ISSN 1861-0641

IT-Sicherheit & Datenschutz

Ausgabe 07/06
21.07. – 18.08.2006

Zeitschrift für rechts- und prüfungssicheres Datenmanagement

Praxis – Anwendungen – Lösungen

Sicherheits- und Datenschutz-Management

Grundlagen – Technik und Methoden

EXTRA

Vorschriften – Gesetze – Urteile

Online-Service
www.it-sd.com

VOGEL

Der Informationsdienst für IT-Manager,
IT-Sicherheits- und Datenschutzverantwortliche.

Prof. Dr. Norbert Pohlmann, Malte Hesse

Kryptographie: Von der Geheimwissenschaft zur alltäglichen Nutzanwendung (II) – Elementare Verschlüsselungsverfahren

In der letzten Ausgabe haben wir in die Grundlagen der Kryptographie eingeführt. Diesmal betrachten wir elementare Verschlüsselungsverfahren in ihrer historischen Bedeutung und erläutern ihre Grundformen.

In der Geschichte haben elementare Verschlüsselungsverfahren über die Schicksale von Menschen und Gesellschaften entschieden. Heute spielen sie in ihrer klassischen Form nur noch beim Austausch von Nachrichten unter Freunden oder als Denksportaufgaben eine unterhaltsame Rolle. Wir wollen dennoch tiefer auf diese Verfahren eingehen und über kleine Übungsaufgaben den Zugang zu grundlegenden Ideen der Kryptographie erleichtern.

Die Betrachtung elementarer Verschlüsselungsverfahren ermöglicht den Zugang zu Grundideen der Kryptographie

Am einfachsten erläutern lassen sich diese am Beispiel der Verschlüsselung. Deren Ziel besteht darin, Daten in einer solchen Weise einer mathematischen Transformation zu unterwerfen, dass es einem Unbefugten unmöglich ist, die Original- aus den transformierten Daten zu rekonstruieren. Damit die verschlüsselten Daten für ihren legitimen Benutzer dennoch verwendbar bleiben, muss es diesem aber möglich sein, durch Anwendung einer inversen Transformation aus ihnen wieder die Originaldaten zu generieren. Die Originaldaten bezeichnet man als „Klartext“ (*clear text, plain text, message*), die transformierten Daten werden „Schlüsseltext“ (Chiffretext, Chiffrat, Kryptogramm, *cipher text*) genannt. Die Transformation heißt „Verschlüsselung“, ihre Inverse folglich „Entschlüsselung“.

Zu den elementaren Verschlüsselungsverfahren gehören zunächst alle Verfahren der Textverschlüsselung, bei denen Buchstaben oder Zeichen durch jeweils andere Buchstaben oder Zeichen ersetzt werden. Ein Beispiel aus der Geschichte liefert das Babington-Komplott von 1586, der Versuch, die protestantische englische Königin Elisabeth I. zu stürzen und durch ihre katholische Rivalin Maria Stuart, die schottische Throninhaberin, zu ersetzen, die zu dieser Zeit in einem Gefängnis in Derbyshire saß. Babington, ein ehemaliger Page Stuarts, und seine Mitverschwörer sendeten ihr verschlüsselte Briefe, die jedoch abgefangen und von dem Chiffrierungsexperten Thomas Phelippes entschlüsselt wurden, was zum Todesurteil gegen die schottische Königin und ihre Unterstützer führte.

Ein weiteres populäres Beispiel für elementare Verschlüsslungsverfahren und Basis für Hollywood-Filme ist die deutsche *Enigma*-Maschine aus dem Zweiten Weltkrieg. Diese elektromechanische Rotor-Schlüsselmaschine ver- und entschlüsselte mit Hilfe von Walzen. Bis zu ihrer endgültigen Kompromittierung durch den britische Mathematiker Alan Turing 1940 verrichtete die Enigma ihre Dienste besonders für die deutsche U-Boot-Flotte, danach profitierten die Alliierten. Die Entschlüsselung war von entscheidender Bedeutung für den weiteren Kriegsverlauf.

