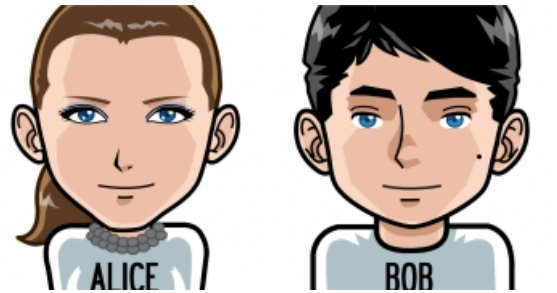
Angewandte Kryptographie

Mathematical Weaknesses of Cryptosystems

Inhalt

- Einleitung und Begriffsklärung
- Public Key Verfahren
- Angriffe
- Ciphers
- Kryptografische Funktionen
- Zufallszahlengenerierung

Dramatis Personae



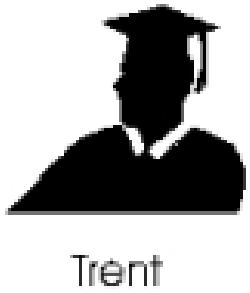
Wollen Nachrichten austauschen

http://wikis.zum.de/rmg/Benutzer:Deininger_Matthias/Facharbeit/Alice_Bob_und_Mallory

- Will die Nachrichten abhören
- Alle Kommunikation passiert Eve

http://www.powayusd.com/pusdtbes/cs/class7.htm

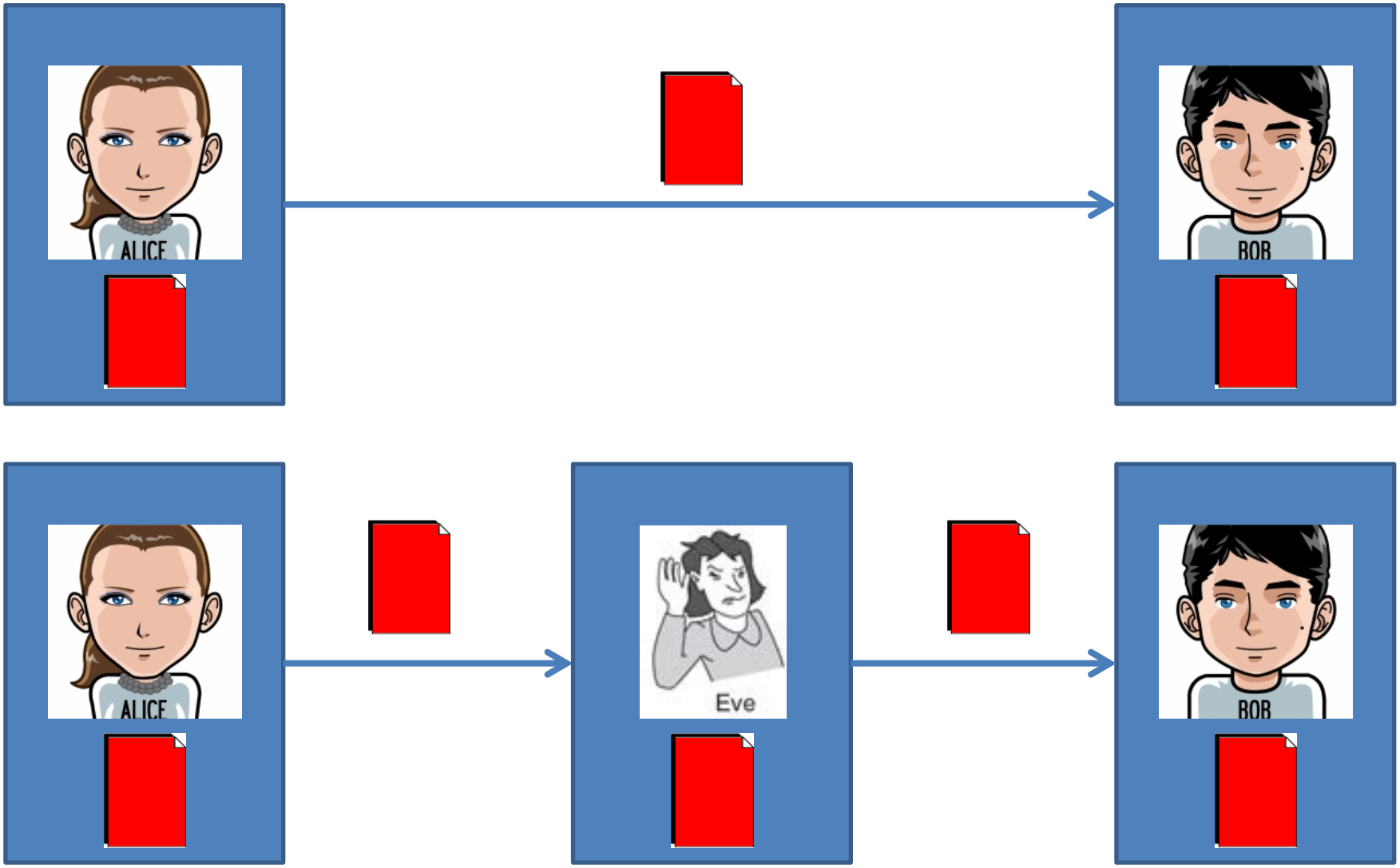
- Will die Nachrichten abhören
- Kann selbst Nachrichten senden oder manipulieren
- Alle Kommunikation passiert Mallory



