Weniger Klartext reden!

Dipl.-Math. Bastian Rieck

Arbeitsgruppe Computergraphik und Visualisierung
Interdisziplinäres Zentrum für Wissenschaftliches Rechnen

2. September 2013

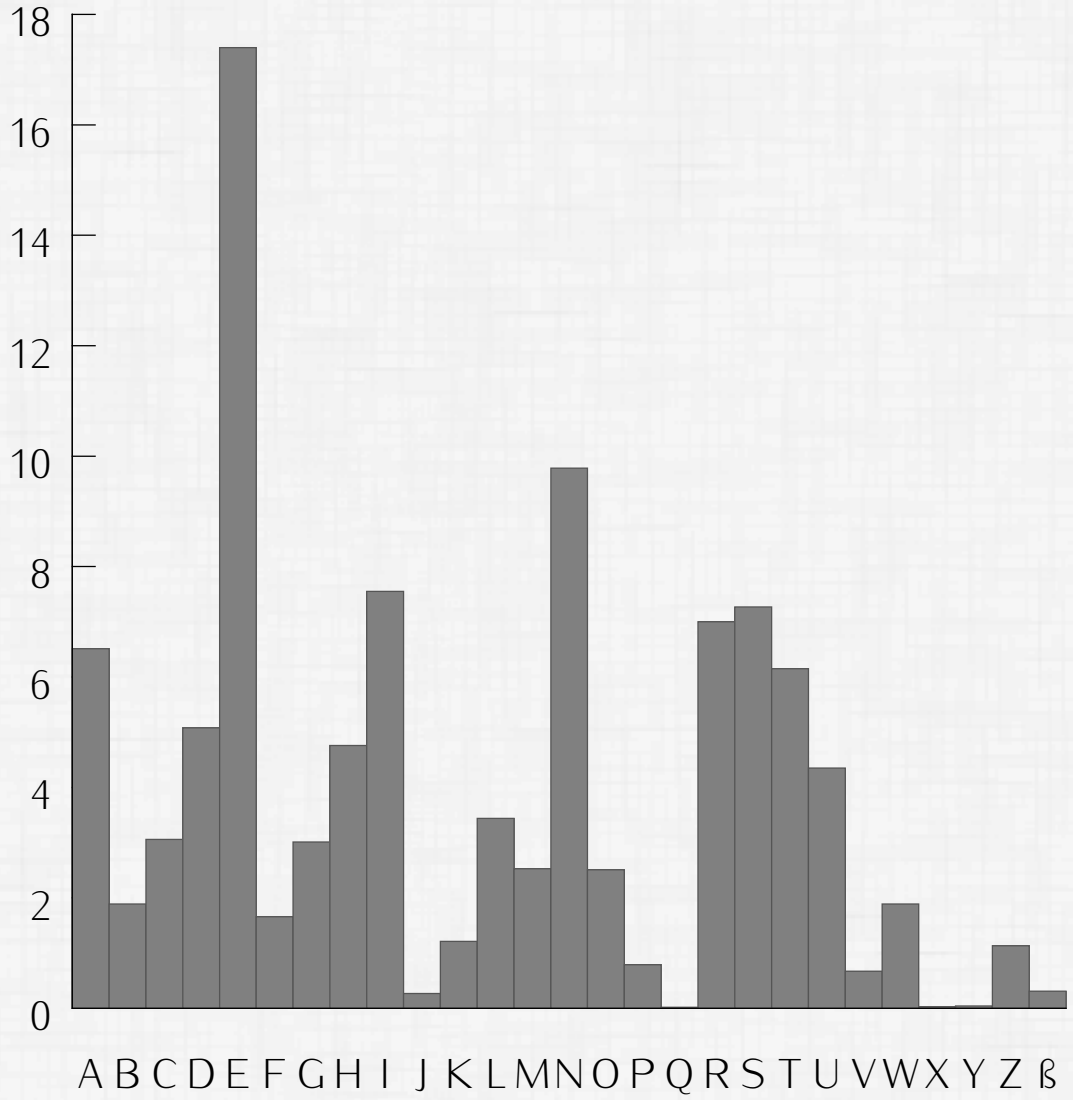
Kryptographie

1. kryptós (verborgen, geheim)
2. gráphein (schreiben)

