Idee der polyalphabetischen Chiffrierung

Bei polyalphabetischer Chiffrierung wird - wie bei der monoalphabetischen - jeder Buchstabe durch eine Substitution verschlüsselt, die durch ein permutiertes Alphabet beschrieben wird. Allerdings wird für jeden Buchstaben, abhängig von seiner Position im Klartext, ein anderes Alphabet verwendet.

Somit durchbricht die polyalphabetische Chiffrierung die Invarianzen, die zur Kryptoanalyse der monoalphabetischen Substitution geführt haben:

- Buchstabenhäufigkeiten,
- Paarhäufigkeiten usw.,
- Zeichenmuster.

Dieses Verfahren galt bis weit ins 19. Jahrhundert als unbrechbar, in seinen besonders sicheren Versionen mit Hilfe von Verschlüsselungsmaschinen sogar bis zum Beginn des Computerzeitalters. Dennoch wurde es selten verwendet, da es bei manueller Ausführung einige Konzentration erfordert. Auch die Arroganz der »Praktiker« mit Abwertung der »Theoretiker« spielte laut KAHN dabei eine Rolle - die man auch heute noch in Form von kryptographischem Analphabetismus weit verbreitet findet.

Schlüssel einer monoalphabetischen Substitution

Bei der monoalphabetischen Substitution war der Schlüssel eine Permutation $\sigma \in \mathbf{S}(\Sigma)$. Er wurde eindeutig durch die Folge der substituierten Zeichen des Alphabets beschrieben, also mathematisch duch die Familie $(\sigma(s))_{s\in\Sigma}$.

Beispiel für das Standard-Alphabet Σ = {A, ..., Z}:

a) Darstellung als Permutation:

```
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 F G H I J K M N W S T U V W X Y Z P A R O L E
```

b) ... oder nur durch das permutierte Alphabet:

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

Die Bezeichnung »monoalphabetisch« kommt daher, dass die gesamte Verschlüsselungsfunktion durch dieses eine (permutierte) Alphabet beschrieben wird.

Schlüssel einer polyalphabetischen Substitution

Schreibt man mehrere solcher permutierten Alphabete auf (am besten untereinander) und verwendet sie der Reihe nach, das erste für den ersten Klartextbuchstaben, das zweite für den zweiten, usw., so führt man eine polyalphabetische Verschlüsselung aus. Sind die Alphabete aufgebraucht, bevor der Klartext zu Ende ist, beginnt man wieder mit dem ersten Alphabet - das Verfahren heißt dann **periodische polyalphabetische Verschlüsselung**.

Beispiel: Standard-Alphabet + 5 permutierte Alphabete:

```
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

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

Damit wird verschlüsselt:

```
UNIVERSITAETMAINZ          = Klartext
S    J    W    X          aus Zeile 1
 Y    N    Q    I         aus Zeile 2
  Y    Y    K             aus Zeile 3
   F    Z    U            aus Zeile 4
    E    S    Q           aus Zeile 5
-----------------
SYYFEJNYZSWQKUQXI          = Geheimtext
```

Klassifizierung polyalphabetischer Chiffren

... nach drei (unabhängigen) Merkmalspaaren:

- **periodisch**,
- **aperiodisch**,

je nachdem, ob die Alphabete zyklisch wiederholt werden oder unregelmäßig bis gar nicht.

- **unabhängige Alphabete**,
- **Primäralphabet + Begleitalphabete**,

wobei Begleitalphabete nach einem gegebenen Schema aus dem Primäralphabet gebildet werden - im obigen Beispiel durch Verschiebung. Wenn man genau hinsieht, erkennt man, dass die Verschiebungen durch das Wort »KLAUS« charakterisiert sind.

- **Alphabetauswahl progressiv**,
- **Alphabetauswahl schlüsselgesteuert**,

je nachdem, ob die Alphabete der Reihe nach verwendet werden oder die Auswahl, wie im Beispiel, durch ein Schlüsselwort beschrieben wird.

Im allgemeinen hat man also eine Menge von Alphabeten (es können höchstens $n!$ verschiedene sein), aus denen man eine Folge auswählt -- periodisch oder nicht. Meistens werden genau n Alphabete so gewählt, dass jedes mit einem anderen Anfangsbuchstaben beginnt; die Alphabetauswahl geschieht dann anhand eines Schlüssels, entweder eines kurzen Worts, das periodisch wiederholt wird, oder eines langen Textes, der mindestens so lang ist wie der zu verschlüsselnde Klartext.

Autor: Klaus Pommerening, 11. November 1999; letzte Änderung: 17. Juli 2002

E-Mail an Pommerening@imsd.uni-mainz.de.