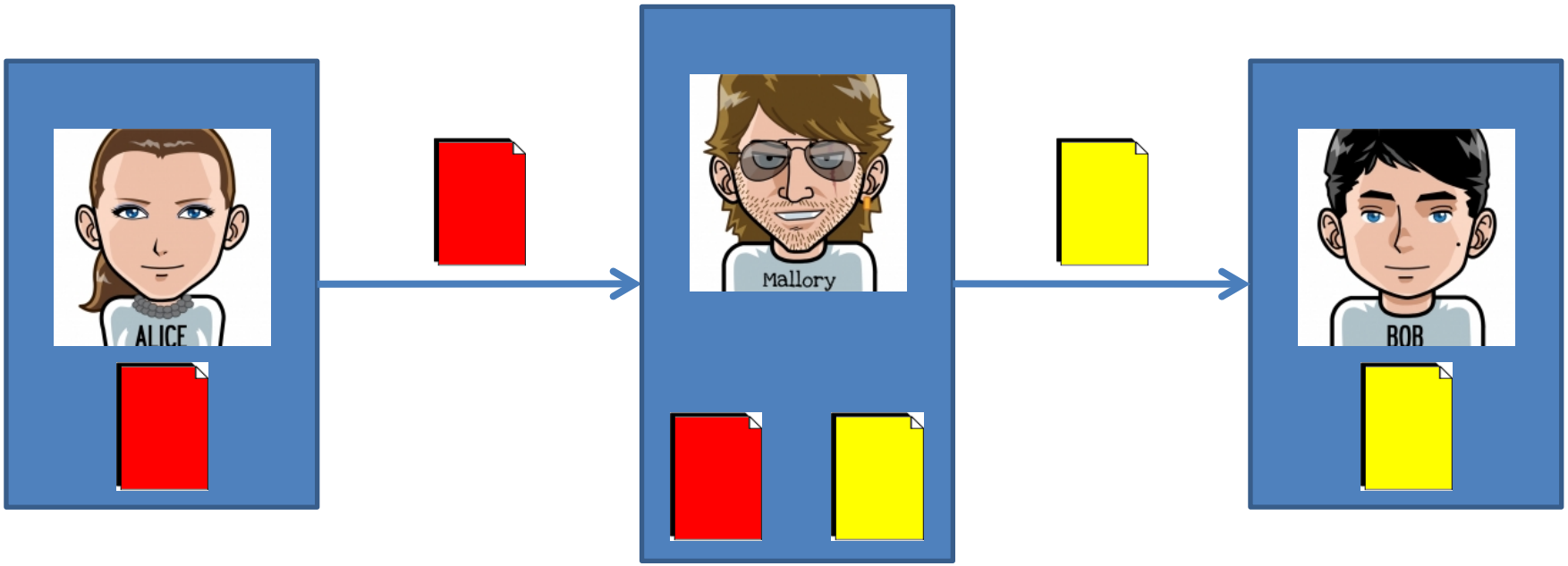
- Ist vertrauenswürdig
- alle vertrauen Trent

