

26. Algorithmus der Woche

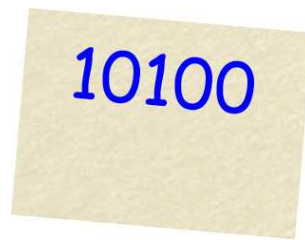
Der One-Time-Pad-Algorithmus

Der einfachste und sicherste Verschlüsselungsalgorithmus

Autor

Till Tantau, Universität zu Lübeck

Die Schule hat kaum angefangen und schon wieder steht eine Informatikklausur an – und Max hat keine Ahnung vom Stoff, irgendwas über Verschlüsselung. Dass Max keine Ahnung hat ist auch nicht weiter verwunderlich, da er sich im Unterricht und auch sonst hauptsächlich mit Lisa, seiner neuen Freundin, beschäftigt. Lisa hingegen findet nicht nur Max, sondern auch Verschlüsselung faszinierend. Deshalb möchte Max, man ahnt es schon, die Klausur von Lisa abschreiben. Lisa sieht allerdings ein kleines Problem: »Peter wird während der Klausur zwischen uns sitzen. Ich muss also Peter einen Zettel mit den Antworten geben und der gibt ihn dann dir. Das sollte aber kein Problem sein, da die Lehrerin das eh nicht merkt, Peter alles macht, was ich ihm sage, und es nur Ankreuzfragen sind: Ich schreibe eine 1 auf, wenn man ein Kreuz machen muss und eine 0, wenn man keines machen darf. Wenn du also bei einer Ankreuzaufgabe mit fünf Möglichkeiten beim ersten und dritten Kästchen ein Kreuz machen sollst, dann schicke ich dir folgenden Papierschnipsel:«



Gesagt, getan. Und tatsächlich schreiben Lisa, Max und auch Peter hervorragende Klausuren. Die Lehrerin ist allerdings ob der sonstigen Leistungen von Max nicht ganz sicher, ob alles mit rechten Dingen zugegangen ist. Für die nächste Klausur beschließt sie deshalb listig, statt Peter die Ex-Freundin von Max zwischen Max und Lisa zu setzen. Die Idee der Lehrerin zeigt Wirkung, denn Max meint aufgeregt zu Lisa: »Lieber falle ich durch die Klausur als dass *sie* die Antworten auch abschreibt!«

Lisa denkt kurz nach und meint dann: »Ok, dann müssen wir eben die Lösung mit einem One-Time-Pad verschlüsseln.«

»One-Time-Pad?« fragt Max etwas ratlos.

»Das bedeutet wörtlich >Einmal-Notizblock< und ist ein Verfahren zur Einmalverschlüsselung.«

»Verschlüsseln?« fragt Max immer noch ratlos.

»Du passt echt nicht auf...« beginnt Lisa, worauf Max sie mit einem »Aber dafür liebe ich dich!« unterbricht, was Lisa ignoriert. »Verschlüsseln bedeutet, dass wir uns einen *Schlüssel* ausdenken, mit dem ich die Lösung für die Aufgaben mit einem One-Time-Pad abschließe. Du kannst die verschlüsselte Lösung mit dem Schlüssel wieder aufschließen. Und deine Ex kann mit der verschlüsselten Lösung ohne den Schlüssel nichts anfangen.«

»Häh?« entgegnet Max nun völlig verwirrt.

Verschlüsselung von Nachrichten

»Gib mal fünf Münzen her. Die Zahl-Seite bedeutet, dass du ein Kreuz machen musst in einem Kästchen, die andere Seite bedeutet, dass du kein Kreuz machen sollst. Wenn du also bei einer Ankreuzaufgabe mit fünf Möglichkeiten beim ersten und dritten Kästchen ein Kreuz machen sollst, dann können wir das mit Münzen wie folgt darstellen:«



»Von mir aus, auch wenn ich nicht sehe, was das bringen soll,« entgegnet Max etwas gelangweilt. »Egal, ob du mir nun 10100 auf einen Zettel schreibst oder die fünf Münzen hinlegst, meine Ex kapiert doch auch, dass das bedeuten soll: Mache Kreuze bei der ersten und dritten Frage.«

»Richtig, aber jetzt kommt die Verschlüsselung ins Spiel. Gib mir mal einen Stapel Zettel – danke. Auf einige schreibe ich »umdrehen«, auf die anderen »nicht umdrehen«. Jetzt darfst du fünf Zettel zufällig wählen und nebeneinander legen.«