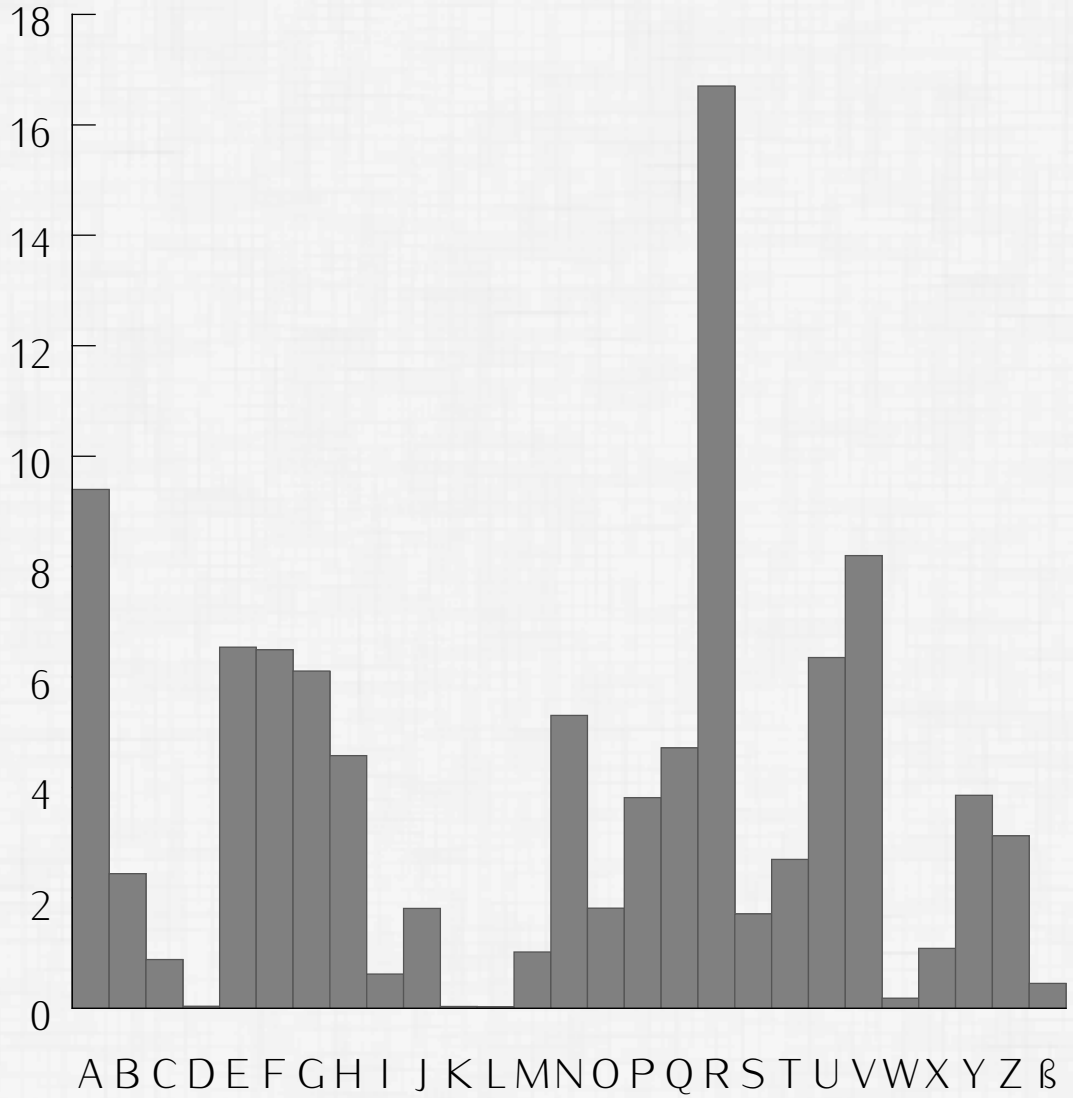
. . . wenn etwas Geheimes zu überbringen war, schrieb er in Zeichen, das heißt, er ordnete die Buchstaben so, dass kein Wort gelesen werden konnte: Um diese zu lesen, tauscht man den vierten Buchstaben, also D, für A aus und ebenso mit den restlichen.

