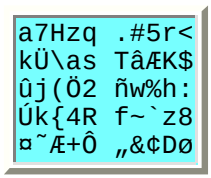
Kryptologie

Die Erfindung der polyalphabetischen Verschlüsselung



Polyalphabetische Verschlüsselung in der Renaissance

- Leon Battista ALBERTI (1404 - 1472) [Bild1, Bild2]
  - »Vater der neuzeitlichen Kryptographie«.
  - 1466: Drehscheibe mit einem festen permutierten Alphabet.
  - [ALBERTI gilt außerdem als Vater der neuzeitlichen Architektur. Unter anderem stammt von ihm ein Verfahren zum perspektivischen Zeichnen mit Hilfe von Gitterlinien.]
- TRITHEMIUS (Johannes von Heydenberg aus Trittenheim/Mosel, 1462 - 1516)
  - Steganographia (1499 - erst 100 Jahre später gedruckt) (Drehscheibe mit Standardalphabet).
  - Polygraphiae (1508 - erstes gedrucktes Buch über Kryptographie): tabula recta (»Vigenère-Tableau«).
  - [Gemisch aus Kryptographie und anderen »Geheimwissenschaften« wie Alchimie.]
- Jacopo SILVESTRI
  - Opus Novum (1528 - zweites gedrucktes Buch über Kryptographie).
  - Sehr viel konkreter und praxisorientierter als die Schriften von Trithemius; Drehscheibe, Raster, Kryptoanalyse.
- Giovan Battista BELASO
  - 1553: Auswahl des verschobenen Alphabets nach Schlüsselwort.
- Giovanni Battista PORTA (1535 - 1615)
  - 1563: Allgemeine Idee der polyalphabetischen Chiffrierung,
  - Drehscheibe + Schlüsselwort.
  - [Die allgemeine Idee wurde als nicht handhabbar angesehen; umgesetzt wurden nur Verfahren mit Primär- und durch Verschiebung gewonnenen Begleitalphabeten.]
- Blaise de VIGENÈRE (1523 - 1596)
  - Traicté des Chiffres 1585: Tabelle wie TRITHEMIUS, aber mit permutiertem Alphabet.
  - Autokey- Verschlüsselung (»autoclave«).
- Giovanni Battista ARGENTI (? - 1591)
  - Kryptoanalyse des BELASO-Verfahrens durch Schlüsselraten.
- Matteo ARGENTI (1561 - ?) - Neffe von G. B.
  - Manual der Renaissance-Kryptologie.

Die Entwicklung von der monoalphabetischen zur polyalphabetischen Substitution ist (spekulativ) in folgenden Schritten nachzuvollziehen:

- Monoalphabetische Verschlüsselung mit Permutationstafel.
- Drehscheibe mit fester Einstellung als Ersatz für die Permutationstafel.
- Leichter Alphabetwechsel durch andere Einstellung der Scheibe.
- Alphabetwechsel *innerhalb* einer Nachricht (ALBERTI).
- Progressiver Alphabetwechsel nach jedem Buchstaben (TRITHEMIUS).
- Schlüsselabhängiger Alphabetwechsel nach jedem Buchstaben (BELASO).
- Allgemeine polyalphabetische Verschlüsselung (PORTA).

TRITHEMIUS-Tafel (»VIGENÈRE-Tableau«)

[Üblicherweise fälschlich nach VIGENÈRE benannt]

Sie besteht aus *n* Zeilen; in der ersten Zeile steht das verwendete Alphabet Σ, in jeder weiteren Zeile das um einen weiteren Platz verschobene Alphabet. Für das Standard-Alphabet {A...Z} sieht das also so aus:

```
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 Z
```

Bei Trithemius wurde sie progressiv verwendet, d. h., die *n* Alphabete wurden der Reihe nach für die einzelnen Klartextbuchstaben verwendet, mit zyklischer Wiederholung.

(Da kein echter Schlüssel im Spiel ist, kann man in unserem Sinne eigentlich nicht von »Verschlüsselung« reden; die Sicherheit des Verfahrens beruht nur auf der Ahnungslosigkeit der Gegner.)

Trotz dieser Einfachheit bringt das Verfahren einen riesigen Fortschritt gegenüber der monoalphabetischen Verschlüsselung: Jeder Buchstabe wird im Mittel gleich oft mit jedem anderen chiffriert - die Buchstabenhäufigkeiten im Geheimtext sind völlig gleichverteilt!

Die BELASO-Chiffre (»VIGENÈRE-Chiffre«)

[Ebenfalls üblicherweise fälschlich nach VIGENÈRE benannt]

Sie verwendet ebenfalls die Trithemius-Tafel, als Alphabet wird aber jeweils die Zeile gewählt, die mit dem aktuellen Buchstaben des Schlüsselworts beginnt. Da ein Schlüssel verwendet wird, handelt es sich also um eine echte Chiffre.

Beispiel: Schlüssel `MAINZ`

Das bedeutet: Der 1., 6., 11., ... Buchstabe des Klartexts wird mit der Zeile »M« verschlüsselt, der 2., 7., 12., ... Buchstabe mit der Zeile »A«, usw.

Das läuft auf eine periodische CAESAR-Addition des Schlüsselworts hinaus:

```
p o l y a l p h a b e t i s c h
M A I N Z M A I N Z M A I N Z M
-----------------------------
B O T L Z X P P N A Q T Q F B T
```

Allgemein ist die BELASO-Chiffre also für eine Gruppenstruktur auf dem Alphabet Σ definiert; für den Schlüssel $k = (k_0,...,k_{l-1}) \in \Sigma^l$ ist dann die

Verschlüsselung: $c_i = a_i * k_{i \bmod l}$,

Entschlüsselung: $a_i = c_i * (k_{i \bmod l})^{-1}$.

Autor: Klaus Pommerening, 11. Juli 1977; letzte Änderung: 12. August 2002.

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