Top Secret #1

Symmetrische, klassische Verschlüsselungsverfahren

ARJ/9-2015

Schon der Julius...

...kannte den folgenden Trick und nutze ihn bei seinen geheimen Botschaften:

"Ersetze jeden Buchstaben durch den, der drei Stellen später im Alphabet folgt!"

"Dqjulii huirojw cxu Whhchlw"

Bald schon aber...

...war Cäsar's Trick durchschaut und der gute Mann musste bei seiner Rotationschiffre nachlegen:

"Qre Jhresry vfg trsnyyra"

Was war damit gemeint?

Aber Stopp! Nicht einfach drauflosprobieren! Nutzen sie die Tatsache, dass in der deutschen Sprache das "e" am häufigsten vorkommt!

Vigenère-Verschlüsselung

Schlüssel \ Text	A	B	C	D	E	F
B	C	D	E	F	A
C	D	E	F	A	B
D	E	F	A	B	C
E	F	A	B	C	D
F	A	B	C	D	E

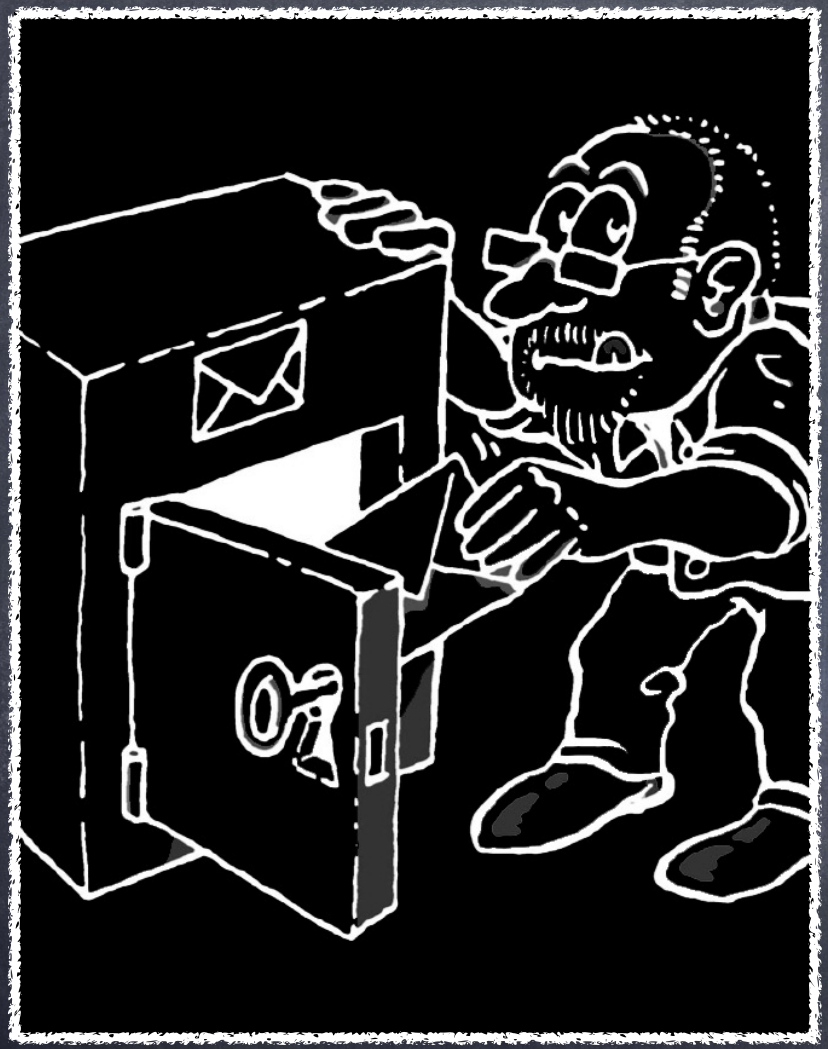
Sollte das Wort "BEEF" mit dem Schlüssel "AFFE" chiffriert werden, ergibt das den Geheimcode "BDDD"
Sollte der Schlüssel kürzer als der Text sein, so wird dieser einfach wiederholt!

Vigenère-Verschlüsselung

Das vollständige Vigenère-Quadrat enthält alle 26 Buchstaben!

Was bedeutet die Chiffre "WRKXQT", wenn das Schlüsselwort "SECRET" heisst?

Funktioniert hier die Häufigkeitsanalyse auch?



Zusammenfassung

Symmetrische Verschlüsselung:
Wir verschlüsseln und entschlüsseln mit demselben Schlüssel

Sehen sie dabei eine Problematik?

- Wie erfolgt die Schlüsselübergabe?
- Wieviele Schlüssel werden bei z.B. 20 Personen nötig?

Zusammenfassung

Symmetrische Verschlüsselung

- Wie erfolgt die Schlüsselübergabe:
  Auf geheimem Weg

- Wieviele Schlüssel werden bei z.B.
  20 Personen nötig:
  S=n*(n-1)/2
  S=Schlüssel, n=Teilnehmer
  Die Schlüsselzahl wächst
  quadratisch!
  20 Personen = 190 Schlüssel

Ergänzungen:

- **Kryptologie**: Wissenschaft vom Entwurf, der Anwendung und der Analyse von kryptografischen Verfahren

- **Kryptografie**: Wie kann eine Nachricht ver- und entschlüsselt werden?

- **Kryptoanalyse**: Wie sicher ist ein Verschlüsselungsverfahren?

Die Akteure:

Alice (Sender)

Eve (Lauscherin)
Mallory (Angreifer)

Bob (Empfänger)