Monoalphabetische Substitution

Als **monoalphabetische Substitution** (von griechisch: μόνο (*mono*) = „einzig“ und αλφάβητο (*alphabeto*) = „Alphabet“ sowie von lateinisch: *substituere* = „ersetzen“) bezeichnet man in der Kryptographie, also in dem Wissenschaftszweig der Kryptologie, der sich mit den Geheimschriften befasst, Verschlüsselungsverfahren, bei denen nur ein einziges (festes) Alphabet zur Verschlüsselung, also zur Umwandlung des Klartextes in den Geheimtext, verwendet wird.

Inhaltsverzeichnis

Prinzip

Die Buchstaben oder Zeichen oder auch Buchstabengruppen oder Zeichengruppen des Klartextes werden nach Vorgabe dieses einen Alphabets, das auch Schlüsselalphabet oder Geheimalphabet genannt wird, durch andere Buchstaben, Zeichen oder Gruppen ersetzt.

Klassische Beispiele für monoalphabetische Substitutionen sind die Caesar-Verschlüsselung und das Playfair-Verfahren. Im Gegensatz zur monoalphabetischen Substitutionen stehen die *polyalphabetischen Substitutionen*, bei denen zur Verschlüsselung mehrere (viele) verschiedene Alphabete verwendet werden. Beispiele hierfür sind die Vigenère-Verschlüsselung und die Schlüsselmaschine Enigma.

Beispiele

Einfache monoalphabetische Substitution

Ein Beispiel für eine monoalphabetische Verschlüsselung ist das folgende Verfahren: Hierbei werden einzelne Buchstaben des Klartextes mithilfe des Schlüsselalphabets in einzelne Zeichen des Geheimtextes substituiert. Diese Methode wird daher präzise als „monographische monoalphabetische monopartite Substitution“ oder schlicht auch als „einfache monoalphabetische Substitution“ bezeichnet.

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

Aus dem Klartext „wikipedia ist informativ“ wird nach Verschlüsselung der Geheimtext „ZSMSYWPSU STE SNDQVOUESH“. Der Klartext lässt sich durch Entschlüsselung wieder aus dem Geheimtext rekonstruieren, indem man dort die

Buchstaben in der zweiten Zeile durch die der ersten Zeile ersetzt. Der

Geheimtext, auch als Chiffrat bezeichnet, wird zur leichteren Unterscheidung vom Klartext zumeist mit Großbuchstaben geschrieben.

Caesar-Verschlüsselung

Hauptartikel: Caesar-Verschlüsselung

Dies ist ein Sonderfall der einfachen monoalphabetischen Substitution, wobei das zur Verschlüsselung verwendete Alphabet durch zyklisches Verschieben jedes einzelnen Buchstabens des Standardalphabets gewonnen wird. Die Anzahl der Plätze, um die verschoben wird, ist der Schlüssel. Schon Caesar benutzte dieses Verfahren, zumeist mit dem Schlüssel „C“, was einer Verschiebung um drei Buchstaben entspricht.

Beispiel für die Caesar-Verschlüsselung:

```
 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
```

Bei diesem Beispiel wird das Wort „wikipedia“ als „ZLNLSHGLD“ verschlüsselt.

Geheimalphabeterstellung

Es gibt unterschiedliche Methoden, um das zur Ver- und Entschlüsselung benötigte Geheimalphabet zu erzeugen. Besonders einfache (und besonders unsichere) Varianten sind

- Caesar-Verschiebung: Hier sind nur 25 verschiedene Schlüssel möglich.

Beispiel mit Schlüssel E, also Verschiebung um fünf Zeichen:

```
  Klar: abcdefghijklmnopqrstuvwxyz
Geheim: FGHIJKLMNOPQRSTUVWXYZABCDE
```

- Atbasch: Revertiertes Alphabet, nur ein einziger fester Schlüssel verfügbar:

```
  Klar: abcdefghijklmnopqrstuvwxyz
Geheim: ZYXWVUTSRQPONMLKJIHGFEDCBA
```

Daneben ist die Erzeugung eines verwürfelten Geheimalphabets mithilfe eines

Kennworts (Schlüssel) üblich. Vorteil dieser Methode ist, dass so eine Vielzahl von unterschiedlichen Geheimalphabeten gebildet werden kann, ohne dass man den Schlüssel in schriftlicher Form übermitteln müsste. Es genügt, dem befugten Empfänger das entsprechende Kennwort (Schlüssel) mündlich oder auf irgendeine andere (geheime) Weise zukommen zu lassen. Das Kennwort ist leicht zu merken und auf diese Weise gut vor Ausspähung geschützt. Sowohl Verschlüssler (Sender) als auch Entschlüssler (Empfänger) bilden auf gleiche Weise aus dem Kennwort das identische Geheimalphabet.