Quelle: Sueton, De Vita Caesarum: Divus Julius LVI

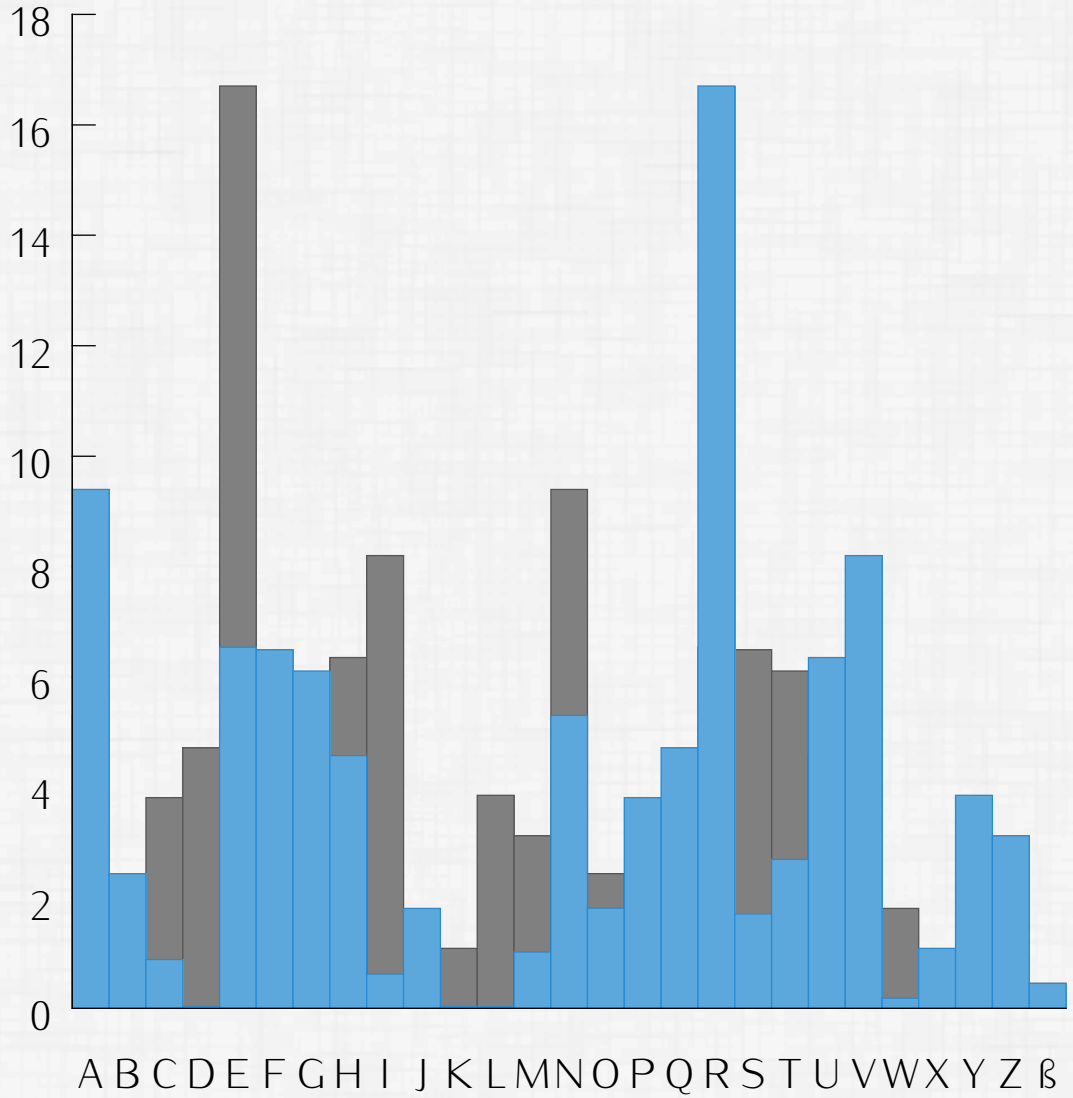
Ist das sicher?



Häufigkeiten deutscher Buchstaben



Häufigkeiten in einer verschlüsselten Fassung von “Faust”



Vergleich beider Häufigkeitstabellen

$$E = R$$

Quelle: memebase.com

Können wir es wenigstens schön beschreiben?

Exkurs: Modulo-Rechnung

Die Modulo-Operation, kurz **mod**, beschreibt den *Rest* bei ganzzahliger Division.

- $14 \bmod 12 = 2$
- $16 \bmod 12 = 4$
- $21 \bmod 12 = 9$

Quelle: flickr.com, Benutzer "GirlInLimbo"

