondern den allgemeinen Prinzipien.

Bevor wir jedoch visuelle Kryptographiesysteme genauer studieren können, müssen wir einige Grundlagen der Kryptographie lernen. Dies wird das Ziel dieses und des nächsten Kapitels sein.

1.1 Ziele der Kryptographie

Das Wort *Kryptographie* kommt aus dem Griechischen von $\kappa\rho\upsilon\pi\tau o\sigma$ (geheim) und $\gamma\rho\alpha\varphi\epsilon\iota\nu$ (schreiben) und bezeichnet alle Methoden der Verschlüsselung. Dabei soll eine Nachricht so verändert werden, dass es für einen Unbefugten praktisch unmöglich wird den Inhalt zu entziffern. Der befugte Empfänger, der den speziellen *Schlüssel* kennt, kann die Nachricht jedoch ohne Schwierigkeiten lesen.

Im Grundmodell der Kryptographie will Alice (der *Sender*) Bob (dem *Empfänger*) eine Nachricht zukommen lassen. Dazu einigen die beiden sich auf einen gemeinsamen *Schlüssel* S und ein *Verschlüsselungsverfahren* V. Heute ist S in der Regel eine lange und zufällige Folge von Nullen und Einsen (eine typische Länge ist 128) und V ein Computerprogramm. In dem folgenden Abschnitt werden wir einige einfache Beispiele für Verschlüsselungsverfahren kennenlernen. Für den Moment reicht es aber zu wissen, dass V_S eine Funktion ist, die einer lesbaren Nachricht (dem *Klartext*) K einen *Geheimtext* G zuordnet. Wenn Alice Bob eine Nachricht K schicken möchte, berechnet sie den Geheimtext $G = V_S(K)$ und schickt G an Bob. Bob kennt das zugehörige Entschlüsselungsverfahren E und kann $K = E_S(G)$ berechnen.

Das einfachste mögliche *Angriffsszenario* ist das folgende: Christine kennt den gemeinsamen Schlüssel von Alice und Bob nicht. Das Verschlüsselungsverfahren und das Entschlüsselungsverfahren sind ihr jedoch bekannt. Weiterhin ist es Christine möglich, die Sendung von Alice an Bob zu belauschen, d.h. Christine kennt den Geheimtext G. Ein gutes Verschlüsselungsverfahren muss sicherstellen, dass Christine unter diesen Umständen nicht von dem Geheimtext G auf den Klartext K schließen kann.

Es gibt jedoch noch viele weitere Möglichkeiten für einen Angreifer, z.B. könnte Christine versuchen, den Geheimtext G durch einen anderen Geheimtext G' zu ersetzen, ohne dass Bob diese Veränderung bemerkt. Dies kann sehr

drastische Konsequenzen haben. Stellen Sie sich z.B. ein System zum Online Banking vor, bei dem ein Angreifer zwar nicht in der Lage ist, die getätigte Überweisung zu lesen, aber trotzdem jederzeit den überwiesenen Betrag verzehnfachen kann. Ein solches System würde niemand benutzen wollen. (Ein anderes Beispiel für einen solchen Angriff finden Sie in Aufgabe 1.1) Um sich gegen solche *aktiven Angreifer* zu schützen, werden in der modernen Kryptographie zusätzlich zu den klassischen Verfahren zur Nachrichtensicherheit auch Verfahren zur Identitätskontrolle usw. untersucht. Die klassischen Verschlüsselungsverfahren machen daher nur noch einen Teil der Kryptographie aus.

In antiken Verfahren wurde nicht streng zwischen Schlüssel und Verschlüsselungsverfahren unterschieden. Doch es gibt einen wesentlichen Unterschied. Das Verschlüsselungsverfahren ist relativ groß. Zum Beispiel umfasst die Spezifikation von AES (advanced encryption standard), ein heute oft eingesetzten Verfahren, 45 Seiten (worin allerdings auch Tipps zur effizienten Implementierung usw. enthalten sind). Der Schlüssel ist jedoch relativ kurz (z.B. ein Passwort). Dadurch ergibt sich, dass es sehr schwer ist das Verschlüsselungsverfahren selbst geheimzuhalten. Die verwendete Maschine oder das entsprechende Programm sind sehr leicht zu stehlen. Die Erfahrung hat uns gelehrt, dass ein entschlossener Gegner früher oder später (meistens früher) das Verschlüsselungsverfahren kennenlernt. Zum Beispiel konnten im zweiten Weltkrieg die Alliierten mehrere Exemplare der von den Deutschen eingesetzten Verschlüsselungsmaschine ENIGMA erbeuten. Die erfolgreiche Analyse des Verfahrens ermöglichte das Knacken der verschlüsselten deutschen Funksprüche. Die so gewonnenen Informationen haben den Kriegsverlauf wesentlich zugunsten der Engländer beeinflusst [18].