Beispielsweise vereinbaren sie als ihren geheimen Schlüssel das Kennwort „Regenschirmstaender“. Zunächst entfernen sie alle mehrfach auftretenden Buchstaben aus dem Kennwort. Aus „Regenschirmstaender“ wird so REGNSCHIMTAD. Diese Buchstaben bilden den Anfang des Geheimalphabets. Der Rest des Alphabets, also die im Kennwort nicht auftretenden Buchstaben werden rechts aufgefüllt (unten durch Fettdruck hervorgehoben). So erhält man als Geheimalphabet

```
  Klar: abcdefghijklmnopqrstuvwxyz
Geheim: REGNSCHIMTADBFJKLOPQUVWXYZ
```

Besser ist es, die restlichen Buchstaben nicht alphabetisch, sondern in umgekehrt alphabetischer Reihenfolge (revertiert) aufzufüllen. So vermeidet man den Nachteil, dass ansonsten das Geheimalphabet häufig (wie auch hier) mit ...XYZ endet. Durch revertierte Auffüllung der restlichen Buchstaben des Alphabets nach dem Kennwort ergibt sich so als Geheimalphabet:

```
  Klar: abcdefghijklmnopqrstuvwxyz
Geheim: REGNSCHIMTADZYXWVUQPOLKJFB
```

Als Alternative kann man auch die noch fehlenden Alphabetbuchstaben in alphabetischer Reihenfolge an den letzten Buchstaben des Kennworts anhängen (progressive Auffüllung) und so ein möglichst verwürfeltes Geheimalphabet erzeugen:

```
  Klar: abcdefghijklmnopqrstuvwxyz
Geheim: REGNSCHIMTADFJKLOPQUVWXYZB
```

Ebenso ist es denkbar, ein völlig zufällig verwürfeltes Geheimalphabet zu

verwenden. Nachteilig dabei ist allerdings, dass sich die beiden Partner dieses in der Regel nicht im Kopf merken können. Es muss also notiert werden und kann dann eventuell ausgespäht werden.

```
  Klar: abcdefghijklmnopqrstuvwxyz
Geheim: NKJSZWHMLAVYFCPTBQRUOGIDXE
```

Unter Verwendung des obigen Geheimalphabetes wird der Klartext „Wasser kocht im Teekessel“ in den Geheimtext „INRRZQ VPJMU LF UZZVZRRZY“ umgewandelt. Natürlich würde man vor Übermittlung des Geheimtextes zur Erschwerung der unbefugten Entzifferung die Leerzeichen entfernen und den Text als „Wurm“ „INRRZQVPJMULFUZZVZRRZY“ oder in Gruppen „INRRZ QVPJM ULFUZ ZVZRR ZY“ übermitteln.

Sicherheit

Im Gegensatz zur Caesarverschlüsselung mit nur 25 Möglichkeiten gibt es sehr viele Möglichkeiten zur Verwürfelung des Standardalphabetes: Der erste Buchstabe „A“ kann an eine von 26 mögliche Alphabetpositionen platziert werden. Für den zweiten Buchstaben „B“ gibt es dann noch 25 mögliche Plätze zur Auswahl, für den dritten 24, und so weiter. Insgesamt berechnen sich so $26 \cdot 25 \cdot 24 \cdot 23 \cdots 4 \cdot 3 \cdot 2 \cdot 1 = 26!$ (Fakultät) Möglichkeiten zur Verwürfelung des Alphabets. Das sind ungefähr $4 \cdot 10^{26}$ Fälle und entspricht etwa 88 bit. Demzufolge ist eine Entzifferung durch Ausprobieren aller Fälle (Brute-Force-Methode) praktisch unmöglich. Dennoch ist die monoalphabetische Substitution unsicher und leicht zu „knacken“. Selbst relativ kurze Geheimtexte, die monoalphabetisch verschlüsselt sind (dreißig bis fünfzig Zeichen reichen völlig aus), können mit Hilfe statistischer Untersuchungen (Häufigkeitszählungen) und durch Mustersuche entziffert werden.

Entzifferung

Häufigkeitsanalyse

Zur Entzifferung monoalphabetischer Verschlüsselungen ohne bekannten Schlüssel führt man eine Häufigkeitsanalyse der Buchstaben im Schlüsseltext durch und kann so auf gewisse Buchstaben schließen, woraus dann Wörter und

somit immer mehr Assoziationen zu Klartextbuchstaben gezogen werden können. (Einige Häufigkeitstabellen findet man unter Deutsches Alphabet.)

