Mtarvqitcrjkg

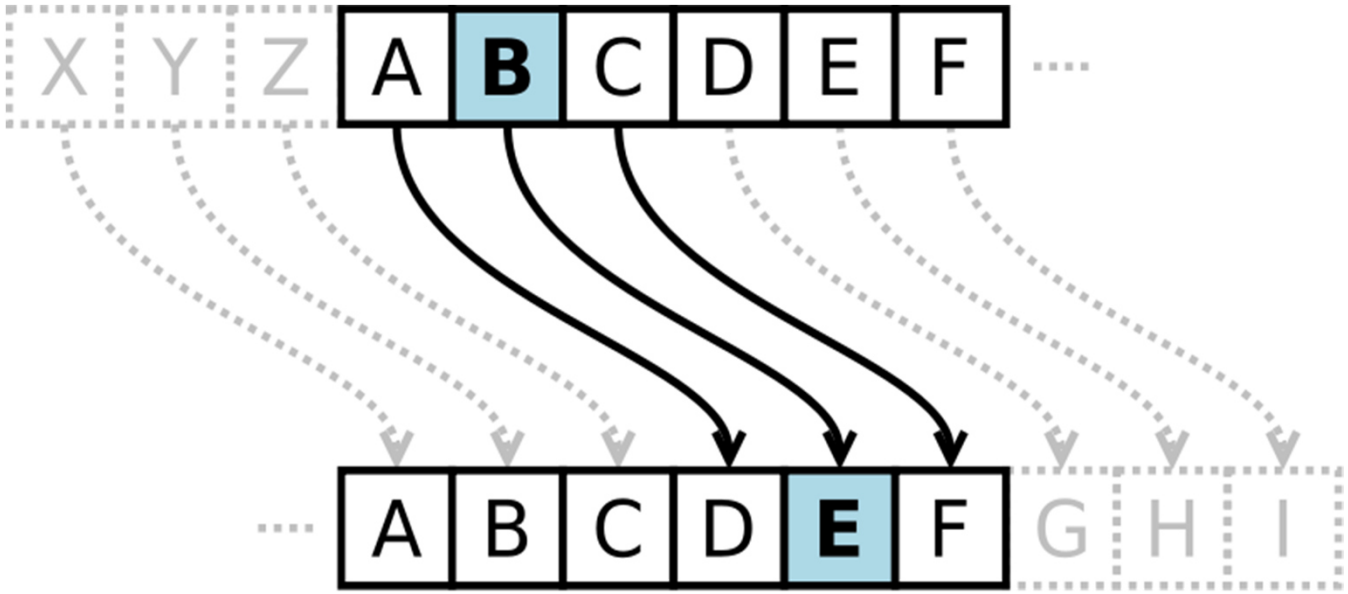
Kryptographie

Romeo und Julia

JGEWG AUZ DAWTW VAUZ

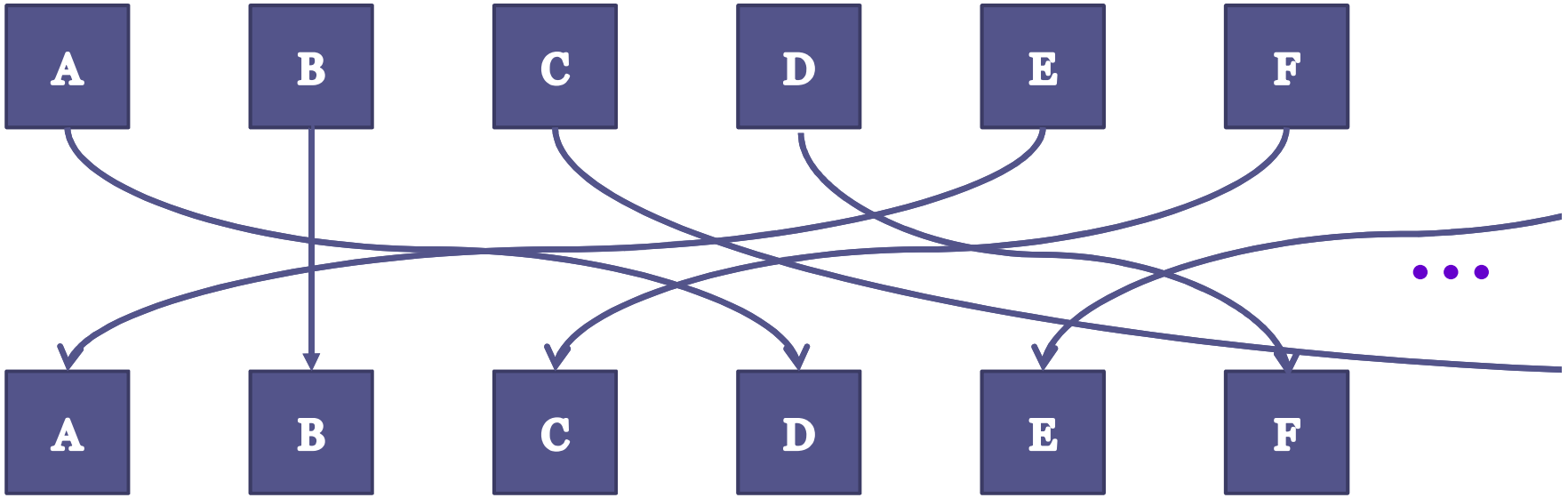
Verschiebung