Max tut wie ihm geheißen und legt unter die Münzen Folgendes:



»Gut,« meint Lisa. »Diese Zettel bilden unseren »Schlüssel«, den wir vor der Klausur festlegen und auswendig lernen.«

»Ah,« entgegnet Max, der ja auch nicht blöd ist, »du schickst dann statt der ursprünglichen Münzen die entsprechend unseres Schlüssels umgedrehten Münzen, also Folgendes:

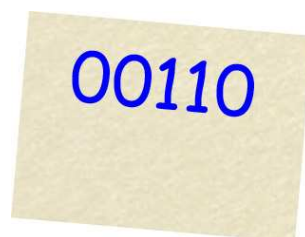


Wenn meine Ex das sieht, dann kann sie damit herzlich wenig anfangen – wenn sie zum Beispiel die erste Münze betrachtet, dann kann das sowohl »mache ein Kreuz« bedeutet oder eben gerade »mache kein Kreuz«. Die Chance, dass wir in unserem Schlüssel gerade »umdrehen« stehen haben, ist ja fifty-fifty.

Aber – warum sollte sie mir dann überhaupt den Zettel weiterreichen und nicht gleich zerreißen oder runterschlucken oder verbrennen oder ... «

»Sie will doch auch, dass du versetzt wirst – damit sie dich auch nächstes Jahr durch ihre Anwesenheit ärgern kann.«

»Na toll... Jetzt aber nochmal der Schlachtplan: In der Klausur löst du die erste Aufgabe und möchtest mir mitteilen, dass ich im ersten und dritten Kästchen ein Kreuz machen soll. Das entspricht 10100. Da aber unser Schlüssel sagt, dass die erste und vierte »Münze« umgedreht werden sollen, schickst du mir stattdessen



Ich habe mir auch den Schlüssel gemerkt und >drehe die Münzen wieder zurück< und erhalte 10100. Schließlich mache ich meine Kreuze im ersten und dritten Kästchen.<<

»Ich wusste doch, dass ich einen schlaunen Freund habe. Wie du siehst, ist dieses One-Time-Pad-Verfahren nicht schwierig und trotzdem sehr sicher. Wir sind auch nicht die einzigen, die es benutzen – wenn sich Staatsoberhäupter Nachrichten schicken und nicht wollen, dass jemand die Nachrichten mitlesen kann, dann benutzen sie auch dieses Verfahren.<<

Jetzt muss Max lachen. »Glaubst du wirklich, wenn Herr Bush an Frau Merkel eine Nachricht schicken will, dann dreht er Münzen herum und schreibt Nullen und Einsen auf eine Postkarte?!<<

»Natürlich nicht,<< grummelt Lisa, »das macht ein Computer für ihn. Dazu muss man das Verfahren als Algorithmus aufschreiben, was für dich eine gute Übung wäre.<<

Der Algorithmus

»Mal sehen,<< beginnt Max, der immernoch grinst. »Erstmal scheint mir, dass es tatsächlich nur einen Algorithmus gibt, denn der zur Verschlüsselung und der zur Entschlüsselung sind gleich: Jedesmal beginnen wir mit Nullen und Einsen und einem Schlüssel und bekommen wieder Nullen und Einsen heraus. Dann muss einfach im Algorithmus jede Null in eine Eins verwandelt werden und umgekehrt, wo im Schlüssel >umdrehen< steht.<<

»Und wie speicherst du den Schlüssel? Du kannst ja keine gelben Zettel im Computerspeicher haben.<<

»Da nehme ich ein Array, in dem stehen eben die Zeichenketten >umdrehen< und >nicht umdrehen<. Dann lautet der Algorithmus wie folgt:<<

Die Funktion ONETIMEPAD führt eine Verschlüsselung oder Entschlüsselung des Arrays A mit n Einträgen mittels Schlüssel durch.

```

1  function ONETIMEPAD (A, Schlüssel)
2  begin
3    for i := 1 to n do
4      if Schlüssel[i] = "umdrehen" then
5        if A[i] = 0 then
6          A[i] := 1
7        else
8          A[i] := 0
9      endfor
10 end

```

»Genau,<< entgegnet Lisa. »So könnte man das machen. Normalerweise ist der Schlüssel allerdings nicht ein Array in denen Zeichenketten wie >umdrehen< oder >nicht umdrehen< stehen, sondern ebenfalls ein Array von Nullen und Einsen. Dabei bedeutet eine Eins gerade >umdrehen< und eine Null >nicht umdrehen<. Damit kann man den Algorithmus auch ganz kurz schreiben:<<