http://www.remote.org/frederik/projects/cash/cash-2.html

Kommunikation

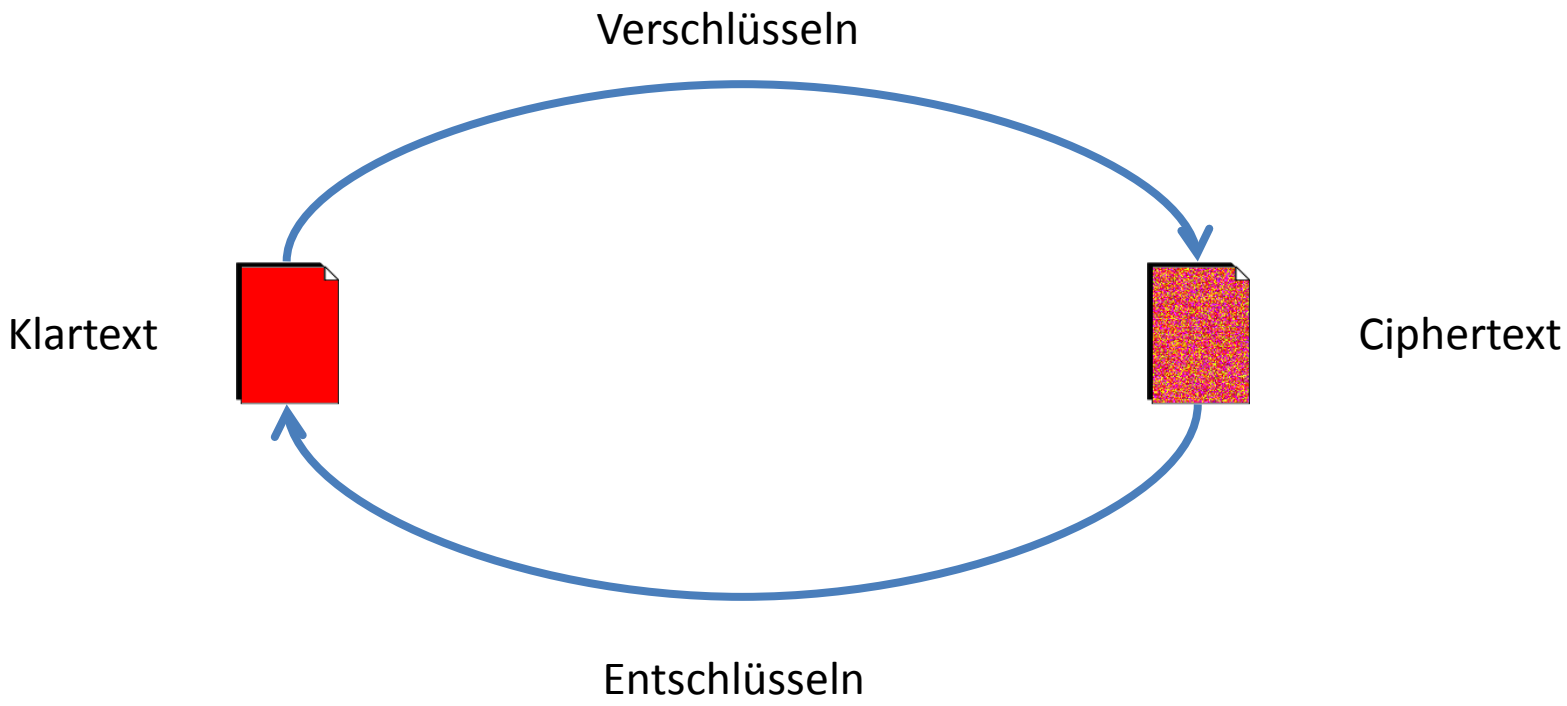


Kommunikation

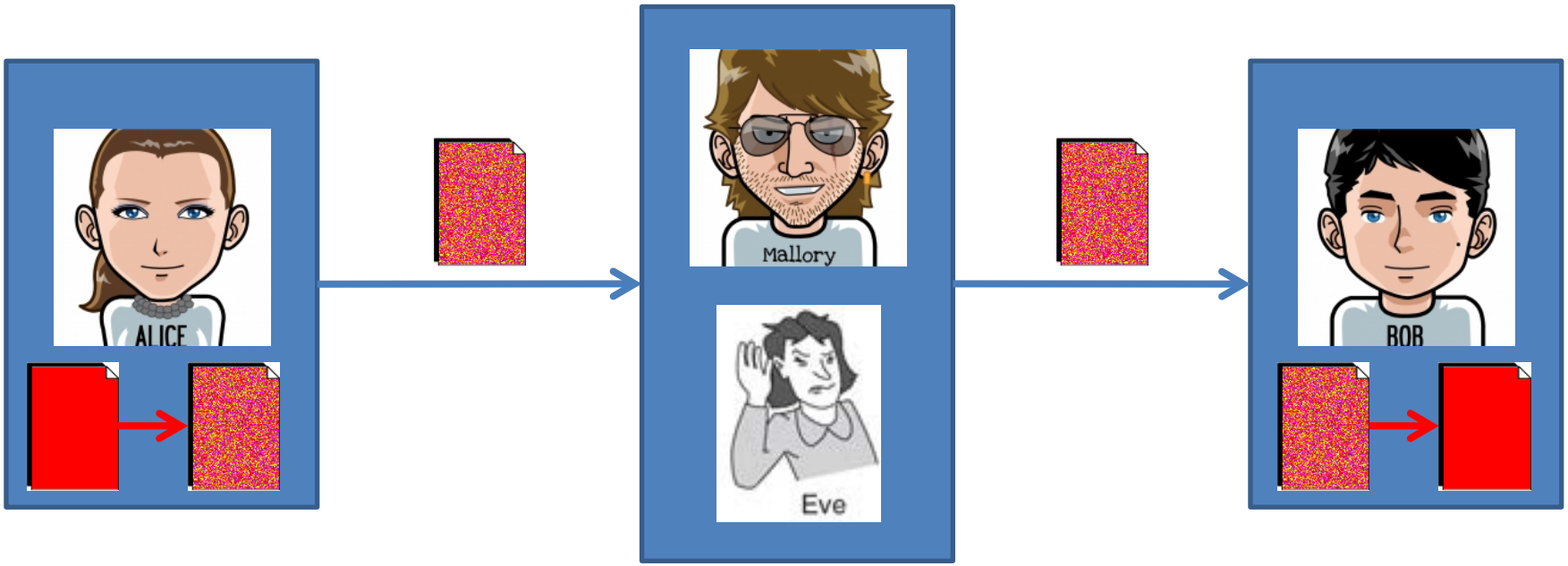


Grundbegriffe

Kryptografie
Kryptoanalyse
Kryptologie
Entziffern