Daraus ergibt sich die Forderung die als *Prinzip von Kerckhoff* (1835 – 1903) bekannt ist:

> Die Sicherheit eines Verschlüsselungsverfahrens darf nicht von der Geheimhaltung des Verfahrens selbst, sondern nur von der Geheimhaltung des Schlüssels abhängen.

Heute werden Verschlüsselungsverfahren daher in aller Regel öffentlich vorgestellt und in Fachkreisen diskutiert. Zum Beispiel haben bei der Entwicklung des aktuellen AES-Verfahrens 15 Forscherteams je einen Algorithmus vorgeschlagen. Von diesen 15 Vorschlägen haben sich fünf als fehlerhaft erwiesen (d.h. die Verfahren wurden mindestens teilweise gebrochen). Weitere fünf wurden aus allgemeinen Überlegungen verworfen, ohne dass ein Fehler gefunden worden wäre. Die restlichen fünf Verfahren sind alle gut und werden auch heute eingesetzt. Dieser öffentliche Auswahlprozess stärkt das Vertrauen der Benutzer in das System. (Es gibt immer wieder Leute, die denken, dass sie eine höhere Sicherheit erreichen könnten, wenn sie zusätzlich zum Schlüssel auch das Verschlüsselungsverfahren geheim halten. Dies hat bisher jedoch noch niemals funktioniert. Das Verfahren wird immer früher oder später allgemein bekannt. Der Versuch es anfangs geheimzuhalten ist also im besten

Fall nutzlos, in der Regel führt er jedoch zu einem schlampig entworfenen und daher unsicheren Verfahren. Ein Beispiel aus der jüngeren Vergangenheit bietet die in Mobiltelefonen eingesetzte Verschlüsselung, wo der Verstoß gegen das Prinzip von Kerckhoff zu einem schwachen Verfahren geführt hat [5, 2].)

1.2 Einfache Kryptosysteme

1.2.1 Die Cäsar-Chiffre

Eine der frühsten bekannten Anwendungen von Kryptographie finden wir bei dem römischen Feldherren Julius Cäsar (100 – 44 v.Chr.). Bei Sueton lesen wir

> *Exstant et [epistolae] ad Ciceronem, item ad familiares de rebus, in quibus, si qua occultius perferenda erant, id est sic structo litterarum ordine, ut nullum verbum effici poset; quae si qui investigare et persequi velit, quartam elementorum litteram, id est D pro A et perinde reliquas commutet.*

Auf deutsch

> Es existieren auch [Briefe von Cäsar] an Cicero und an Bekannte über Dinge, in denen er, wenn etwas vertraulich übermittelt werden musste, in Geheimschrift schrieb. D.h. er veränderte die Ordnung der Buchstaben derart, dass kein einziges Wort mehr ausgemacht werden konnte. Wenn jemand das entziffern und den Inhalt erkennen wollte, so musste er den vierten Buchstaben des Alphabets, also D nach A umwandeln und auf gleiche Weise mit den anderen [Buchstaben verfahren].

Die Verschlüsselungsfunktion ist also durch die folgende Tabelle gegeben. (Hier wie auch in allen folgenden Beispielen werden wir zur besseren Unterscheidung Kleinbuchstaben für den Klartext und Großbuchstaben für den Geheimtext verwenden.)

Klartext	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
Geheimtext	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Cäsar hat bei seiner Chiffre noch nicht zwischen Schlüssel und Verschlüsselungsverfahren unterschieden. Allerdings lässt sich sein Verfahren leicht verallgemeinern. Das Verschlüsselungsverfahren ist eine beliebige zyklische Verschiebung des Alphabets. Der Schlüssel ist das Geheimtextäquivalent zu `a`. Das Cäsar-Verfahren ist also eine *Verschiebechiffre* mit Schlüssel `D`.

Verschiebechiffren sind so einfach, dass es verwunderlich erscheint, dass sie jemals ausreichende Sicherheit geboten haben. Es gibt immerhin nur 26 mögliche Schlüssel. (Wenn wir die „Verschlüsselung“ $a \to A$, $b \to B$, …, $z \to Z$ nicht mitzählen wollen, sind es sogar nur 25 Schlüssel.) Selbst per

Hand ist es kein Problem sämtliche Schlüssel nacheinander auszuprobieren und so den Klartext zu finden.

