Sage Praxis
u23 2015

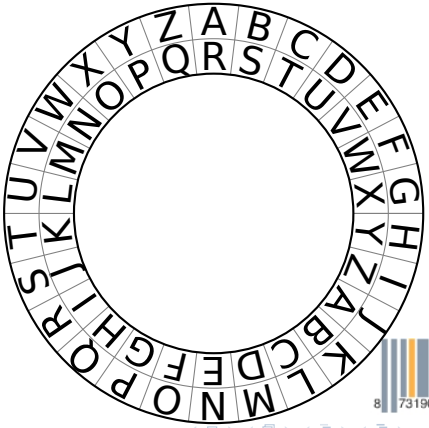
Simon, Florob

Chaos Computer Club Cologne e.V.
https://koeln.ccc.de

Cologne
2015-10-04

Caesar-/Verschiebungschiffre

- klassiche Substitutionschiffre
- ordnet jedem Buchstaben den Buchstaben n Positionen später im Alphabet zu
- beim überschreiten des ’Z’ wird veim ’A’ fortgesetzt
- verbreitet:
  - $n = 13$: rot13
  - $n = 17$: caesar



Siomon <schneid@cs.uni-bonn.de>, Florob <florob@babelmonkeys.de>

Caesar: Aufgaben

1. Ver- und Entschlüssele eine Nachricht mittels des Caesar Chiffres
2. Zähle die Häufigkeit jedes Zeichens in Klartext und Geheimtext; Vergleiche die Verteilungen
3. Entschlüssele die Geheimtexte in `http://trillian/ftp/u23-crypto/Caesar/`

Siomon <schneid@cs.uni-bonn.de>, Florob <florob@babelmonkeys.de>

Vigenère

- klassiche Substitutionschiffre
- zu dem Text wird ein sich wiederholendes Schlüsselwort “addiert”
- Verfahren bei der Addition pro Zeichenpaar wie Caesar

	T	O	B	E	O	R	N	O	T	T	O	B	E	…
⊕	K	E	Y	K	E	Y	K	E	Y	K	E	Y	K	…
	D	S	Z	O	S	P	X	S	R	D	S	Z	O	…

Siomon <schneid@cs.uni-bonn.de>, Florob <florob@babelmonkeys.de>

Vigenère: Aufgaben

1. Ver- und Entschlüssele eine Nachricht mittels des Vigenère-Chiffres
2. Zähle die Häufigkeit jedes Zeichens in Klartext und Geheimtext
3. Zerteile den Klartext und Geheimtext in Blöcke, welche genau so lang sind wie der verwendete Schlüssel
4. Betrachte jeweils nur das *i*-te Zeichen jedes Blocks; Zähle jeweils die Häufigkeit jedes Zeichens in Klartext und Geheimtext; Vergleiche die Verteilungen
5. Entschlüssele die Geheimtexte in `http://trillian/ftp/u23-crypto/Vernam/`
   - `enc1.txt`: Schlüssellänge 5
   - `enc2.txt`: Schlüssellänge 8
   - `enc3.txt`: Schlüssellänge 4

Vernam-Chiffre/One-Time-Pad

- Variante des Vigenère Verfahrens, bei dem das Schlüsselwort genau so lang ist wie der Klartext
- Wird der Schlüssel echt Zufällig erzeugt nennt sich dieses Verfahren One-Time-Pad
- One-Time-Pads sind beweisbar perfekt sicher (nach Shannon)
- Heutzutage meistens auf Bit-Ebene (Alphabet der Größe 2, statt 26)

Siomon <schneid@cs.uni-bonn.de>, Florob <florob@babelmonkeys.de>

Vernam: Aufgaben

1. Schreibe eine Funktion die eine zufällige Zeichenkette mit gegebener Länge erzeugt: randstr$(n) \in \{A, \cdots, Z\}^n$
2. Ver- und Entschlüssele eine Nachricht mittels des Vernam-Chiffres

Siomon <schneid@cs.uni-bonn.de>, Florob <florob@babelmonkeys.de>