SS 2004, TU Darmstadt

Erforderliche Kenntnisse: keine

von Stephan Petsch

Einfache Codierverfahren

Das Ziel des Codierens ist es, Nachrichten so zu verschlüsseln, das nur der Absender und der Empfänger sie verstehen können. Dazu verschlüsselt der Absender die Nachricht mit Hilfe eines Schlüssels. Das einfachste Verfahren ist das

Ersetzen von Buchstaben durch Zahlen

Um einen Text zu verschlüsseln, schreibt man zuerst das Alphabet auf. Darunter werden dann Zahlen geschrieben, also etwa so:

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Eine solche Auflistung, der man entnehmen kann, welche Buchstaben wie getauscht wurden, bezeichnet man als Schlüssel.
In der zu verfassenden Nachricht werden nun alle Buchstaben gemäß dem Schlüssel durch die entsprechende Zahl ersetzt, so wird z.B. aus

WER WEISS, WIE DIE BUCHSTABEN GETAUSCHT SIND
die Zahlenfolge
23 5 18 23 5 9 19 19 23 9 5 4 9 5 2 21 3 8 19 20 1 2 5 14 7 5 20 1 21 19 3 8 20 19 9 14 4

Um die Nachricht zu entschlüsseln, braucht der Empfänger nun den entsprechenden Schlüssel und ersetzt die Zahlen wieder durch Buchstaben. Natürlich kann man auch andere Zahlen zur Verschlüsselung nehmen, es müssen nicht die ersten 26 sein. Alternativ besteht die Möglichkeit, Buchstaben durch andere Buchstaben zu ersetzen, zum Beispiel durch den Buchstaben, der im Alphabet 3 Stellen weiter links steht:

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
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

So bekommen wir ZHUZHLVVZLHGLHEXFKVWDEQJHWDXVFKWVLQH
Natürlich ist es noch sinnvoll, auch Zeichen, wie Komma, Punkt, Bindestrich etc. zu verschlüsseln, sogar Leerzeichen können verschlüsselt werden. Der Nachteil ist allerdings, dass in der Nachricht die gleiche Zahl immer für den gleichen Buchstaben steht. Dadurch sind Rückschlüsse auf den Text möglich. So ist im Deutschen „e“ der häufigste Buchstabe, es wäre also sinnvoll, in der verschlüsselten Nachricht nach dem häufigsten Buchstaben oder der häufigsten Zahl zu suchen, dann nach dem/der

zweithäufigsten usw.. Nach ein paar Durchgängen kann man schauen, ob sich irgendwelche Wörter andeuten und „sinnvoll raten“.

Das Verschlüsseln mithilfe von Matrizen

Ein komplizierteres, aber deutlich sichereres Verfahren ist das Verschlüsseln mithilfe von Matrizen. Dazu eine kleine Exkursion:

Eine Matrix ist ein rechteckiges Schema von Zahlen.

$$A = \begin{pmatrix} a11 & a12 & \dots & a1m \\ a21 & a22 & \dots & a2m \\ \dots & \dots & \dots & \dots \\ an1 & an2 & \dots & anm \end{pmatrix}$$

Die Zahlen a_{nm}, wobei n und m natürliche Zahlen sind, werden Elemente oder Koeffizienten der Matrix genannt. Die Multiplikation zweier Matrizen erfolgt auf folgende Weise:

Zuerst muss eine Bedingung erfüllt sein: Die Anzahl der Spalten der ersten Matrix muss gleich der Anzahl der Zeilen der zweiten Matrix sein, ansonsten kann die Multiplikation nicht erfolgen. Daraus folgt auch, dass man beim Multiplizieren von Matrizen die Faktoren nicht immer vertauschen kann. Es wird nun auf folgende Weise multipliziert: es wird jeweils die **u**-te Zeile der ersten Matrix mit der **v**-ten Spalte der zweiten Matrix skalar multipliziert. Bsp:

$$\begin{pmatrix} 1 & 2 & 1 \\ 2 & 5 & 3 \\ 3 & 5 & 4 \end{pmatrix} \times \begin{pmatrix} 3 & 5 \\ 4 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1x3+2x4+1x2 & 1x5+2x2+1x1 \\ 2x3+5x4+3x2 & 2x5+5x2+3x1 \\ 3x3+5x4+4x2 & 3x5+5x2+4x1 \end{pmatrix} = \begin{pmatrix} 13 & 10 \\ 32 & 23 \\ 37 & 29 \end{pmatrix}$$