Eine Grundforderung an jedes Kryptosystem muss daher sein, dass die Anzahl der möglichen Schlüssel so groß ist, dass das Durchprobieren aller Schlüssel zu lange dauert. Bei der momentan verfügbaren Rechenleistung wären etwa 2^{80} mögliche Schlüssel ausreichend. Vorsichtshalber nimmt man jedoch 128-Bit Schlüssel (2^{128} Möglichkeiten) oder, wenn man ganz sicher sein will, 256-Bit Schlüssel.

Verschiebechiffren haben sogar eine Schwäche, die es dem Angreifer erlaubt, ohne Raten den richtigen Schlüssel zu finden. Im Deutschen (wie auch in den meisten anderen europäischen Sprachen) ist `e` der mit Abstand häufigste Buchstabe. Auch bei kurzen Texten von etwa 50 Zeichen wird man Mühe haben ein Beispiel zu finden, in dem `e` nicht der häufigste Buchstabe ist.

Diese Beobachtung erlaubt uns einen sehr effizienten Angriff auf mit der Cäsar-Verschlüsselung erzeugte Texte.

Beispiel

Man betrachte den Geheimtext:

```
MRNBNACNGCRBCWRLQCPNQNRV
```

Der häufigste Buchstabe im Geheimtext ist das `N` (fünfmaliges Auftreten). Wir raten daher, dass das `N` im Geheimtext für `e` steht. Dies würde bedeuten, dass die Verschlüsselung eine Verschiebung von 9 Zeichen nach rechts ist. Wir entschlüsseln den Text unter dieser Annahme und erhalten:

```
Dieser Text ist nicht geheim
```

Unsere Vermutung war also richtig.

Selbstverständlich können wir insbesondere bei sehr kurzen Texten nicht erwarten, dass `e` immer der häufigste Buchstabe ist. Im obigen Beispiel sind die Buchstaben `C` und `R` (jeweils vierfach vorhanden) auch sehr häufig. Auf Grund ihrer Häufigkeit wären auch diese Buchstaben naheliegende Kandidaten für `e`.

Erstaunlicherweise gibt es eine alte literarische Tradition, deren Ziel es ist Texte zu verfassen, in denen ein bestimmter Buchstabe nicht vorkommt. Solche Texte werden *lipogrammatisch* oder *leipogrammatisch* genannt. Diese Tradition geht angeblich auf den Griechen Lasos (um 550 vor Chr.) zurück, der das Sigma wegen seines Zischlautes vermeiden wollte. Lipogrammatische Werke waren schon immer eine Herausforderung an Schriftsteller, so wurden schon im Altertum ernste Versuche unternommen, die Ilias und die Oddysee lipogrammatisch umzuschreiben, so dass im ersten Kapitel das A, im zweiten Kapitel das B und schließlich im letzten Kapitel das Ω fehlt. Der Höhepunkt lipogrammatischer Literatur ist zweifellos der 1969 auf französisch erschienene Roman *La Disparition* von George Perec [27], der ganz ohne `e` auskommt (bei immerhin über 300 Seiten)! Dieser Roman wurde von Eugen Helmlé lipogrammatisch ins Deutsche übersetzt was eine mindestens ebenso große Leistung ist. Wer sich für lipogrammatische Literatur interessiert sei auf das hervorragende Nachwort des Übersetzers verwiesen.

1.2.2 Die Vigenère-Chiffre

Die Probleme der Cäsar-Verschlüsselung (zu wenig mögliche Schlüssel, Buchstabenhäufigkeiten verraten das Geheimtextäquivalent von `e`) motivieren die folgende Chiffre, die nach dem französischen Diplomaten BLAISE DE VIGENÈRE (1523 – 1596) benannt wurde.

Konstruktion 1.2

Man wähle ein Schlüsselwort, z.B. `GEHEIM`. Wenn man einen Text verschlüsseln will, schreibt man das Schlüsselwort Buchstabe für Buchstaben über den Klartext, so lange bis man die Länge des Klartextes erreicht hat, z.B.

```
GEHEIMGEHEIMGEHEIMGEHEIMGEHEIMGE
diesisteinesehrwichtigenachricht
```

Nun werden die Buchstaben des Klartextes wie bei einer Verschiebechiffre verschlüsselt. Nur anstelle der immer gleichen Verschiebung gibt nun der zugehörige Buchstabe des Schlüsselworts die Weite der Verschiebung an.

