SCHOOL-SCOUT.DE

Unterrichtsmaterialien in digitaler und in gedruckter Form

Auszug aus:

Informatik konkret: Kryptografie: Verschlüsselungen und Codes

Das komplette Material finden Sie hier:

School-Scout.de

Inhaltsverzeichnis

Vorwort

Liebe Kollegin, lieber Kollege,

die Kryptografie ist sicher nicht das grundlegendste Thema im Informatikunterricht und sie wird vielleicht in Ihrem Bildungsplan eher am Rande erwähnt. Aber sie ist ein Thema, das die Menschen seit jeher fasziniert hat – und bestimmt auch Ihre Schüler faszinieren wird. Mich hat diese Faszination gepackt, nachdem ich das Buch „Codes“ von Simon Singh gelesen hatte, und so habe ich mich dazu entschlossen, eine entsprechende Unterrichtseinheit für den Informatikunterricht zu erstellen. Diese halten Sie nun in den Händen.

Das Heft lässt sich auf zweierlei Arten verwenden:

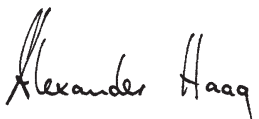
– Für Schüler, die noch keine Programmiersprache beherrschen, bietet es neben den umfangreichen Informationen über die in chronologischer Reihenfolge vorgestellten kryptografischen Verfahren eine Fülle von Aufgaben, bei denen Texte „von Hand“ bzw. mithilfe von kleinen Programmen, die sich auf der Begleit-CD zum Heft befinden, verschlüsselt oder entschlüsselt werden sollen. Der Lehrer muss dafür überhaupt nichts vorbereiten, die Schüler arbeiten selbstständig mit dem ausgeteilten Material und können sich anhand der Lösungen (hinten im Heft sowie auf der Begleit-CD) sogar selbst kontrollieren. Die verschlüsselten Nachrichten enthalten oft einen witzigen Spruch und sind teilweise bewusst flapsig, um die Schüler zu motivieren. Sollte Ihnen das nicht zusagen, können Sie mit den Programmen auf der Begleit-CD auch Aufgaben mit eigenen Lösungssätzen erstellen.

– Für Schüler, die bereits eine Programmiersprache (zumindest in Grundzügen) beherrschen, gibt es zusätzlich Programmieraufgaben. In diesen geht es darum, Programme zu schreiben, die die verschiedenen Codierverfahren automatisieren, sodass man nur noch die Nachricht und – falls erforderlich – ein Codewort eingeben muss und die Nachricht dann vom Computer ver- bzw. entschlüsselt wird. Auch hierbei ist der Aufwand für die Lehrperson minimal, da sich alles, was benötigt wird (inklusive Musterlösungen der Programmieraufgaben in Free Pascal!), auf der beiliegenden CD befindet.

Auf der CD finden Sie alle Aufgaben aus dem Buch, alle Lösungen zu den Aufgaben, alle Lösungen zu den Programmieraufgaben, einige grundlegende Hinweise zur Veränderung von Strings (darauf beruht fast jede Ver- bzw. Entschlüsselung) sowie eine Vielzahl an von mir geschriebenen Programmen, die bei einzelnen Aufgaben benötigt werden. Für nähere Informationen siehe Seite 56.

Die Musterlösungen zu den Programmieraufgaben wurden mit Lazarus erstellt, einer Entwicklungsumgebung, die man unter http://sourceforge.net/projects/lazarus/files/ herunterladen kann. Die verwendete Programmiersprache – Free Pascal – entspricht bis auf winzige Details der Programmiersprache Delphi. Ein solches winziges, aber entscheidendes Detail ist, dass Free Pascal und Lazarus absolut kostenlos sind und uneingeschränkt genutzt werden können. Nach der Installation von Lazarus (Free Pascal braucht nicht extra installiert zu werden!) kann man sofort mit dem Programmieren loslegen und auch die Musterlösungen anschauen. Natürlich kann aber auch jede andere Programmiersprache verwendet werden.

Viel Spaß bei der Kryptografie wünscht Ihnen



Alexander Haag

1. Steganografie

Die Übermittlung geheimer Nachrichten, bei der verborgen wird, dass überhaupt eine Botschaft existiert, nennt man Steganografie. Auch wenn die Steganografie eigentlich kein Unterzweig der Kryptografie ist, wird sie hier dennoch kurz angesprochen, da sie geschichtlich eng mit der Kryptografie verwandt ist.