Mathematische Beschreibung der Caesar-Chiffre

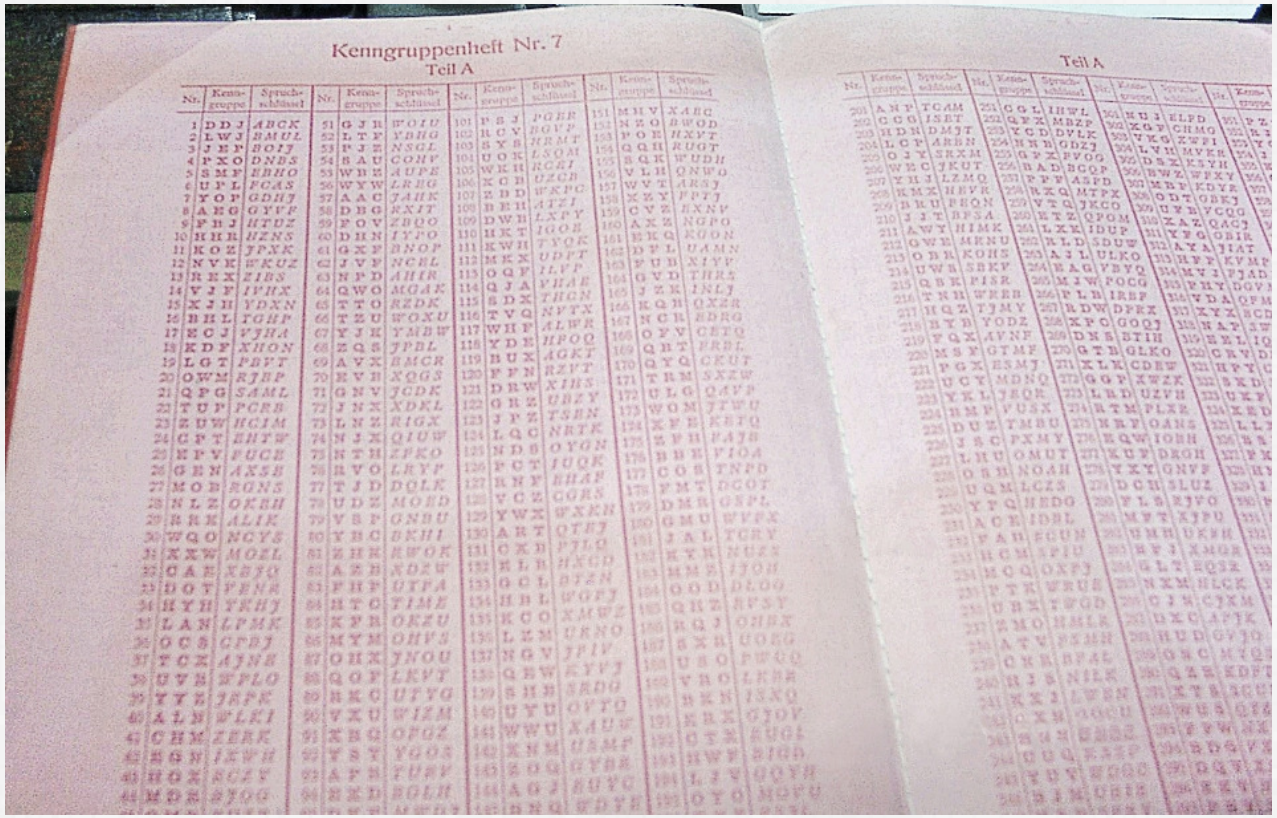
Sei k der Schlüssel, d.h. die Anzahl der Stellen, um die verschoben wird. Wir setzen $A = 0$, $B = 1$, …, $Z = 25$.

$$E_k(x) = (x + k) \bmod 26$$
$$D_k(x) = (x - k) \bmod 26$$

Einige Maschinen

Quelle: Wikimedia Commons

Problem: Die Schlüsselverteilung!



- Zu wenige Möglichkeiten zur Verschlüsselung
- Verfahren sind *symmetrisch*

Quelle: Wikimedia Commons

“Der Feind kennt das System”

Quelle: Claude Shannon

Ron Rivest

Adi Shamir

Leonard Adleman

RSA®

Quelle: Wikimedia Commons, privat

Exkurs: Primzahlen

Eine Primzahl ist eine natürliche Zahl größer 1, die nur durch sich selbst und 1 teilbar ist.

Exkurs: Primzahlen

Eine Primzahl ist eine natürliche Zahl größer 1, die nur durch sich selbst und 1 teilbar ist.

Beispiele: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853 . . .

Exkurs: Primzahlen

Eine Primzahl ist eine natürliche Zahl größer 1, die nur durch sich selbst und 1 teilbar ist.

Beispiele: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853 . . .

Jede natürliche Zahl lässt sich als (im Wesentlichen eindeutiges) Produkt von Primzahlen darstellen.

Die Grundlage von RSA

Die Grundlage von RSA

Diese Richtung ist einfach:

$$2161 \cdot 2179 = 4708819$$
$$7883 \cdot 9199 = 72515717$$
$$48673 \cdot 26711 = 1300104503$$

Die Grundlage von RSA

Diese Richtung ist einfach:

$$2161 \cdot 2179 = 4708819$$
$$7883 \cdot 9199 = 72515717$$
$$48673 \cdot 26711 = 1300104503$$