Monoalphabetische Substitution

Populär sind vor allem sog. Substitutionsverfahren, die jedes Zeichen des Klartextes nach einem festen Schema durch ein anderes ersetzen

Als erstes elementares Verfahren wollen wir die Substitution betrachten. Die monoalphabetische Substitution ist eine recht einfache Methode, um einen Klartext zu verschlüsseln. Dabei wird jedes Zeichen des Klartextes nach einem festgelegten Schema, der Verschlüsselungsvorschrift, durch ein anderes, ihm zugeordnetes Zeichen ersetzt (substituiert).
Die Verschlüsselungsvorschrift sieht vor, jeden Buchstaben des lateinischen Alphabets durch genau einen anderen zu ersetzen: I durch U, T durch Q, S durch P usw. Aus dem Klartext „ITSICHERHEIT“ wird der Schlüsseltext „UQPUXKLYKLUQ“. Bei einer anderen Verschlüsselungs-, also Zuordnungsvorschrift sieht auch der Schlüsseltext anders aus. Für dieses Verfahren lassen sich auch verschiedenartige Alphabete einsetzen, so können etwa lateinische Buchstaben und 26 ausgewählte chinesische Schriftzeichen verwendet werden.

Beispiel Verschlüsselungsvorschrift:

(1)	**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**
(2)	**G**	**W**	**X**	**V**	**L**	**O**	**A**	**K**	**U**	**B**	**C**	**N**	**D**	**R**	**M**	**F**	**H**	**Y**	**P**	**Q**	**T**	**Z**	**E**	**I**	**J**	**S**

Klartext:	**I**	**T**	**S**	**I**	**C**	**H**	**E**	**R**	**H**	**E**	**I**	**T**	
Schlüsseltext:	**U**	**Q**	**P**	**U**	**X**	**K**	**L**	**Y**	**K**	**L**	**U**	**Q**	

Derartige Kunstgriffe lenken jedoch nur notdürftig davon ab, dass die monoalphabetische Substitution sehr leicht zu brechen ist. Der Schlüssel dazu liegt in der charakteristischen Häufigkeit, mit der Buchstaben in natürlichen Sprachen auftauchen. Die folgende Tabelle zeigt diese Verteilung für das Deutsche:

A: 6,51	B: 1,89	C: 3,06	D: 5,08	E: 17,40	F: 1,66	G: 3,01	H: 4,76	I: 7,55
J: 0,27	K: 1,21	L: 3,44	M: 2,53	N: 9,78	O: 2,51	P: 0,79	Q: 0,02	R: 7,00
S: 7,27	T: 6,15	U: 4,35	V: 0,67	W: 1,89	X: 0,03	Y: 0,04	Z: 1,13	

Nach der Statistik kommt im Deutschen also das E am häufigsten vor, gefolgt von N, I, S, R usw. Diese Verteilung bleibt auch nach der monoalphabetischen Substitution erhalten, und mit ihrer Hilfe können Kryptoanalytiker aus dem Schlüsseltext den Klartext berechnen, vorausgesetzt, dass dieser in deutscher Sprache verfasst wurde.

Homophone Substitution

Man unterscheidet zwischen monoalphabetischer, homophoner und polyalphabetischer Substitution

Die homophone Substitution ist eine Verbesserung der monoalphabetischen Substitution. Die Verbesserung wird durch eine Verschleierung der Häufigkeit erreicht. Das heißt, die Verschlüsselungsvorschrift wird so gestaltet, dass alle Schlüsseltextzeichen mit der gleichen Wahrscheinlichkeit auftreten: Jedem Buchstaben ist eine Menge von Zeichen zugeordnet, und zwar so, dass die Anzahl der Schlüsseltextzeichen, die zu ihm gehören, seiner Häufigkeit entspricht. Demnach existieren für das E die meisten Zeichen, während für Raritäten wie X oder Y ein einzelner Ersatz ausreicht. Bei der Verschlüsselung wird der Klartextbuchstabe zufällig einem passenden Schlüsseltextzeichen zugeordnet. Da letztere zufällig gewählt werden, kommt jedes Zeichen gleich häufig vor.
Beispiel:
Der Klartext werde aus den 26 Großbuchstaben gebildet, der Schlüsseltext aus den Zahlen 1 bis 99 bestimmt. Die Zuordnung der Zahlen zu den Großbuchstaben hängt von der Häufigkeit der Buchstaben ab.