Die ältesten bekannten Beispiele für Steganografie sind unter anderem:

- Von einer Schreibtafel wurde das Wachs abgeschabt, anschließend wurde die Nachricht auf das Holz der Tafel geschrieben und diese sodann wieder mit Wachs bedeckt. Der Empfänger musste nur das Wachs wieder abkratzen und konnte die Botschaft lesen (bereits im 5. Jahrhundert vor Christus erfolgreich angewandt).

- Der Kopf eines Boten wurde rasiert und die Nachricht wurde in die Kopfhaut eingebrannt. Der Bote wurde erst losgeschickt, nachdem das Haar wieder nachgewachsen war. Am Ziel angekommen wurde der Bote dann wiederum rasiert und die Nachricht konnte gelesen werden (Nachteil: sehr zeitaufwendig).

Nur so wird die Nachricht wieder sichtbar.

- Die alten Chinesen schrieben Botschaften auf feine Seide, rollten sie zu Bällchen und tauchten diese in Wachs. Diese Wachskügelchen schluckte dann der Bote (Nachteil: ziemlich unappetitlich für den Empfänger).

- Mit einer Alaun-Essig-Mischung wird die Nachricht auf die Schale eines hartgekochten Eis geschrieben. Auf der Schale ist dies unsichtbar – schält man das Ei jedoch, kann man die Botschaft auf dem Eiweiß lesen.

- Eine Botschaft wird mit unsichtbarer Tinte (z. B. Milch der Thithymallus-Pflanze, viele andere organische Flüssigkeiten, Urin) auf ein Blatt geschrieben. Wird dieses erhitzt, wird die Schrift sichtbar.

Das Hauptproblem der Steganografie ist offensichtlich: Wird die Nachricht gefunden, kann jeder sie lesen. Daher entstand zugleich mit der Steganografie auch die Kryptografie, deren Ziel nicht ist, die Existenz einer Botschaft zu verschleiern, sondern ihren Sinn zu verbergen, und dies mittels eines Verfahrens der Verschlüsselung. Die Kryptografie verwendet hauptsächlich zwei Verfahren:

– die Transposition (Buchstaben anders anordnen) und
– die Substitution (Buchstaben durch andere ersetzen).

2. Transposition

Während bei sehr kurzen Mitteilungen (z. B. „hey“) nur eine geringe Anzahl von Anordnungsmöglichkeiten existieren (ehy, eyh, hey, hye, yeh, yhe), gibt es bereits bei Sätzen wie „Lieber krank feiern als gesund arbeiten“ knapp 300 Millionen Millionen Millionen Millionen Millionen Millionen verschiedene Möglichkeiten, die 34 Buchstaben des Satzes umzuordnen. Könnte ein Mensch eine Anordnung pro Sekunde prüfen, und arbeiteten alle Menschen der Erde Tag und Nacht, dann würde immer noch die hundertmilliardenfache Lebensspanne des Universums nötig sein, um alle Möglichkeiten durchzuprüfen.

Eine Zufallstransposition von Buchstaben bietet also ein sehr hohes Maß an Sicherheit. Doch die Sache hat einen Haken: Der eigentliche Empfänger kann ebenso wenig wie der gegnerische Abhörer die Nachricht entschlüsseln. Die Umstellung muss also nach einem handhabbaren System erfolgen. Zwei dieser Systeme wollen wir uns ein bisschen genauer anschauen.

Die „Gartenzaun“-Transposition

Bei der „Gartenzaun“-Transposition werden die Buchstaben des Textes abwechselnd auf zwei Zeilen geschrieben und anschließend wird die zweite Zeile an die erste angehängt:

LIEBERTUGENDHAFTALSJUGENDHAFT

Klartext

L E E T G N H F A S U E D A T
I B R U E D A T L J G N H F

LEETGNHFASUEDATIBRUEDATLJGNHF

Geheimtext

Der Name kommt daher, dass die versetzte Anordnung der Buchstaben auf zwei Zeilen mit etwas Fantasie an einen Gartenzaun erinnert.

1 Du willst einer Freundin folgende traurige Nachricht schicken:

HABEAMSONNTAGKEINEZEITMUSSLERNENSORRY

Verschlüssle den Satz mit der „Gartenzaun“-Transposition.