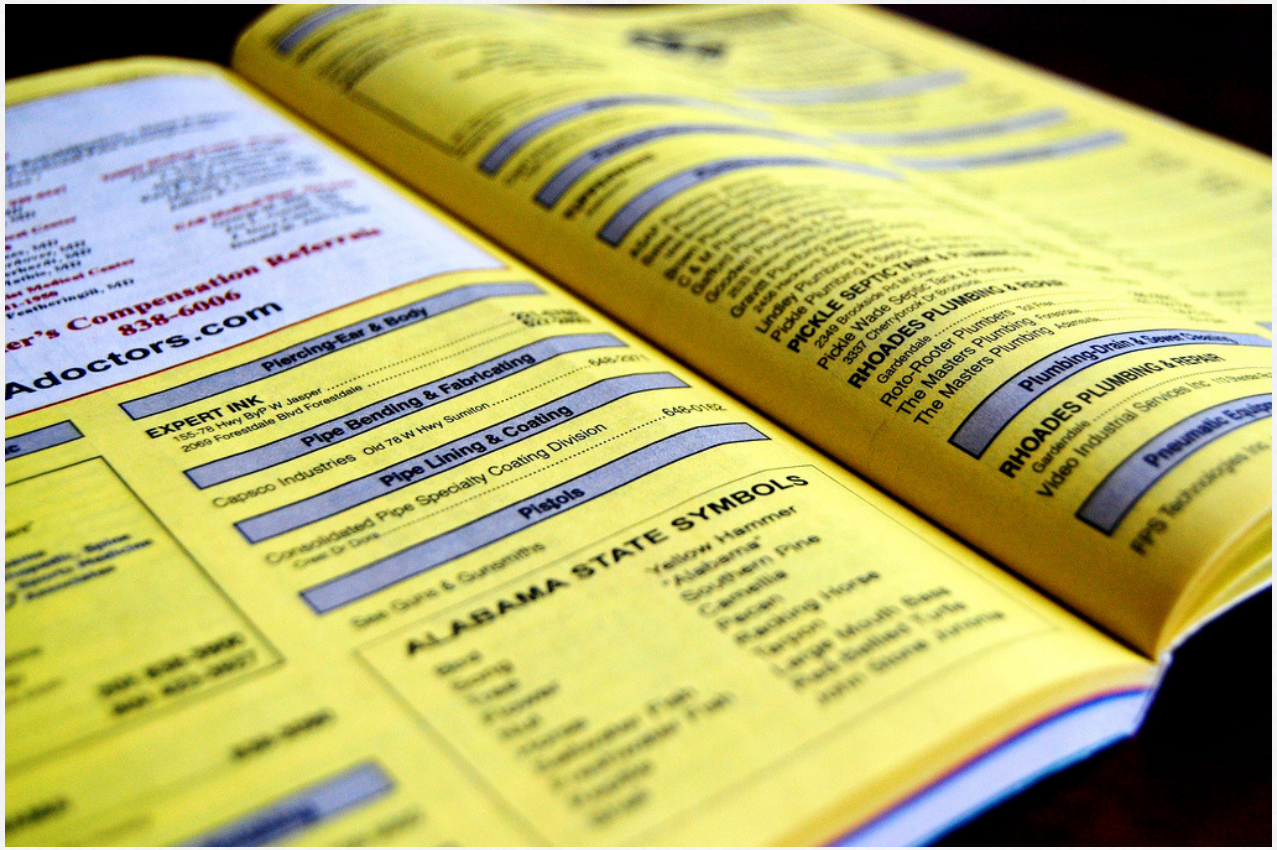
Diese Richtung nicht so sehr:

$$50621 = 223 \cdot 227$$
$$11840417 = 3433 \cdot 3449$$
$$2985959 = 1723 \cdot 1733$$

Multiplikation ist leichter als Faktorisierung

Mathematisch formuliert

Die Multiplikation von zwei Primzahlen p und q ist eine *Einwegfunktion*: Den Funktionswert zu berechnen ist einfach (Multiplikation), aber die zu einem Funktionswert gehörenden Primzahlen zu finden, ist schwer (Faktorisierung).