Klartext:	**Schlüsseltext:**
A	(10,21,52,59,71)
B	(20,34)
C	(28,06,80)
D	(19,58,70,81,87)
E	(09,18,29,33,38,40,42,54,55,60,66,75,85,86,92,93,99)
F	(00,41)
G	(08,12,97)
H	(01,07,24)
I	(14,39,50,65,76,88,94)
J	(57)
K	(23)
L	(02,05,82)
M	(27,11,49)
N	(30,35,43,62,67,68,72,77,79)
O	(26,53)
P	(31)
Q	(25)
R	(17,36,51,69,74,78,83)
S	(15,16,45,56,61,73,96)
T	(13,32,90,91,95,98)
U	(03,04,47)
V	(37)
W	(22)
X	(44)
Y	(48)
Z	(64)
Klartext:	K R Y P T O L O G I E
Schlüsseltext:	23 69 48 31 90 26 05 53 08 94 33

Fortsetzung auf Seite 337

Fortsetzung von Seite 332

In dem Beispiel werden die einzelnen Buchstaben durch zufällig ausgewählte Schlüsseltextzeichen substituiert, die ihnen zugeordnet sind: K durch 23, R durch 69 (möglich wären auch 17, 36 etc.), Y durch 48 usw.
Natürlich können auch homophone Substitutionen gebrochen werden. Ein Ansatz dafür basiert auf der Beobachtung, dass nicht nur einzelne Buchstaben, sondern auch bestimmte Buchstabenpaare statistisch gesehen häufiger vorkommen als andere, wie aus nachstehender Aufstellung hervorgeht. Diese Vorgehensweise ist natürlich noch längst keine vollständige Kryptoanalyse. Sie zeigt aber deutlich, dass auch ein auf den ersten Blick „praktisch unknackbares“ Verfahren sich bei näherem Hinsehen als durchaus angreifbar entpuppt. Dies ist ein weiteres Beispiel dafür, dass die Entwicklung von Kryptosystemen sehr komplex ist und erklärt, warum nur wenige Experten sie erfolgreich betreiben.

EN: 3,88	ER: 3,75	CH: 2,75	TE: 2,26	DE: 2,00
ND: 1,99	EI: 1,88	IE: 1,79	IN: 1,67	ES: 1,52

Polyalphabetische Substitution

Weitere Chiffriermethoden verschleiern die Häufigkeit noch stärker. Dazu zählen alle polyalphabetischen Substitutionsverfahren mit ihrer bekanntesten Methode, der Vignére-Verschlüsselung. Diese arbeitet mit einem Schlüssel, der aus einer Zeichenfolge besteht. Mit Hilfe der darin verwendeten Zeichen wird eine bestimmte Zeile einer Tabelle „angewählt“; darin wiederum ist jedem Klartextzeichen eine bestimmte Spalte zugeordnet. Der Kreuzungspunkt von Zeile und Spalte enthält dann das zugehörige Schlüsseltextzeichen. Ist der Schlüssel kürzer als das zu chiffrierende Klartextwort, wird er wiederholt. Die Entschlüsselung erfolgt auf umgekehrtem Weg und setzt die Kenntnis des Schlüssels voraus.
In **ABB.1** sehen wir ein Beispiel für eine solche Tabelle.
In diesem Beispiel werden die einzelnen Klartext-Zeichen schlüsselabhängig substituiert: D durch J, da das erste Zeichen des Schlüssels (G) dafür die entsprechende (siebte) Zeile bestimmt; A durch E, da das zweite Zeichen des Schlüssels die fünfte Zeile vorgibt – und so weiter bis zum letzten Buchstaben.

Obwohl es aufwändiger statistischer Analyse bedarf, können auch polyalphabetische Verfahren gebrochen werden. Ein genügend langer Schlüsseltext weist viele statistisch erfassbare Regelmäßigkeiten auf, die es ermöglichen, den Schlüssel zu ermitteln.