Im Beispiel muss an der ersten Stelle das Alphabet um 6 Buchstaben nach hinten verschoben werden (`a`→`G`, ...), d.h. dem Klartextzeichen `d` entspricht das Geheimtextzeichen `J`. Entsprechend wird an der zweiten Stelle das Alphabet um 4 Zeichen verschoben (`a`→`E`, ...), so dass wir `i` durch `M` verschlüsseln.

```
JMLWQEZIPRMEKLYAQONXPKMZGGOVQONX
```

Um sich die Arbeit etwas zu erleichtern, erzeugt man sich vor der Verschlüsselung das Vigenère-Tableau (Abbildung 1.3).

Mit Hilfe des Vigenère-Tableaus kann man verschlüsseln, indem man in der Zeile, die durch den Klartextbuchstaben, und der Spalte, die durch den Buchstaben des Schlüsselworts bestimmt wird, den zugehörigen Geheimtextbuchstaben nachschlägt. Die Arbeit ist ganz mechanisch und kann von einem geübten Benutzer sehr schnell erledigt werden. (Dies war vor der Erfindung der Computer ein sehr wichtiges Kriterium. Verschlüsselungsverfahren mussten für Hilfskräfte, die zum Teil nicht einmal lesen konnten, durchführbar sein. Heute wählt man entsprechend Verfahren aus, die für die verfügbare Hardware möglichst einfach zu bewältigen sind.)

Die Vigenère-Verschlüsselung behebt viele Probleme der Cäsar-Verschlüsselung. Zum einen gibt es, selbst wenn man nur kurze Schlüsselwörter zulässt, eine große Anzahl von Schlüsseln (z.B. gibt es $26^5 = 11881376$ Schlüsselwörter mit fünf Buchstaben), sodass ohne Computer ein Ausprobieren aller Schlüssel unmöglich ist. Zum anderen kann je nach Position im Geheimtext das gleiche Geheimtextzeichen für verschiedene Klartextzeichen stehen (im Beispiel steht `G` einmal für `a` und einmal für `c`). Schlussendlich wird ein Klartextzeichen je nach Position durch verschiedene Geheimtextzeichen verschlüsselt (im Beispiel sind sowohl `G` als auch `O` Geheimtextäquivalente für `c`). Eine einfache Analyse der Buchstabenverteilung, wie bei der Cäsar-Chiffre, wird uns daher nicht helfen.

	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
a	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
b	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	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	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

Abb. 1.3: Das Vigenère-Tableau

Trotzdem genügt die Vigenère-Verschlüsselung nicht einmal annähernd modernen Sicherheitsstandards. Der einfachste Angriff setzt voraus, dass dem Angreifer die Länge des Schlüsselworts bekannt ist. Nehmen wir zum Beispiel an, wir wüssten schon, dass ein Schlüsselwort der Länge sechs verwendet wurde. Dann betrachten wir nur jeden sechsten Buchstaben des Geheimtextes. Da an diesen Stellen immer dasselbe Schlüsselzeichen verwendet wurde, entspricht der entsprechende Geheimtext einer Cäsar-Verschlüsselung. Wir können also durch Auswerten der Buchstabenhäufigkeit das Geheimtextäquivalent von `e` und damit auch den Schlüsselbuchstaben bestimmen. Auf diese Weise erhält man das gesamte Schlüsselwort, d.h. die Chiffre ist gebrochen. (In Aufgabe 1.3 können Sie diesen Angriff an einem Beispiel selbst durchführen.)

Damit haben wir das Brechen einer Vigenère-Verschlüsselung auf das Brechen von (im Beispiel sechs) Cäsar-Verschlüsselungen zurückgeführt. Als einziger Vorteil bleibt, dass ein Angreifer mehr Geheimtext kennen muss, um