2 Du hast einen Zettel gefunden, auf dem nur die folgende, ziemlich sinnlos aussehende, Botschaft steht:

LEEMTEOAEENLMTITROLNIBRIVRNKGLASIDEEBHE

Welche Lebensweisheit wollte der Sender dem Empfänger damit wohl mitteilen?

3 Am Vertretungsplan hat ein Witzbold einen Zettel aufgehängt, auf dem steht:

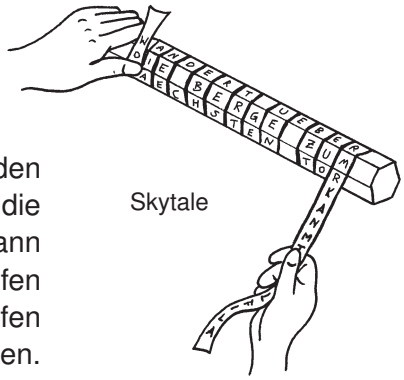
Wichtige Info:
AMTWCFLEDERTNWITNEASMITOHALNIESEZESUDNU

Entschlüssle die Nachricht.

1 *Programmieraufgabe*

Schreibe ein Programm, das einen Klartext mit der „Gartenzaun"-Transposition verschlüsseln kann und zudem einen mit der „Gartenzaun"-Transposition verschlüsselten Geheimtext entschlüsseln kann.

Die Skytale


Skytale

Bei der Skytale (sprich: *Skütale*) handelt es sich um einen Holzstab, um den ein Streifen Leder oder Pergament gewickelt wird. Der Sender schreibt die Nachricht der Länge des Stabes nach auf den Streifen und wickelt ihn dann ab. Liest man die Buchstaben in der Reihenfolge, in der sie auf dem Streifen stehen, ergibt sich nur Kauderwelsch. Der Empfänger wickelt den Streifen um eine Skytale mit demselben Durchmesser und kann die Nachricht lesen.

Dieses Verfahren lässt sich relativ einfach mit einem STABILO-Stift und einem Streifen Papier (ca. 30 cm lang und 5 mm breit) nachvollziehen. Der STABILO-Stift dient dabei als (sechsseitige) Skytale, der Papierstreifen ist unser Pergament (Ende mit Tesafilm festkleben). Zwar funktioniert die Transposition auch mit einem runden Stift, aber mit einem eckigen geht es wesentlich einfacher.

Tipp: Wer es lieber größer mag, kann sich auch mit einer Rolle Klopapier an einem Pfosten versuchen, allerdings reißt das Klopapier relativ schnell ab.

4 Verschlüssle die unten stehende Nachricht mit der STABILO-Skytale. Wechsle dabei nach jeweils 5 Buchstaben auf die nächste STABILO-Seite und achte darauf, dass das erste A ganz oben auf dem Papierstreifen steht.

ALLESGUTEZUMGEBURTSTAGANNEGRET

5

Ein gegnerischer Spion hat bei einer heimlichen Hausdurchsuchung bei dir auf dem Schreibtisch ein Pack STABILOs entdeckt. STABILOs auf dem Schreibtisch sind zwar relativ unauffällig, aber es wäre trotzdem denkbar, dass der Gegner die Verschlüsselung mittels STABILO-Skytale durchschaut hat – als Spion muss man extrem vorsichtig und misstrauisch sein. Du hast deshalb beschlossen, deine geheimen Botschaften ab sofort mit einer achtseitigen Skytale-Codierung zu schützen und dich sicherheitshalber nach Dänemark abzusetzen. Verschlüssle die folgende Botschaft an deinen Kontaktmann und überlege dir vorher, nach wie vielen Buchstaben du auf die nächste Seite der Skytale wechseln musst.

TARNUNGAUFGEFLOGENSTOPBINENTDECKTSTOPFLUCHTNACHDAENEMARK

6

Du sitzt mäßig interessiert im Unterricht und beginnst gerade, dich zu langweilen, als dich ein Papierstreifen mit der folgenden Nachricht erreicht:

KUITKSOHTZEPMETUTIMUAMBESTGBALTEMALEDMISLN

Der Freund, der die Nachricht geschrieben hat, zeigt, als er deinen ratlosen Blick sieht, auf einen STABILO-Stift. Wie lautet die entschlüsselte Botschaft?