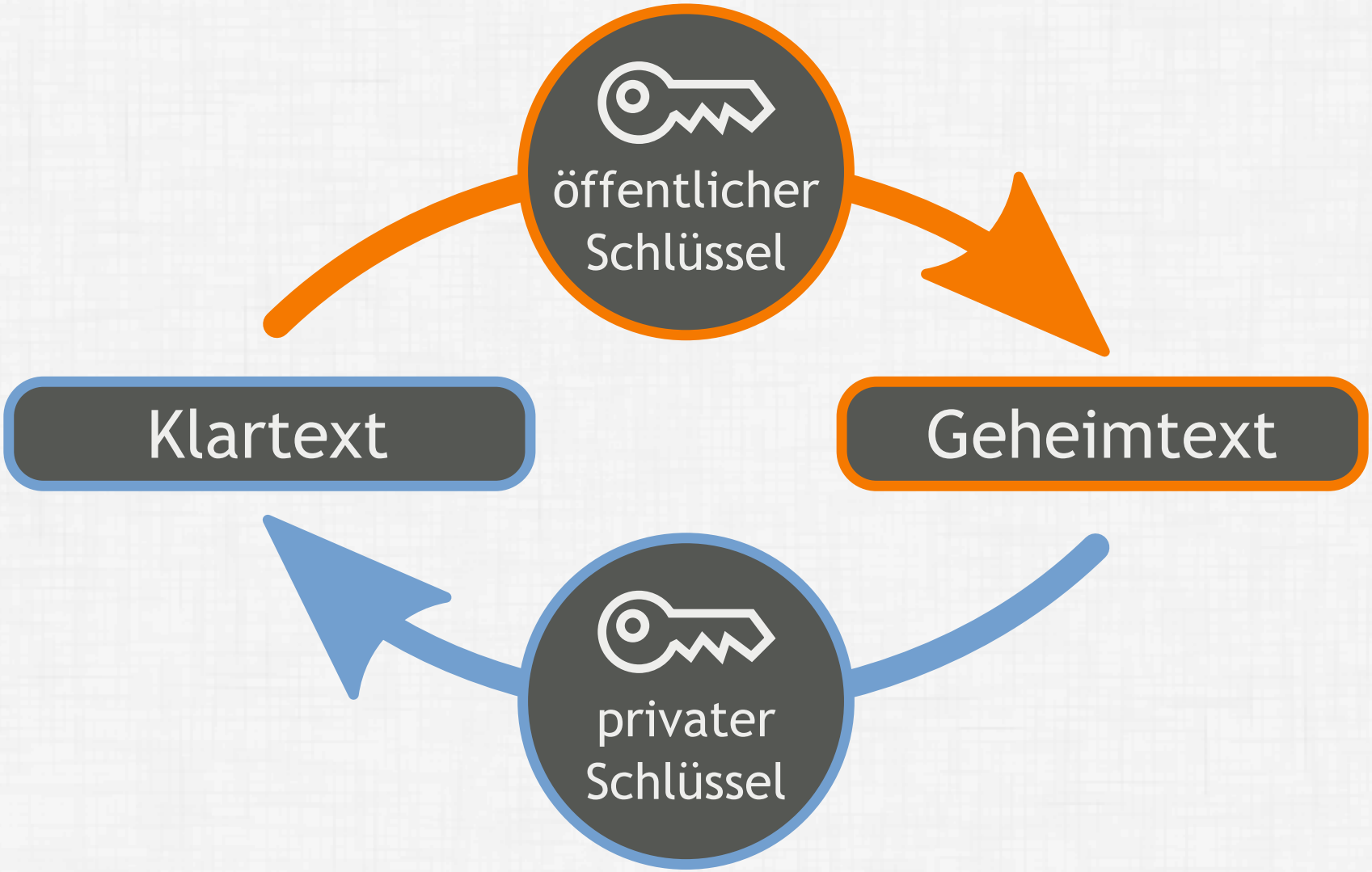
Auch eine Art Einwegfunktion

Quelle: flickr.com, Benutzer "Jamiesrabbits"

RSA

- Öffentlicher Schlüssel (an alle verteilen)
- Privater Schlüssel (geheim halten)
- Nachrichten werden mit dem öffentlichen Schlüssel *verschlüsselt* und mit dem privaten Schlüssel *entschlüsselt*.

Quelle: flickr.com, Benutzer "robinejay"



Quelle: Wikipedia, Benutzer “Bananenfalter”

Algorithmus: Schlüsselerzeugung

- Wähle zwei unterschiedliche Primzahlen p und q

Algorithmus: Schlüsselerzeugung

- Wähle zwei unterschiedliche Primzahlen p und q
- Berechne $n = p \cdot q$ und $\phi = (p - 1) \cdot (q - 1)$

Algorithmus: Schlüsselerzeugung

- Wähle zwei unterschiedliche Primzahlen p und q
- Berechne $n = p \cdot q$ und $\phi = (p - 1) \cdot (q - 1)$
- Wähle $1 < e < \phi$ teilerfremd zu ϕ

Algorithmus: Schlüsselerzeugung

- Wähle zwei unterschiedliche Primzahlen p und q
- Berechne $n = p \cdot q$ und $\phi = (p - 1) \cdot (q - 1)$
- Wähle $1 < e < \phi$ teilerfremd zu ϕ
- Wähle d, sodass $ed \bmod \phi = 1$ (das geht nur, wenn e teilerfremd zu ϕ)

Algorithmus: Schlüsselerzeugung

- Wähle zwei unterschiedliche Primzahlen p und q
- Berechne $n = p \cdot q$ und $\phi = (p - 1) \cdot (q - 1)$
- Wähle $1 < e < \phi$ teilerfremd zu ϕ
- Wähle d, sodass $ed \bmod \phi = 1$ (das geht nur, wenn e teilerfremd zu ϕ)
- (e, n) ist dann der öffentliche Schlüssel

Algorithmus: Schlüsselerzeugung

- Wähle zwei unterschiedliche Primzahlen p und q
- Berechne $n = p \cdot q$ und $\phi = (p - 1) \cdot (q - 1)$
- Wähle $1 < e < \phi$ teilerfremd zu ϕ
- Wähle d, sodass $ed \bmod \phi = 1$ (das geht nur, wenn e teilerfremd zu ϕ)
- (e, n) ist dann der öffentliche Schlüssel
- (d, n) ist dann der private Schlüssel

Algorithmus: Schlüsselerzeugung

- Wähle zwei unterschiedliche Primzahlen p und q
- Berechne $n = p \cdot q$ und $\phi = (p - 1) \cdot (q - 1)$
- Wähle $1 < e < \phi$ teilerfremd zu ϕ
- Wähle d, sodass $ed \bmod \phi = 1$ (das geht nur, wenn e teilerfremd zu ϕ)
- (e, n) ist dann der öffentliche Schlüssel
- (d, n) ist dann der private Schlüssel
- Länge von n ist typischerweise ≈ 300 Dezimalstellen