Zurück zum eigentlichen Verschlüsseln. Um per Matrizen eine Nachricht zu codieren,

werden die Buchstaben zuerst in Zahlen umgewandelt und dann in eine Matrix

geschrieben. Etwa so:

$$\begin{pmatrix} 23 & 5 & 18 \\ 23 & 5 & 9 \\ 19 & 18 & 23 \\ 9 & 5 & 4 \\ 9 & 5 & 2 \\ 21 & 3 & 8 \\ 19 & 20 & 1 \\ 2 & 5 & 14 \\ 7 & 5 & 20 \\ 1 & 21 & 19 \\ 3 & 8 & 20 \\ 19 & 9 & 14 \\ 4 & 0 & 0 \end{pmatrix}$$

Diese Matrix wird nun mit einer beliebigen anderen Matrix, die die Bedingung der Matrizenmultiplikation erfüllt, multipliziert. Diese Matrix ist der Schlüssel und wird auch als Kodiermatrix (K) bezeichnet. Der zweite Schlüssel ist der des Empfängers und wird Dekodiermatrix (D) genannt. Die codierte Matrix (C) muss mit der Dekodiermatrix multipliziert wieder die ursprüngliche Nachricht ergeben. Es soll also gelten:

$$M \times K = C \qquad C \times D = M$$

Daraus folgt:

$$M \times K \times D = M$$

Kodiermatrix mal Dekodiermatrix sollte demnach 1 ergeben. Eine Konstante mal eine

Matrix ist zwar definiert, doch die Umkehrung Matrix mal Konstante ist undefiniert.

Wir müssen die Konstante 1 also in eine Matrix umschreiben. Eine Matrix, die dies

erfüllt (und Einheitsmatrix genannt wird) ist

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Zu jeder Kodiermatrix (außer sie beinhaltet die Null) gibt es also eine Dekodiermatrix, sodass das Produkt der beiden die Einheitsmatrix ergibt, es gibt also praktisch eine unendliche Anzahl von möglichen Schlüsseln.

Verschlüsselung in einem Buchtext

Ein weiteres, jedoch nichtmathematisches Verfahren ist das Verschlüsseln anhand eines Buches. Dazu brauchen Sender und Empfänger jeweils dasselbe Buch in derselben Ausgabe (natürlich funktioniert das auch mit derselben Ausgabe einer Zeitung). Die Buchstaben werden willkürlich durch ihre Position im Text ersetzt (Zeile/Buchstabe), und zwar ohne Reihenfolge und auch für jeden einzelnen Buchstaben immer wieder neu. Ohne die entsprechende Buchseite ist es praktisch unmöglich, diesen Code zu knacken.
Beispiel:

Habe nun, ach! Philosophie,
Juristerei und Medizin,
Und leider auch Theologie
Durchaus studiert, mit heißem Bemühn.
Da steh ich nun, ich armer Tor!
Und bin so klug als wie zuvor;
Heiße Magister, heiße Doktor gar
Und ziehe schon an die zehen Jahr
Herauf, herab und quer und krumm
Meine Schüler an der Nase herum-
Und sehe, daß wir nichts wissen können!
Das will mir schier das Herz verbrennen.
Zwar bin ich gescheiter als all die Laffen,
Doktoren, Magister, Schreiber und Pfaffen;
Mich plagen keine Skrupel noch Zweifel,
Fürchte mich weder vor Hölle noch Teufel-
Dafür ist mir auch alle Freud entrissen,
Bilde mir nicht ein, was Rechts zu wissen,
Bilde mir nicht ein, ich könnte was lehren,
Die Menschen zu bessern und zu bekehren.

Die Botschaft lautet: DIESES ZITAT STAMMT AUS GOETHES FAUST

Der dazugehörige Code wäre 8/3 1/13 18/5 20/17 5/5 11/4 6/19 8/5 16/6 5/2 7/11 12/11 13/18 8/25 12/8 16/5 5/21 13/3 6/1 15/16 3/20 1/17 7/5 4/10 9/1 9/8 10/6 13/32 19/27 6/11 14/13 3/14