7

Es ist dir unter großem Aufwand gelungen, den folgenden Funkspruch abzuhören:

SHLNWRIHIÜATAAENNHTERKDEDNTLDTELDEWLEORLIRIERRSEEPERTWCR

Du vermutest (zu Recht!), die Botschaft könnte mit einer Skytale verschlüsselt worden sein. Leider gibt es aber keinerlei Anhaltspunkte über die Anzahl der Seiten. Es bleibt dir also nichts anderes übrig, als verschiedene Möglichkeiten durchzuprobieren – schließlich könnte die Nachricht die Lösungen der nächsten Mathearbeit enthalten! Doch in diesem Fall hat sich der Sender wohl eher einen Scherz erlaubt. Wie lautet die entschlüsselte Nachricht?

2

Programmieraufgabe

Schreibe ein Programm, das einen Klartext mittels einer Skytale verschlüsseln kann (bzw. dies simuliert) und zudem einen mit der Skytale verschlüsselten Geheimtext entschlüsseln kann.

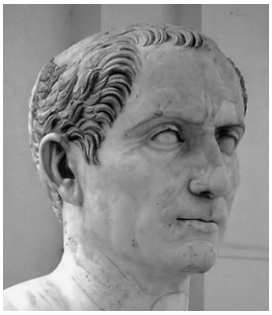
Tipp: Die Skytale-Verschlüsselung ist natürlich davon abhängig, wie viele Buchstaben auf den Streifen passen, wenn dieser genau einmal um den Holzstab gewickelt wird (geht man nicht von einem runden, sondern einem eckigen Stock aus, entspricht diese Zahl der Anzahl der Seiten des Stocks). Da diese Anzahl sowohl für das Ver- als auch für das Entschlüsseln von entscheidender Bedeutung ist, sollte man sie an irgendeiner Stelle im Programm eingeben und auch ändern können. So kann man beim Entschlüsseln quasi verschiedene „Stöcke“ durchprobieren, bis der entschlüsselte Text Sinn macht (und damit die richtige „Stockgröße“ gefunden wurde).

3. Monoalphabetische Substitution

Die Alternative zur Transposition ist die Substitution. Es gibt verschiedene Arten der Substitution, die jedoch alle auf demselben Prinzip beruhen: Nicht die Anordnung der Buchstaben wird verändert, sondern die Buchstaben werden durch andere Buchstaben, Zahlen oder Zeichen ersetzt.

Die einfachste Art der Substitution ist die sogenannte monoalphabetische Substitution.

Die Caesar-Verschlüsselung & ROT13



Julius Caesar

Julius Caesar war der Erste, von dem überliefert ist, dass er eine monoalphabetische Substitution verwendete, um seine geheimen Nachrichten zu verschlüsseln. Deshalb ist diese Verschlüsselung nach ihm benannt. Die Idee ist simpel: Ein Klartextalphabet wird mit einem Geheimtextalphabet verschlüsselt. Das Geheimtextalphabet ist dabei mit dem Klartextalphabet identisch, allerdings **um drei Stellen verschoben**:

Klartextalphabet:	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
Geheimtextalphabet:	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

Klartext: Lieber arm dran als Arm ab!
Geheimtext: Olhehu dup gudq dov Dup de!

8 Ein berühmtes Zitat Caesars lautet: „Proditionem amo, sed proditores non laudo." Frei übersetzt bedeutet das: „Ich liebe den Verrat, aber ich verachte die Verräter." Die Angst vor Verrätern trieb Caesar dazu, seine Botschaften zu verschlüsseln, denn wenn ein Bote eine Nachricht gar nicht lesen konnte, konnte er sie auch nicht ausplaudern. Welches Buchstabengewirr entstand aus der folgenden wichtigen Botschaft, nachdem Caesars Chefkryptograf diese verschlüsselt hatte?

DIE SPINNEN DIE GALLIER

9 Obelix ist bei der Wildschweinjagd auf eine römische Patrouille gestoßen und hat dem Römer Claudius Nimdenbus die folgende Botschaft abgenommen:

XQWHU GHQ NOHLQVWHQ VWHSSGHFNHQ NDQQ GHU
JURHVVWH GHSS VWHFNHQ

Welche Lebensweisheit erhält man, wenn man die Botschaft entschlüsselt?

SCHOOL-SCOUT.DE

Unterrichtsmaterialien in digitaler und in gedruckter Form

Auszug aus:

Informatik konkret: Kryptografie: Verschlüsselungen und Codes

Das komplette Material finden Sie hier:

School-Scout.de