Algorithmus: Verschlüsselung

Sei $0 \leq m < n$ die zu verschlüsselnde Nachricht. m muss teilerfremd zu n sein. Berechne dann:

$$c = m^e \bmod n$$

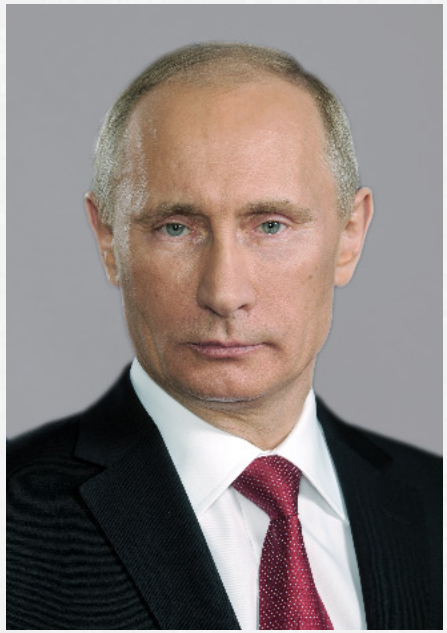
Algorithmus: Entschlüsselung

Sei c die empfangene Nachricht. Berechne dann:

$$c^d \bmod n = m$$

Angela

Barack



Wladimir

Quelle: Offizielle Porträts

Beispiel

Barack erzeugt seine Schlüssel

- Er wählt $p = 7$, $q = 11$

Beispiel

Barack erzeugt seine Schlüssel

- Er wählt $p = 7$, $q = 11$
- Barack berechnet $n = p \cdot q = 77$

Beispiel

Barack erzeugt seine Schlüssel

- Er wählt $p = 7$, $q = 11$
- Barack berechnet $n = p \cdot q = 77$
- Und $\phi = 6 \cdot 10 = 60$

Beispiel

Barack erzeugt seine Schlüssel

- Er wählt $p = 7$, $q = 11$
- Barack berechnet $n = p \cdot q = 77$
- Und $\phi = 6 \cdot 10 = 60$
- Er wählt $e = 23$

Beispiel

Barack erzeugt seine Schlüssel

- Er wählt $p = 7$, $q = 11$
- Barack berechnet $n = p \cdot q = 77$
- Und $\phi = 6 \cdot 10 = 60$
- Er wählt $e = 23$
- Und findet $d = 47$

Beispiel

Barack erzeugt seine Schlüssel

- Er wählt $p = 7$, $q = 11$
- Barack berechnet $n = p \cdot q = 77$
- Und $\phi = 6 \cdot 10 = 60$
- Er wählt $e = 23$
- Und findet $d = 47$
- Er schickt $(23, 77)$ an Angela

Beispiel

Barack erzeugt seine Schlüssel

- Er wählt $p = 7$, $q = 11$
- Barack berechnet $n = p \cdot q = 77$
- Und $\phi = 6 \cdot 10 = 60$
- Er wählt $e = 23$
- Und findet $d = 47$
- Er schickt $(23, 77)$ an Angela
- Er schließt $(47, 77)$ in den Safe ein

Beispiel

Angela verschickt ihre Nachricht

- Angela will $m = 48$ (Anzahl Gäste für Putins Party) senden

Beispiel

Angela verschickt ihre Nachricht

- Angela will $m = 48$ (Anzahl Gäste für Putins Party) senden
- Baracks öffentlicher Schlüssel ist $(23, 77)$

Beispiel

Angela verschickt ihre Nachricht

- Angela will $m = 48$ (Anzahl Gäste für Putins Party) senden
- Baracks öffentlicher Schlüssel ist $(23, 77)$
- Sie berechnet $48^{23} \bmod 77 = 20$

Beispiel

Barack entschlüsselt Angelas Nachricht

- Barack empfängt $c = 20$

Beispiel

Barack entschlüsselt Angelas Nachricht

- Barack empfängt $c = 20$
- Sein privater Schlüssel ist $(47, 77)$

Beispiel

Barack entschlüsselt Angelas Nachricht

- Barack empfängt $c = 20$
- Sein privater Schlüssel ist $(47, 77)$
- Er berechnet $20^{47} \bmod 77 = 48$

Warum funktioniert das überhaupt?