AKA Caesar Verschlüsselung



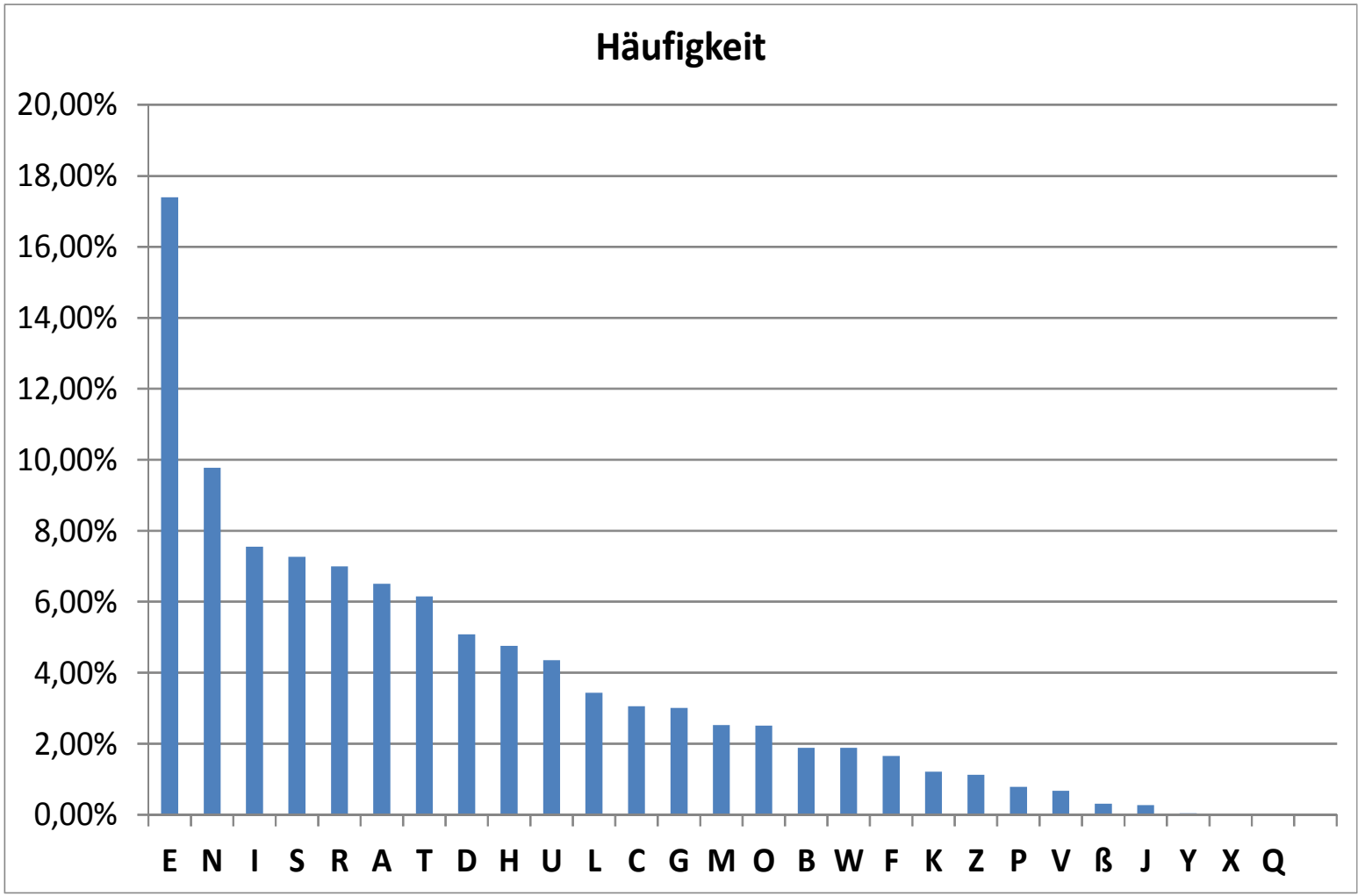
Autor: Cepheus
Public domain
https://commons.wikimedia.org/wiki/File:Caesar3.svg