eine Vigenère-Verschlüsselung zu brechen. Denn wenn man etwa 20 bis 30 Geheimtextzeichen braucht, um eine Cäsar-Verschlüsselung durch Analyse der Buchstabenhäufigkeit zu brechen, so braucht man bei einer Vigenère-Verschlüsselung mit Schlüsselwortlänge n etwa $20n$ bis $30n$ Geheimtextzeichen, um den oben beschriebenen Angriff erfolgreich durchzuführen. Bei plausiblen Schlüsselwortlängen kann man daher davon ausgehen, dass es sehr schwer ist einen Vigenère verschlüsselten Geheimtext von deutlich unter 100 Zeichen zu brechen. Von dieser Beobachtung kommt die alte Empfehlung, verschlüsselte Nachrichten möglichst kurz zu halten. Bei modernen Verfahren bedeutet kurz in der Regel irgend etwas zwischen einem Gigabyte (10^9 Zeichen) und mehreren Tausend Terabytes (10^{12} Zeichen) je nach verwendeten Verfahren. In aller Regel sind Nachrichten wesentlich kürzer aber bei wirklich langen Nachrichten sollte man die Nachricht in mehrere kurze Blöcke unterteilen und für jeden Block einen eigenen Schlüssel benutzen.

Wie kann der Angreifer die Länge des Schlüsselworts ermitteln? Dafür gibt es mehrere Möglichkeiten. Zum einem kann man einfach raten. Da das Schlüsselwort wahrscheinlich höchstens zehn Zeichen lang ist, muss man nur wenige mögliche Längen durchprobieren bis man Erfolg hat. Aber man kann auch durch Analyse des Geheimtextes die Schlüsselwortlänge direkt bestimmen. Entsprechende Angriffe wurden von KASISKI und FRIEDMAN (um 1900) veröffentlicht. Da diese Angriffe für die folgenden Erörterungen nicht notwendig sind, geben wir hier keine Details, sondern verweisen auf gängige Einführungsliteratur (z.B. das schöne Büchlein [4], Kapitel 2.3).

Ein anderes Problem der Vigenère-Verschlüsselung betrifft ihre Schwäche gegen einen *Angriff mit bekanntem Klartext*. Dabei ist dem Angreifer von vornherein ein Teil des Klartextes bekannt. Dies kommt häufiger vor als man zunächst denkt. Zum Beispiel spricht vieles dafür, dass eine geheime Nachricht die von einem gegnerischen U-Boot gesendet wurde, Wörter wie U-Boot oder Schiff enthält. Hat der Angreifer erst einmal ein solches Wort erfolgreich geraten, ist die Verschlüsselung so gut wie gebrochen (siehe Aufgabe 1.4). Bei der Untersuchung moderner Verschlüsselungsverfahren nimmt man in der Regel sogar an, dass der Angreifer in der Lage ist zu jedem von ihm *gewählten* Klartext den passenden Geheimtext zu erfahren. (In unserem einführenden Beispiel mit dem Automaten und der Kreditkarte ist genau dies der Fall.) Die Idee hinter solchen Annahmen ist, dass ein Verfahren, dass einen gut informierten Angreifer abwehren kann, einen schwächeren Angreifer nur um so sicherer abwehrt. Außerdem hat die Erfahrung gezeigt, dass ein Angriff mit einem bekannten oder gewählten Klartext oft so modifiziert werden kann, dass er auch ohne bekannten Klartext funktioniert. Wir werden in Abschnitt 3.4.1 ein Beispiel dafür sehen. Verfahren, die einen Angriff mit einem gewählten Klartext nicht abwehren können, gelten daher heute als unbrauchbar.

Die obigen Schwächen der Vigenère-Verschlüsselung haben in der Vergangenheit zu mehreren Verbesserungsvorschlägen geführt. Dabei ging es darum, möglichst lange Schlüsselwörter zu generieren. Eine dieser Varianten geht wie folgt: Sender und Empfänger einigen sich vorab auf ein Buch, das beiden be-

kannt ist (z.B. Bibel, Genesis). Danach können beide jeden noch so langen Text mit dem folgenden „Schlüsselwort“ verschlüsseln.

> *Am Anfang schuf Gott Himmel und Erde. Und die Erde war wüst und leer, ...*

Angriffe, die auf ein kurzes sich wiederholendes Schlüsselwort ziehlen, versagen an dieser Stelle. (Aber Vorsicht, die Bibel ist ein sehr bekanntes Buch! Vieleicht errät ein Angreifer ihren Schlüssel, nehmen Sie lieber ein etwas weniger bekanntes Werk.) Dieses Verfahren ist jedoch immer noch nicht sicher, wie wir in Abschnitt 3.4.1 sehen werden. Erstaunlicherweise gibt es jedoch immer wieder moderne Anwendungen, bei denen dieser klassische Angriff mit Erfolg angewandt werden kann. Es lohnt sich also diese Variante der Vigenère-Verschlüsselung genau zu studieren.