Kurze Version der Funktion ONETIMEPAD.

```

1  function ONETIMEPAD (A, Schlüssel)
2  begin
3    for i := 1 to n do
4      A[i] := A[i] xor Schlüssel[i]
5    endfor
6  end

```

»Moment,« unterbricht Max, »ich erinnere mich dunkel, dass >xor< für eXklusives OdeR steht. Was war das nochmal?«

»Das exklusive Oder überprüft, ob genau eine von zwei Zahlen eine 1 ist, und liefert eine 1, wenn dies der Fall ist. Damit das exklusive Oder also eine 1 ist, muss $A[i]$ eine 1 sein oder Schlüssel[i] eine 1 sein, aber eine dieser Bedingungen muss >exklusiv< gelten – es darf gerade nicht beides gelten. Schau dir folgende Tabelle an, die zeigt, was passiert.«

	Schlüssel[i] = 0	Schlüssel[i] = 1
$A[i] = 0$	0	1
$A[i] = 1$	1	0

Tabelle mit den Werten von $A[i]$ xor Schlüssel[i].

»Ich glaube, ich verstehe, was hier passiert. Das >xor< macht genau, was wir brauchen: Es dreht den Wert von $A[i]$ um, wenn Schlüssel[i] = 1 ist, und lässt ihn so wie er ist, wenn Schlüssel[i] = 0 gilt.«

Brechen der Verschlüsselung

»So langsam gefällt mir dieses Verfahren,« fährt Max fort. »Und das beste ist, ich brauche mir nur fünf gelbe Zettel zu merken für die gesamte Klausur, denn wir können ja die Verschlüsselung immer wieder verwenden!«

»Nein, so einfach ist das leider nicht,« wendet Lisa ein. »Stelle dir mal vor, wir würden für alle zwanzig Aufgaben in der Klausur, jede mit fünf Kästchen, jedesmal denselben Schlüssel verwenden. Was würde denn passieren, wenn deine Ex eine der Aufgaben selber lösen würde und dann meine verschlüsselte Lösung sehen würde? Nehmen wir an, ich finde heraus, dass du die letzten drei Kästchen ankreuzen musst. Dann lautet die Lösung >in Münzen geschrieben<:



Diesen Wert kennt deine Ex dann auch, wenn sie die Aufgabe gelöst bekommt. Dann sieht sie den Zettel, den sie von mir bekommt, auf dem der verschlüsselte Wert 01010 steht. Dies entspricht den Münzen



Siehst du, was jetzt passiert?«

»Ja, sie kann den Schlüssel ausrechnen. Da du auf den Zettel eine 0 an die erste Stelle geschrieben hast, weiß sie, dass du die erste Münze nicht umgedreht hast. Die zweite hingegen hast du umgedreht, und so weiter. Sie weiß dann, dass der Schlüssel lautet:



Und wenn sie erstmal den Schlüssel kennt, dann kann sie alle anderen Aufgabe auch lösen!«

»Deshalb heißt das Verfahren auch One-Time-Pad, also Einmalverschlüsselung. *Man kann einen Schlüssel bei diesem Verfahren nur einmal verwenden.* Wenn man das nicht macht, so kann man das Verfahren schnell umgehen. So benutzte beispielsweise ein älteres Verfahren zum Verschlüsseln beim schnurlosen Surfen mit Laptops in Cafés immer wieder denselben Schlüssel – weshalb der Schlüssel schnell herauszubekommen war. Die hochbezahlten Leute, die sich dieses Verfahren ausgedacht haben, haben offenbar in der Schule nicht sonderlich aufgepasst.

Wir werden uns für die Klausur für jede Aufgabe einen neuen Schlüssel ausdenken müssen.«

»Aber das ist ja schrecklich! Da muss ich mir ja die richtige Reihenfolge von 100 mal >umdrehen< oder >nicht umdrehen< merken. Da kann ich ja gleich den Stoff lernen!«

»Hmm, vielleicht wäre das sowieso die beste Lösung. So schwierig ist Verschlüsselung ja nun auch wieder nicht.«

Autoren:

- Prof. Dr. Till Tantau
<http://www.tcs.uni-luebeck.de/pages/tantau>

Externe Links:

- Wikipedia zu One-Time-Pad
<http://de.wikipedia.org/wiki/One-Time-Pad>
- Wikipedia zu Verschlüsselung allgemein
<http://de.wikipedia.org/wiki/Verschlüsselung>