Von Vigenère zum One-Time-Pad

Michael Brand und Anna Höpli

Lernziel

Die Aufgabe stellt die One Time Pad Verschlüsselung vor. Die SuS sollen erkennen, dass die Verschlüsselung bei einmaligem Gebrauch absolut sicher ist, aber nur schon bei einem zweiten Gebrauch entschlüsselbar wird.

Als zweites zeigt die Aufgabe, wie man mittels Lochstreifen eine Verschlüsselung von Binärzahlen erreichen kann. Dies ist eine historische Methode aus der Praxis. Die Lochstreifen Methode wird danach so abstrahiert, dass das One Time Pad für binäre Zahlen verständlich wird.

Vorwissen

Die Aufgabe ist konzipiert als aufbauender Stoff nach der Einführung der Vigenère- Verschlüsselung. Die SuS sollen bereits sowohl das Verschlüsselungsverfahren, als auch dessen Entschlüsselungsmöglichkeiten kennen. Es ist sinnvoll, wenn die Kodierung mittels ASCII Tabelle bereits besprochen wurde.

Material und Vorgehen

Je nach Klassenstufe und Abstraktionsfähigkeit, kann man Lochstreifen mitbringen und die Lochstreifen Methode direkt physisch mit der Klasse ausprobieren. Die Aufgabe lässt sich aber auch rein theoretisch lösen.

Im Moment sind die Lösungen in den Text integriert, für eine SuS Fassung lohnt es sich, die Lösungen nicht mitzugeben, sondern diese nach und nach aufzudecken.

Zeitaufwand

Etwa 2 Lektionen.

Einstiegsaufgabe -- Teil 1

Zwei Agenten verabreden sich in BASEL. Natürlich kommunizieren sie den Treffpunkt nicht im Klartext, sondern haben ihn mit dem Vigenère-Verfahren verschlüsselt. Der Geheimtext lautet PXEMJ. Findest du den Schlüssel, den die beiden Agenten verwendet haben?

Jetzt nehmen wir an, dass ein feindlicher Spion den Geheimtext PXEMJ abgefangen hat, aber er kennt den Schlüssel nicht. Findest du weitere Schlüssel, so dass ein Städtename zum Geheimtext PXEMJ verschlüsselt wird? Mache dir zuerst eine Liste mit einigen Städten, deren Name aus 5 Buchstaben bestehen.

Welche Beobachtung machst du? Und welche Konsequenz hat deine Beobachtung für den Spion, der nur den Geheimtext kennt?

Lösung und Erklärung

Um die Entschlüsselung für einen Spion möglichst schwierig zu machen, wählen die Agenten einen möglichst langen Schlüssel, am besten so lange, wie der Klartext selber.

BASEL wurde mit dem Schlüssel OXMIY verschlüsselt.

Mögliche weitere Treffpunkte könnten folgende Städte sein:

Klartext:	PARIS	MAINZ	ATHEN	KABUL
Schlüssel:	AXNER	DXWZK	PEXIW	FXDSY
Geheimtext:	PXEMJ	PXEMJ	PXEMJ	PXEMJ

Tatsächlich kann man zu jedem Klartext-Wort mit 5 Buchstaben einen Schlüssel finden, der dieses Wort zu PXEMJ chiffriert. Das liegt einfach daran, dass der Schlüssel aus ebenso vielen frei wählbaren Buchstaben besteht wie der Klartext selber. Für den Spion sind das keine gute Nachrichten: Jede Stadt mit fünf Buchstaben könnte der Treffpunkt sein. Und wenn er nicht weiss, dass der Geheimtext einen Städtenamen enthält, sieht es für ihn noch schlimmer aus.

Haben wir damit etwa ein Kryptosystem gefunden, das nicht zu knacken ist? Im Prinzip ja, man muss dazu aber noch einige Punkte beachten:

- Der Schlüssel darf nur ein einziges Mal verwendet werden, denn sonst kann ein Spion, der mehrere Geheimtexte abfängt, wieder nach Wiederholungen suchen, wie beim Angriff auf die Vigenère-Verschlüsselung. Aus diesem Grund nennt man das Verfahren auch One-Time-Pad (Einmalblock)
- Der Schlüssel muss eine rein zufällig gewählte Buchstabenfolge sein. Um einen längeren Text zu verschlüsseln, muss ja auch der Schlüssel entsprechend lang gewählt sein. Würde man für den Schlüssel einen Satz wählen, den man sich leicht merken kann, dann wären die Buchstabenhäufigkeiten im Schlüssel nicht mehr gleichverteilt und würde somit für eine statistische Analyse anfällig.