Alle drei Verfahren sind durch statistische Methoden relativ einfach zu brechen

Übung zum polyalphabetischen Substitutionsverfahren:

Sie können den Schlüsseltext einer Nachricht abfangen, von der Sie bereits den Klartext kennen. Sie gehen davon aus, dass auch

ABB. 1: Die erste Spalte des Schlüsseltextblocks steht für die Zeichen des Schlüssels.

```
Klartextzeichen:  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

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

Schlüssel:        G E H E I M G E H E I
Klartext:         D A T E N S C H U T Z
Schlüsseltext:    J E A I V E I L B X H
```

Schlüssel:	**?**
Klartext:	**D A T E N S C H U T Z**
Schlüsseltext:	**V I V L R J J L C M R**

zukünftige Nachrichten mit diesem Schlüssel übertragen werden. Wie lautet der Schlüssel, mit dem diese Nachricht verschlüsselt wurde?

Transpositionsverfahren

Eine weitere Gruppe bilden die Transpositionsverfahren, die auch in modernen Kryptosystemen noch eine Rolle spielen

Als letzte Gruppe elementarer Verschlüsselungsoperationen wollen wir die Methoden betrachten, bei denen einzelne Zeichen des Klartextes nach einer bestimmten Regel permutiert, d. h. vertauscht werden. Als Beispiel führen wir hier das Zick-Zack-Verfahren an. Der Klartext wird hierbei in einer Zick-Zack-Kurve, z. B. über fünf Zeilen verteilt, aufgeschrieben und anschließend zeilenweise von oben nach unten ausgelesen (die Fachleute sagen, der Schlüsselwert beträgt 5). Das sieht so aus:

Schlüssel: **Tiefe der Zick-Zack-Kurve (hier 5)**
Klartext: **D A T E N M A N A G E M E N T**

1	D								A						
2		A						N		G					
3			T				A				E				T
4				E		M						M		N	
5					N								E		

Schlüsseltext: **D A A N G T A E T E M M N N E**

In dem Beispiel werden die einzelnen Klartext-Zeichen permutiert: Das erste Zeichen D bleibt erhalten, das zweite Zeichen ist nun das neunte (A), das dritte Zeichen ist das zweite (erneut A), das vierte das achte (N) usw.

Auch für die Permutationsverfahren gilt, dass sie prinzipiell mit Hilfe der Kryptoanalyse entschlüsselt werden können. Dennoch werden wir erkennen, dass diese elementaren Verschlüsselungsoperationen in der modernen Kryptographie immer noch eine Rolle spielen.

Übung zum Transpositionsverfahren:
Sie wissen, eine Nachricht wurde mit dem Zick-Zack-Verfahren verschlüsselt. Es gelingt Ihnen, den Schlüsseltext abzuhören. Wie lautet der Klartext?

Hinweis: Die Tiefe der Zick-Zack-Kurve kennen Sie nicht, das heißt, Sie müssen mehrere Tiefen ausprobieren, um ein sinnvolles Ergebnis zu erzielen.

Schlüsseltext: **IÜTINFRE–ETS––NSHTTIRIRIUNECETTH**

Ausblick

In der nächsten Ausgabe gehen wir auf symmetrische Verschlüsselungsoperationen ein, wie sie heute in sehr vielen Anwendungen verwendet werden. Bis dahin wünschen wir Ihnen viel Vergnügen bei der Auflösung. Die Lösungen zu den Übungen finden Sie unter http://www.internet-sicherheit.de/lehre-ergebnisse.html. Für diejenigen, die tiefer in das Thema einsteigen wollen, empfehlen wir das frei erhältliche Lernprogramm CrypTool, welches bei der Kryptoanalyse und dem Verständnis von Verschlüsselungsverfahren hilft. Dieses Tool finden Sie unter www.cryptool.de.

Zu den Autoren:
Prof. Dr. Norbert Pohlmann ist Geschäftsführender Direktor des Instituts für Internet-Sicherheit der Fachhochschule Gelsenkirchen
E-Mail-Kontakt: norbert.pohlmann@informatik.fh-gelsenkirchen.de

Malte Hesse ist Mitarbeiter am Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen. E-Mail-Kontakt: hesse@internet-sicherheit.de