Exkurs: Satz von Euler-Fermat

Für zwei Primzahlen p und q und jede natürliche Zahl m, die teilerfremd zu pq ist, gilt:

$$m^{(p-1)(q-1)} \bmod pq = 1$$

(Der Fundamentalsatz von RSA)

$$
\begin{aligned}
c^d \bmod n &= m^{ed} \bmod n \text{ (nach Definition von } c\text{)} \\
&= m^{1+k\phi} \bmod n \text{ (denn } ed \mod \phi = 1\text{)} \\
&= m^{1+k(p-1)(q-1)} \bmod n \text{ (nach Definition von } \phi\text{)} \\
&= m \cdot m^{k\cdot(p-1)(q-1)} \bmod n \text{ (ausmultipliziert)} \\
&= m \cdot m^{(p-1)(q-1)^k} \bmod n \text{ (Potenzierung geändert)} \\
&= m \text{ (nach Euler-Fermat)}
\end{aligned}
$$

Warum ist das sicher?

- Wladimir kennt (e, n)

Warum ist das sicher?

- Wladimir kennt (e, n)
- Er braucht aber d zur Entschlüsselung, damit er $c^d \bmod n = m$ berechnen kann!

Warum ist das sicher?

- Wladimir kennt (e, n)
- Er braucht aber d zur Entschlüsselung, damit er $c^d \bmod n = m$ berechnen kann!
- e und d stehen durch $ed \bmod \phi = 1$ in Verbindung

Warum ist das sicher?

- Wladimir kennt (e, n)
- Er braucht aber d zur Entschlüsselung, damit er $c^d \bmod n = m$ berechnen kann!
- e und d stehen durch $ed \bmod \phi = 1$ in Verbindung
- Wladimir braucht also $\phi = (p-1) \cdot (q-1)$

Warum ist das sicher?

- Wladimir kennt (e, n)
- Er braucht aber d zur Entschlüsselung, damit er $c^d \bmod n = m$ berechnen kann!
- e und d stehen durch $ed \bmod \phi = 1$ in Verbindung
- Wladimir braucht also $\phi = (p-1) \cdot (q-1)$
- Dazu braucht er aber p und q

Warum ist das sicher?

- Wladimir kennt (e, n)
- Er braucht aber d zur Entschlüsselung, damit er $c^d \bmod n = m$ berechnen kann!
- e und d stehen durch $ed \bmod \phi = 1$ in Verbindung
- Wladimir braucht also $\phi = (p-1) \cdot (q-1)$
- Dazu braucht er aber p und q
- Er muss also $n = p \cdot q$ faktorisieren!

Warum ist das sicher?

- Wladimir kennt (e, n)
- Er braucht aber d zur Entschlüsselung, damit er $c^d \bmod n = m$ berechnen kann!
- e und d stehen durch $ed \bmod \phi = 1$ in Verbindung
- Wladimir braucht also $\phi = (p-1) \cdot (q-1)$
- Dazu braucht er aber p und q
- Er muss also $n = p \cdot q$ faktorisieren!
- Für große Zahlen braucht das lange (länger als das Universum alt ist?)

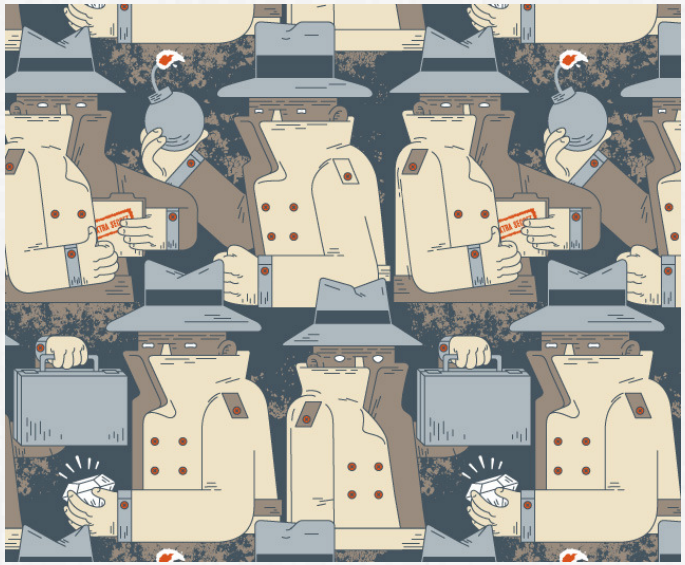
Warum ist das sicher?

- Wladimir kennt (e, n)
- Er braucht aber d zur Entschlüsselung, damit er $c^d \bmod n = m$ berechnen kann!
- e und d stehen durch $ed \bmod \phi = 1$ in Verbindung
- Wladimir braucht also $\phi = (p-1) \cdot (q-1)$
- Dazu braucht er aber p und q
- Er muss also $n = p \cdot q$ faktorisieren!
- Für große Zahlen braucht das lange (länger als das Universum alt ist?)
- Barack kann einfach zusätzliches Bit benutzen, was den Aufwand verdoppelt!

Wie geht es weiter?

Literatur:

- Simon Singh: *Codes – Die Kunst der Verschlüsselung*
- Bruce Schneier: *Angewandte Kryptographie*
- Neal Stephenson: *Cryptonomicon*



Software:

- *HTTPS Everywhere*
- *Off-the-record messaging*
- *The GNU Privacy Guard*
- *RedPhone*