Aufgaben

1) Wie viele mögliche Schlüssel mit 5 Buchstaben gibt es?
   Antwort: 26^5

2) Welcher Nachteil ergibt sich, wenn der Schlüssel die gleiche Länge hat, wie die Nachricht selber und nur einmal benutzt werden darf?
   Antwort: Jeder Schlüssel muss zuerst ausgetauscht werden. Egal, über welchen Kanal das geschieht, könnte man mit gleichem Aufwand auch gleich die Nachricht selber austauschen.

3) Der feindliche Spion hat mitbekommen, dass der Geheimtext PXEMJ ein Städtename ist, und er hat sich – so wie wir – eine Liste mit möglichen Städtenamen und dazugehörigen Schlüsseln gemacht.
   Die beiden Agenten tauschen jetzt eine weitere Nachricht aus, die den Namen der Person enthält, die sie beschatten wollen. Aus Nachlässigkeit verwenden sie den gleichen Schlüssel wie beim ersten Mal und der Spion kann die verschlüsselte Nachricht wieder abfangen. Sie lautet HFFCQ.
   Vervollständige die Tabelle und begründe, warum der Spion jetzt beide Nachrichten ohne Probleme entschlüsseln kann.

Geheimtext:	HFFCQ	HFFCQ	HFFCQ	HFFCQ	HFFCQ
Schlüssel:	AXNER	DXWZK	PEXIW	FXDSY	OXMIY
Klartext:	_____	_____	_____	_____	_____

   Antwort:

Geheimtext:	HFFCQ	HFFCQ	HFFCQ	HFFCQ	HFFCQ
Schlüssel:	AXNER	DXWZK	PEXIW	FXDSY	OXMIY
Klartext:	HISYZ	EIJDG	SBIUU	CICKS	TITUS

   Nur TITUS macht als Name Sinn. Somit kennt der Spion nun den Schlüssel OXMIY und kann auch die erste Nachricht mit dem Treffpunkt übersetzen.

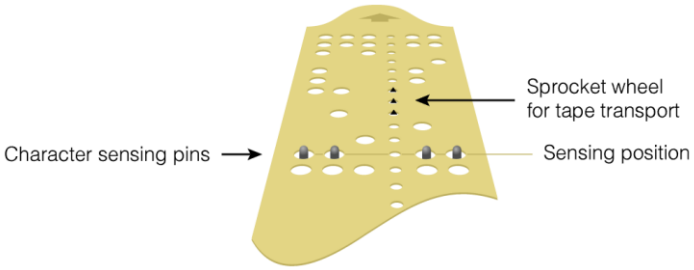
Hintergrund – Teil 2

Das One-Time-Pad wurde tatsächlich verwendet, z.B. mittels Lochstreifen. Diese Methode wird z.T. auch als One-Time-Tape bezeichnet. (Quelle: https://www.cryptomuseum.com/crypto/ott.htm)

Klartext-Tape und Schlüssel-Tape

Verschlüsselungs-Teleprinter («Mixer»)

Um eine Nachricht auf einen Lochstreifen zu schreiben, wurde der ITA-2 Standard (International Telegraph Alphabet No 2) verwendet, welcher 1963 durch den ITA-5 Standard (besser bekannt als ASCII) abgelöst wurde. Bei diesem Standard handelt es sich um eine öffentlich bekannte 5-bit Codierung und nicht um eine Chiffrierung. 5-bit bedeutet, dass damit maximal $2^5 = 32$ Zeichen dargestellt werden können. (Quelle: https://www.cryptomuseum.com/ref/ita2/index.htm)



Da man 26 Buchstaben, 10 Ziffern und noch etwa 10 Satz- und Sonderzeichen verwenden möchte, reichen 32 Zeichen nicht aus. Aus diesem Grund wurden Lochmuster doppelt belegt und durch spezielle Codes wird vorgängig angegeben, ob es sich um Buchstaben (`Ltr` = Letters) oder um Zahlen/Zeichen (`Fig` = Figures) handelt. Die Tabelle unten fasst die Codierung zusammen (1 = Loch, 0 = kein Loch).
(Quelle: https://www.cryptomuseum.com/ref/ita2/index.htm)