Beispiel:

```
Mjjp nop cni Hzgfzqosmqgr zqo scd Gjdkqpcmucmcngf. Cm rjddp tjd
ciabnogfci qis fcnoop vjcmpbngf qcucmocpyp: Vqmycb.
```

Buchstabenhäufigkeiten: 12,6 %: c, Jeweils 6,7 %: mp, 5,9 %: oq, 5 %: dgj Aus der Verteilung lässt sich vermuten, dass das e als häufigster Buchstabe durch c codiert ist. Damit ergibt sich folgendes:

```
Mjjp nop cni Hzgfzqosmqgr zqo scd Gjdkqpcmucmcngf. Cm rjddp tjd
Ciabnogfci qis fcnoop vjcmpbngf qcucmocpyp: Vqmycb.
.... ... e.. ............ ... .e. ......e..e.e.... E. ..... ...
E.......e. ... .e.... ..e...... .e....e...: ....e..
```

Nun wird nach Wortzusammenhängen gesucht. Wörter mit 3 Buchstaben und e in der Mitte sind in der Regel Artikel (*der*, *den*, *dem*, …), besonders, wenn sie mehrfach vorkommen; so lässt sich also auf das d schließen. Ein Wort mit 3 Buchstaben und e am Anfang ist oft *ein*. Hier gilt es auszuprobieren und die Schritte zu dokumentieren, so dass man bei Fehlern durch Backtracking weitermachen kann.

```
Mjjp nop cni Hzgfzqosmqgr zqo scd Gjdkqpcmucmcngf. Cm rjddp tjd
ciabnogfci qis fcnoop vjcmpbngf qcucmocpyp: Vqmycb.
.... i.. ein .......d.... ... de. ......e..e.e.... E. ..... ...
En..i...en .nd .ei... ..e...i.. .e....e...: ....e..
```

Daraus lassen sich leicht die Wörter *und* und *ist* entnehmen:

```
...t ist ein .....u.d.u.. .us de. ....ute..e.e.... E. ....t ...
En..is..en und .eisst ..e.t.i.. ue.e.set.t: .u..e..
```

Woraus sich mit etwas Phantasie und Übung leicht weitere Wörter und Buchstabenfolgen (wie *aus*, *sch*/*ch*, *en* etc.) und zu guter Letzt der Klartext schließen lassen:

```
...t ist ein Fachausd.u.. aus de. C...ute..e.e.ch. E. ....t ...
En..ischen und heisst ..e.t.ich ue.e.set.t: .u..e..
Root ist ein Fachausdruck aus dem Computerbereich. Er kommt vom
```

```
Englischen und heisst woertlich uebersetzt: Wurzel.
```

Die Entzifferung des Geheimtextes durch Auswertung der Buchstabenhäufigkeiten kann durch einen leipogrammatischen Text erschwert bis unmöglich gemacht werden. Dadurch, dass in einem leipogrammatischen Text einer oder mehrere Buchstaben nicht verwendet werden (z. B. Nichtverwenden von Wörtern mit *e*), verschiebt sich die ganze Buchstabenhäufigkeit, und ohne das Wissen um den/die vermiedenen Buchstaben kann keine oder nur eine stark erschwerte Auswertung erfolgen.

Klartextangriff (Mustersuche)

Hauptartikel: Mustersuche

Sind Teile des Klartextes bekannt (einzelne Begriffe), so kann man nach deren Muster im Geheimtext suchen, indem man beispielsweise nach Doppelbuchstaben Ausschau hält. Im Klar- sowie im Geheimtext sollten bei einer monoalphabetischen Substitution an denselben Stellen doppelte Zeichen vorkommen. In gleicher Weise kann man auch nach Mustern im Geheimtext suchen, die dem Muster des vermuteten Wortes entsprechen.