Der Fehler in dem vorhergehenden Verfahren war, dass das Schlüsselwort noch immer ein sinnvoller Text sein musste. Daher wählen wir als nächste Verbesserung eine zufällige Folge von Buchstaben, die mindestens so lang wie der zu verschlüsselnde Text ist, als „Schlüsselwort“. Im nächsten Kapitel werden wir zeigen, dass es unmöglich ist diese, als One-Time-Pad bekannte, Vigenère-Variante zu brechen. Allerdings ist dieses Verfahren sehr unpraktisch. Da der Schlüssel ebenso lang wie die Nachricht ist, ist der sichere Transport des Schlüssels vom Sender zum Empfänger fast ebenso schwer wie der Transport der Nachricht selbst. Als einziger Vorteil bleibt, dass Sender und Empfänger den Zeitpunkt des Schlüsselaustausches selbst bestimmen können, während normalerweise nicht beeinflussbare äußere Umstände den Zeitpunkt, zu dem die Nachricht gesendet werden muss, bestimmen. Dieses Problem des *Schlüsselaustausches* ist der Grund dafür, dass dieses absolut sichere Verfahren in der Praxis nur selten eingesetzt wurde.

Die Grundidee der Vigenère-Verschlüsselung

> „Verwende für jedes Zeichen eine sehr einfache Verschlüsselung mit nur wenigen möglichen Schlüsseln, aber wechsle den Schlüssel bei jedem neuen Zeichen.“

ist trotz allem auch heute noch aktuell. Die modernen Nachfolger der Vigenère-Verschlüsselung heißen *Strom-* oder *Flusschiffren* und einige der schnellsten modernen Verschlüsselungsfunktionen gehören zu dieser Klasse. Als Grundbaustein werden nicht länger Buchstaben und Verschiebechiffren, sondern Bits und die XOR-Operation (exklusives Oder, $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$, $1 \oplus 1 = 0$) genommen. Da $(x \oplus s) \oplus s = x$ gilt und es nur zwei mögliche Schlüssel gibt ($s = 0$ oder $s = 1$), ist die Grundstruktur noch einfacher als beim klassischen Vigenère-Verfahren. Natürlich darf man bei einer Stromchiffre nicht einfach kurze Folgen von 0 und 1 periodisch wiederholen, sondern man muss eine möglichst zufällig wirkende Folge von 0 und 1 erzeugen. Die modernen Stromchiffren unterscheiden sich in den Algorithmen, die so eine Pseudozufallsfolge erzeugen. Wir werden in Abschnitt 3.3 genauer darauf eingehen.

Auch bei dem Verfahren zur visuellen Kryptographie, das wir am Anfang des Kapitels besprochen haben, ist die Verschlüsselung eines einzelnen Bildpunktes sehr einfach. Hier gibt es nur zwei mögliche Schlüssel nämlich und  . Die Sicherheit des Verfahrens wird erst dadurch erreicht, dass man für jeden Bildpunkt eine neue zufällige Kombination wählt. Damit ist visuelle Kryptographie auch ein moderner Nachfolger der Vigenère-Verschlüsselung.

Aufgaben

1.1 Wir nehmen an, dass in dem Beispiel mit der Kreditkarte und dem Automaten die Karte immer dieselbe Schrift benutzt, um den Betrag zu codieren. Dies führt dazu, dass der Automat das verschlüsselte Bild erraten kann.

Wie kann der Automat unter diesen Umständen auf die geheime Folie schließen? Welche Möglichkeit zum Betrug eröffnet sich damit?

1.2 Die folgenden zwei Texte wurden mit einer Verschiebechiffre verschlüsselt.

(a) `MVIJTYZVSVTYZWWIVE JZEU EZTYK JZTYVI.`
(b) `EZOUO!`

1.3 Entschlüsseln Sie den folgenden Vigenère-verschlüsselten Text. (Das Schlüsselwort hat die Länge 4.)

```
IIVV SIUR ZWKU QRAV ZHLN HSVM GYMO QVHR GKMA PEAF
QWSR URON ZDTR UGPG QWQF FIQA QQMG TSLR PIZT QLMV
YWKU DMNG LYNV ZHMA PMMQ QVMA FWKU XYMF EITH ZKBE
AXHG
```

1.4 Der folgende Geheimtext wurde mit einer Vigenère-Verschlüsselung erzeugt. Wir vermuten, dass der Klartext mit `komme` beginnt.

```
WCZFE SAFTX NFGAI XRKUB OTRZQ BGKEL RDHGK Z
```

Wie lautet der Klartext?