Ltr	Letters (A-Z)
Fig	Figures (Numbers and punctuation marks)
Ctrl	Control characters
Hex	Hexadecimal code
Bin [1]	Binary, Positions of the holes in the paper tape

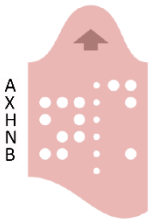
#	Ltr	Fig	Hex	Bin	
0	NUL		00	000·00	NULL, Nothing (blank tape)
1	E	3	01	000·01	
2	LF		02	000·10	Line Feed (new line)
3	A	-	03	000·11	
4	SP		04	001·00	Space
5	S	'	05	001·01	
6	I	8	06	001·10	
7	U	7	07	001·11	
8	CR		08	010·00	Carriage Return
9	D	ENC	09	010·01	Enquiry (Who are you?, WRU)
10	R	4	0A	010·10	
11	J	BEL	0B	010·11	BELL (ring bell at the other end)
12	N	,	0C	011·00	
13	F	!	0D	011·01	Can also be %
14	C	:	0E	011·10	
15	K	(	0F	011·11	
16	T	5	10	100·00	
17	Z	+	11	100·01	
18	L	)	12	100·10	
19	W	2	13	100·11	
20	H	$	14	101·00	Currency symbol — Can also be £
21	Y	6	15	101·01	
22	P	0	16	101·10	
23	Q	1	17	101·11	
24	O	9	18	110·00	
25	B	?	19	110·01	
26	G	&	1A	110·10	Can also be @
27	FIGS		1B	110·11	Figures (Shift on)
28	M	.	1C	111·00	
29	X	/	1D	111·01	
30	V	;	1E	111·10	
31	LTRS		1F	11·111	Letters (Shift off)

4) Der Klartext, den wir verschlüsseln wollen, sei HELLO. Du findest den Text auf dem gelben Lochstreifen.

Als Schlüssel wollen wir AXHNB verwenden.

a) Codiere den Schlüssel auf dem roten Papierstreifen.

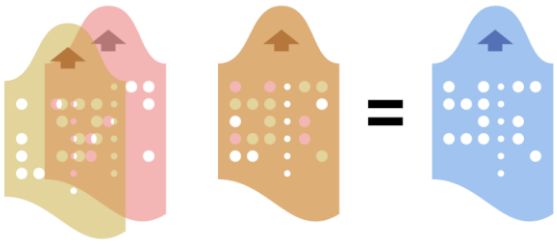
Antwort:



b) Lege nun die beiden Lochstreifen übereinander und halte sie gegen das Licht. Wir erzeugen den blauen Lochstreifen mit dem Geheimtext wie folgt:

- Wenn an einer Position nur der gelbe oder nur der rote Streifen ein Loch hat, dann stanze an dieser Position ein Loch in den blauen Streifen.
- Wenn an einer Position weder der gelbe noch der rote Streifen ein Loch haben, dann hat auch der blaue Streifen kein Loch an dieser Position.
- Wenn an einer Position sowohl der gelbe als auch der rote Streifen ein Loch haben, dann hat der blaue Streifen kein Loch an dieser Position.

Antwort:

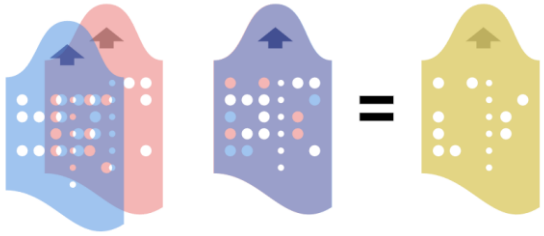


c) Wie lautet nun der Geheimtext auf dem blauen Streifen?

Antwort: QMIVE

d) Überlege dir nun, wie du aus dem blauen Geheimtext-Streifen und dem roten Schlüsselstreifen wieder den Klartextstreifen finden kannst.