Substitution



Ersetzung (Substitution) von Buchstaben durch andere ohne erkennbares Muster

Kryptoanalyse



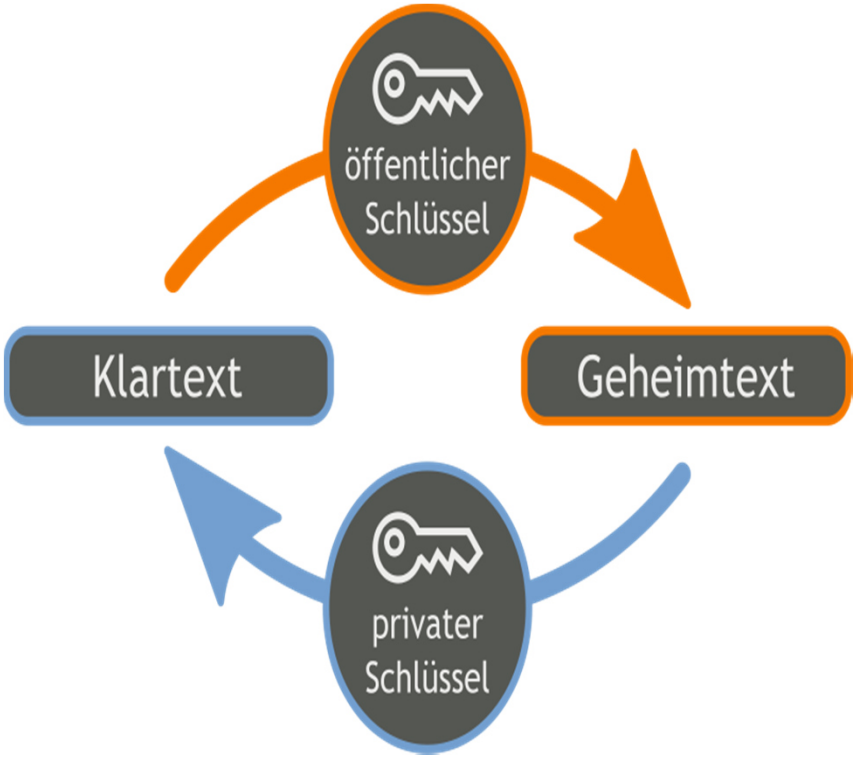
Schlüsselaustausch

RSA Kryptosystem: Geschichte

- 1978 Public-Key-Algorithmus (ziemlich sicher)
- Entwickelt von : Rivest, Shamir, Adleman

Asymmetrische Verschlüsselungsverfahren

- Einwegfunktion (Erzeugung der Schlüssel)
- Nachrichtenaustausch ohne privaten Schlüssel zu vermitteln



RSA Kryptosystem: Verfahren

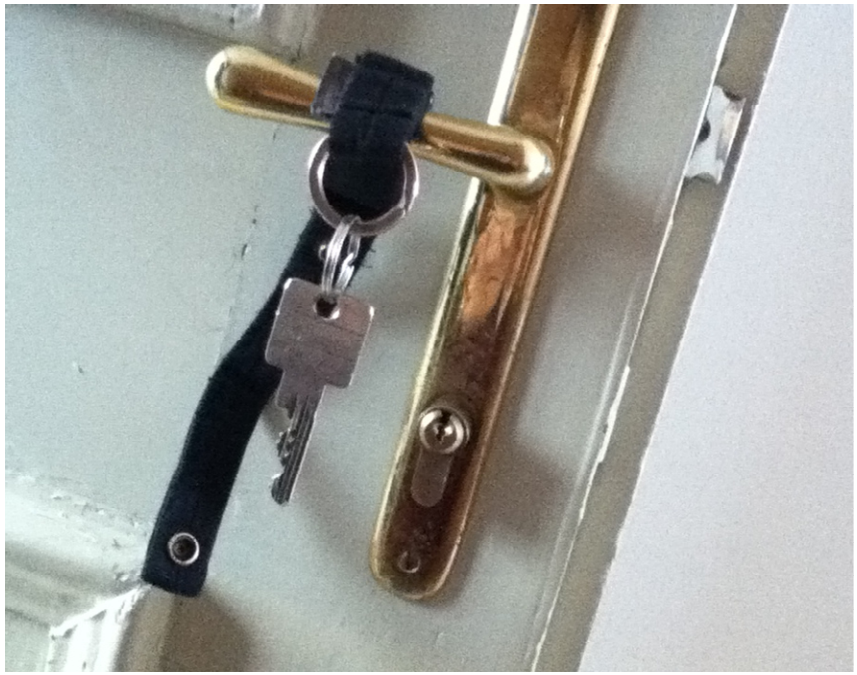
- Nutzt Einwegfunktion
  (Problem der Primfaktorenzerlegung)
- Öffentlicher Schlüssel → Verschlüsselung
- Privater Schlüssel → Entschlüsselung

RSA Kryptosystem: Anwendung

- Schlüsselaustausch
- z.B.:
  - Internet- und Telefoninfrastruktur
  - Übertragungsprotokolle
  - E-Mail Verschlüsselung
  - Kartenzahlung (Kreditkarten, …)

RSA-Angriffe

N=364615485029501136970713101143871109540
079913994317049087258562868354903436255 2
065955809589514611470241298944167703929333
752888490885711614193520646632973108751496
411205454301933653621610762952359760633 0
154669196064144182472739556974502462402 43
890311584572563094642894376854071409826 4
727068026730424033578827886916761701429 2
6495057389918617 7



BYLIC DSCP GFPC YSDKCPIQYKOCGR!