Beispiel:

```
Vermutet:    INTERNET
Geheimtext: WXMNASXUAXSXNA
'INTERNET' → 'NASXUAXS'
```

MAKE-PROFIT-Verschlüsselung

Diese sehr einfache monoalphabetische Verschlüsselung von *Ziffern* beruht darauf, dass Ziffern durch die ihnen zugeordneten Buchstaben aus dem leicht merkbaren Satz „MAKE PROFIT.“ ersetzt werden:

```
  Ziffern: 1 2 3 4 5 6 7 8 9 0
Schlüssel: M A K E P R O F I T
Beispiele: 3719346 87550 46025504 12892
           KOMIKER FOPPT ERTAPPTE MAFIA
```

Eine derartige Verschlüsselung ist weniger als Geheimcode geeignet, sondern

man benutzt den Schlüssel, um Buchstaben dort in Ziffern umzuwandeln, wo keine Buchstaben verwendet werden können oder verwendet werden sollen. Ein

Beispiel sind Typencodes in Katalogen[1] und Preisangaben in Listen für Verkäufer. Bei der Siemens AG, so der ehemalige Siemens-Manager Michael Kutschenreuter gegenüber der Staatsanwaltschaft in München, sei der Code im Zusammenhang mit Anweisungen zu Schmiergeldzahlungen auch als Geheimschlüssel verwendet worden.[2][3]

Verwandte Verschlüsselungsverfahren

Homophone Verschlüsselung
Die Klartextzeichen können durch unterschiedliche Geheimtextzeichen substituiert werden.

Playfair
Eine *bigraphische* monoalphabetische Substitution.

Polyalphabetische Substitution
Für die Zeichen des Klartextes werden „viele“ Geheimtextalphabete verwendet.

Polygrammsubstitution (auch: polygraphische Substitution)
Statt einzelner Klartextzeichen werden Zeichen-N-Gramme (beispielsweise Buchstabengruppen) substituiert.

Siehe auch

- Terminologie der Kryptographie

Literatur

- Friedrich L. Bauer: *Entzifferte Geheimnisse. Methoden und Maximen der Kryptographie.* 3. überarbeitete und erweiterte Auflage. Springer, Berlin u. a. 2000, ISBN 3-540-67931-6.
- Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone: *Handbook of Applied Cryptography*. CRC Press, Boca Raton FL u. a. 1996, ISBN 0-8493-8523-7, S. 17.
- Simon Singh: *Geheime Botschaften. die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet*. Hanser, München 2000, ISBN 978-3-446-19873-9

- Fred B. Wrixon: *Codes, Chiffren & andere Geheimsprachen – Von den ägyptischen Hieroglyphen bis zur Computerkryptologie*. Könemann, Köln 2000, ISBN 3-8290-3888-7, S. 168ff.

Weblinks

- CrypTool.de Freies Kryptologie-Lernprogramm CrypTool
- CrypTool-Online – Online-Verschlüsselung von Caesar und ca. 25 weiteren klassischen Verfahren
- Kryptographiespielplatz – Online-Verschlüsselung von Caesar und etlichen weiteren klassischen Verfahren
- Caesar-Verschlüsselung – Online-Caesar-Verschlüsselung
- MAKE-PROFIT-Verschlüsselung – Online-MAKE-PROFIT-Verschlüsselung
- Substitution Cipher Toolkit Anwendung, die mit monoalphabetischer Substitution verschlüsselte Texte *automatisch* entschlüsseln kann (Programmsprache ist Englisch)

Einzelnachweise

1. Beispiel: Codierung von Identifizierungsschlüsseln für Pistolen und Revolver im *Gun Stock Book Record* von Army & Navy Store Ltd. (London). Selbst dieser einfache Code wird häufig fehlerhaft beschrieben. In *Using the Army & Navy Co-Operative Society firearms records*. (PDF; 555 kB) University of Glasgow, Oktober 2008. ist T = 10 und S = 11, die Null könnte also nicht codiert werden. Auch in der deutschen Berichterstattung über die Anwendung des Codes bei Siemens wurde ein S zum Code hinzugefügt.

2. David Crawford, Mike Esterl: *At Siemens, witnesses cite pattern of bribery*. In: *The Wall Street Journal*, 31. Januar 2007. “Back at Munich headquarters, he [Michael Kutschenreuter] told prosecutors, he learned of an encryption code he alleged was widely used at Siemens to itemize bribe payments. He said it was derived from the phrase ‘Make Profit,’ with the phrase’s 10 letters corresponding to the numbers 1-2-3-4-5-6-7-8-9-0. Thus, with the letter A standing for 2 and P standing for 5, a reference to ‘file this in the APP file’ meant a bribe was authorized at 2.55 percent of sales. - A spokesman for Siemens said it has no knowledge of a ‘Make Profit’ encryption system.”

3. Christian Buchholz: *Der Code zum Schmiergeld.* In: *Manager-Magazin*, 8. Februar 2007, „… Das System, das unter anderem den meisten

Außendienstmitarbeitern im Vertrieb bekannt gewesen sein soll, hielt sich nach Informationen aus Unternehmenskreisen bis ins Jahr 1997 …“

In einer anderen Sprache lesen