Antwort:
Auf die gleiche Weise wie bei der Verschlüsselung:



(Quelle der Abbildungen: https://www.cryptomuseum.com/crypto/vernam.htm)

5) Jede Zeile des Lochstreifens stellt eine Binäre Ziffer dar, welche wiederum je einen Buchstaben chiffriert. Mit dem Trick des Übereinanderlegens, konntest du das Auflösen im Binärcode vermeiden, dies wollen wir in dieser Aufgabe nun tun.

a) Schreibe jeden Buchstaben des Wortes Hallo, des Schlüssels und des Geheimwortes je untereinander.

Buchstabe:	H	E	L	L	O
Binär Klartext:	101 00	000 01	100 10	_____	_____
Binär Schlüssel:	000 11	111 01	101 00	_____	_____
Binär Geheimtext:	101 11	111 00	_____	_____	_____

Antwort:

Buchstabe:	H	E	L	L	O
Binär Klartext:	101 00	000 01	100 10	100 10	110 00
Binär Schlüssel:	000 11	111 01	101 00	011 00	110 01
Binär Geheimtext:	101 11	111 00	001 10	111 10	000 01

b) Kannst du mit Hilfe der Beispiele aus Aufgabe 5a) erklären, wie man im Binärcode vom Klartext mit Schlüssel zum Geheimtext kommt ohne die Lochstreifen?

Antwort: Je nach Vorwissen Version i), ii) oder iii) als Antwort geben:

i) Benutze bitweise Binäre Addition ohne Übertrag
ii) Addiere bitweise modulo 2
iii) Wenn der Schlüssel 0 ist, passiert nichts, bei Schlüssel 1 switched das Bit.

c) Wie kommst du vom Geheimtext wieder zum Klartext?

Antwort: Gleich wie bei der Verschlüsselung, nur wendest du den Schlüssel umgekehrt auf den Geheimtext an.

d) Anna, Lisa und Maja kodieren ihre Namen mit ASCII und verschlüsseln diese mit einem dir unbekannten Schlüssel. Du fängst den Geheimtext
`101 01  111 11  000 00  101 01`
ab. Wieso kannst du nichts darüber aussagen, welchen Namen du abgefangen hast?

Antwort: Da der Schlüssel nicht bekannt ist, kann ich zu jedem Namen einen möglichen Schlüssel finden, der diesen Geheimtext ergibt. Die drei möglichen Schlüssel sind:

Anna:	`000 11`	`011 00`	`011 00`	`000 11`
mit Schlüssel:	`101 10`	`100 11`	`011 00`	`101 10`
Lisa:	`100 10`	`001 10`	`001 01`	`000 11`
mit Schlüssel:	`001 11`	`110 01`	`001 01`	`101 10`
Maja:	`111 00`	`000 11`	`010 11`	`000 11`
mit Schlüssel:	`010 01`	`111 00`	`010 11`	`101 10`

e) Nun fängst du noch einen zweiten Text ab, du weisst, dass derselbe Schlüssel verwendet wurde. Kannst du nun sagen, wessen Texte du abfängst?
Der zweite Geheimtext lautet: `100 00  011 10  010 00  100 01`

Antwort: Ja, nun ist es klar welches Mädchen die Texte schickt. Nur der dritte Schlüssel ergibt einen sinnvollen Text beim Übersetzen und zwar die Farbe
blau: `110 01  100 10  000 11  001 11`
Möchte man eine sichere Übertragung, darf der Schlüssel nur einmal gebraucht werden.

Zusammenfassung

Das One-Time-Pad bietet eine Möglichkeit die Vigenère-Verschlüsselung absolut sicher zu machen, dabei muss beachtet werden, dass

i) Der Schlüssel genau gleich lang ist wie der Text
ii) Der Schlüssel zufällig gewählt ist
iii) Der Schlüssel nur einmal verwendet wird

Diese Restriktionen sind so strickt, dass das One Time Pad kaum praktikabel ist.
Das One-Time-Pad lässt sich auch auf Binäre Zahlen mit entsprechenden Binären Schlüsseln anwenden. Historisch wurden Texte binär kodiert und auf Lochstreifen festgehalten. Mit Hilfe eines zweiten Lochstreifens, der den Schlüssel enthielt, konnten die Texte leicht verschlüsselt und wieder entschlüsselt werden.