Beale 1.0
Programm zum Chiffrieren und Dechiffrieren

Willi Amberg
Klasse 9a

Ursulinen-Gymnasium Mannheim

„Beale 1.0“

Ziel für das Programm „Beale 1.0“ ist

Vorteile der Buchverschlüsselung

- Code schwierig zu brechen
- Hohe Sicherheit

und der Monoalphabetischen Verschlüsselung

- Einfache Programmierung

zu kombinieren

Der Schlüssel…

… nicht ein Buch,

sondern ein abgewandeltes … **Pangramm**

- Verwendetes Pangramm enthält z.B. die Buchstaben

  e, n, i, r, s, a, t

  „entsprechend“ ihrer Häufigkeit in der deutschen Sprache

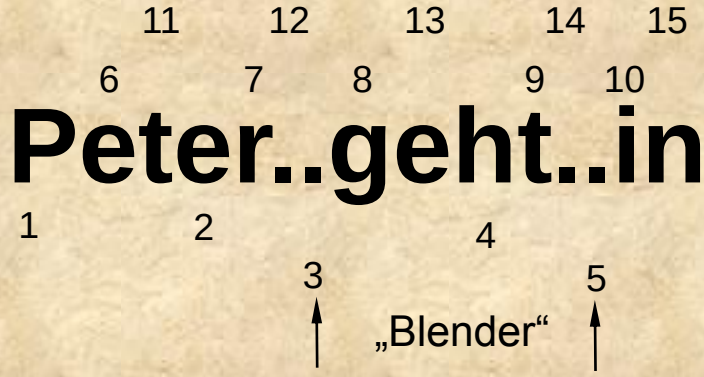
- **Jedem** Buchstaben des Pangramms wird eine Zahl zugeordnet (→ Homophone)

Pangramm Nummerierung

„Pangramm 3SB“ Verschlüsselung

- Buchstaben inklusive aller Spacer werden im „3“er Abstand nummeriert (**3**)*
- Zwei Wörter werden durch 2(!) Leerzeichen getrennt
  - → 1. Leerfeld = „Spacer“ (**S**)*
  - → 2. Leerfeld = „Blender“ (sinnloses Zeichen) (**B**)*

Beispiel:



* *Abstand/Anzahl Spacer und Blender beliebig wählbar z.B. „4S2B“*

Vorteile der „Pangramm3SB-Verschlüsselung“

- Schlüssel einfach zu behalten (lustiger Satz)
- Häufigste Buchstaben erhalten die meisten Homophone
  → Beispiel: „e“ hat 10 verschiedene Zahlen
- Leerzeichen des Pangramms können ebenfalls Zahlen zugeordnet werden
  → Leerzeichen im Klartext können mit-codiert werden
- Es können „Blender“ codiert werden

- Häufigkeitsanalyse wird deutlich schwieriger
- Programmierung relativ „einfach“

Problemfeld Häufigkeitsanalyse

Häufigste Homophone: e = 10; n = 5; i = 6, r = 6; s = 4;
a = 4; t = 7; Leerzeichen = 10

→ Entsprechende Häufigkeiten von

- Einzelnen Buchstaben,
- Bigrammen,
- Trigrammen und
- Leerzeichen

Werden stark reduziert

Beispiel „ein“: insgesamt 10x6x5 = 300 Möglichkeiten *

** Häufigkeiten weiterer n-Gramme siehe Ende*

Speziell Berücksichtigt:

- Wichigste Homophone werden zufällig gewählt
  - Verwendung von Homophonen wird bis zu 200 x zufällig gewählt
- Bigramm „CH“ und Trigramme „ICH“, „UND“ werden mit Blendern verschleiert.
- Pangramm durch spezielle Nummerierung gesichert (siehe oben)

Angestrebte Verbesserungen für "Beale 2.0"

- Verwendung der Homophone über „Zufalls-Funktion“
- Besseres Verschleiern von speziellen Bi/Trigrammen
- Einführen von „Spreizern“ (zwei/drei Buchstaben durch eine Zahl ersetzen)
- Einfügen von „Blendern“ über Zufalls-Funktion an beliebiger Stelle des Textes
- Pangramm optimieren
- Automatische Nummerierung von Pangrammen
- Codierung von Sonderzeichen/Zahlen ?
- … Vorschläge von der Jury

Häufigkeit der Homophone:

Buchstabe	rel. Häufigkeit	Buchstabe	rel. Häufigkeit
E	~ 1.7 %	O	~ 1.3 %
N	~ 2.0 %	B	~ 1,9 %
I	~ 1.3 %	W	~ 1,9 %
S	~ 1.8 %	F	~ 1,7 %
R	~ 1,2 %	K	~ 1,2 %
A	~ 1.4 %	Z	~ 1,1 %
T	~ 0.9 %	P	~ 0.8 %
D	~ 2.5 %	V	~ 0.7 %
H	~ 2.4 %	J	~ 0.3 %
U	~ 2.1 %	Y	~ 0.04 %
L	~ 1.7 %	X	~ 0,03 %
C	~ 1.5 %	Q	~ 0,02 %
G	~ 3.0 %	Leerzeichen	~ 1.9 %
M	~ 1.3 %	Blender	~ 1.7 % *

* Verwendungsabhängig

Kombinationsmöglichkeiten der Homophone für wichtige Bigramme

Bigramm	Häufigkeit in 1000	Mögl. Kombinationen
en	39	50
er	38	60
ch	28	4 *
te	23	70
de	20	40
nd	20	10 *
ei	19	60
ie	18	60
in	17	30
es	15	40

** ohne Blender*

→ Bigramme „ch/nd“ über Blender verschleiern

Kombinationsmöglichkeiten der Homophone für wichtige Trigramme

Trigramme	Häufigkeit in 10000	Mögl. Kombinationen
ein	122	300
ich	111	36 *
nde	89	50 *
die	87	120
und	87	20 *
der	86	120
che	75	40 *

** ohne Blender*

→ Trigramme „ich/und“ über Blender verschleiern

„Beale 1.0“

Ausdruck des Programms