Kryptosystem



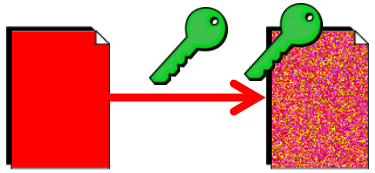
Kryptografie



Hier: Security through Obscurity

Schlüssel

Ein Schlüssel ist ein Parameter für ein Verschlüsselungsverfahren

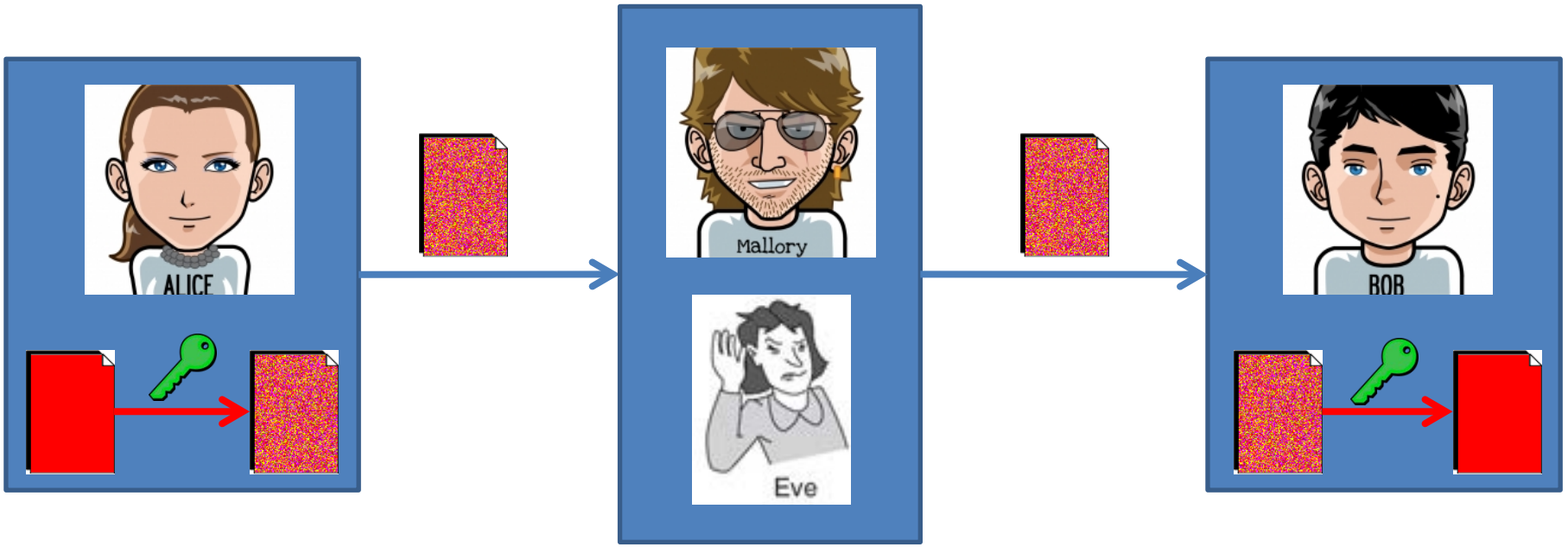


Kerkhoffs‘ Prinzip:

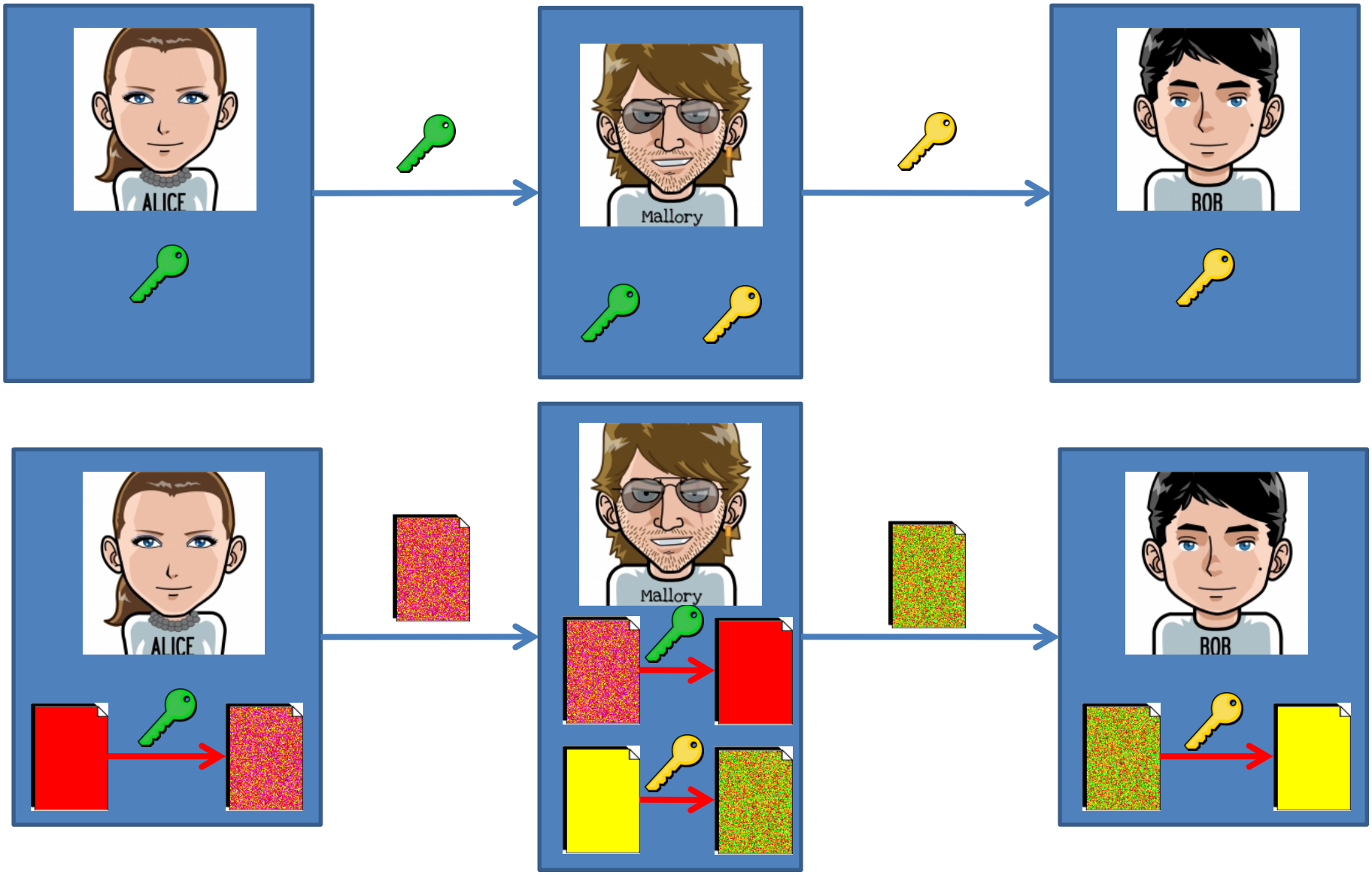
„Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus abhängen.
Die Sicherheit gründet sich nur auf die Geheimhaltung des Schlüssels.“

Auguste Kerckhoffs, 1883

Kryptografie mit Schlüssel



Schlüsselübertragung



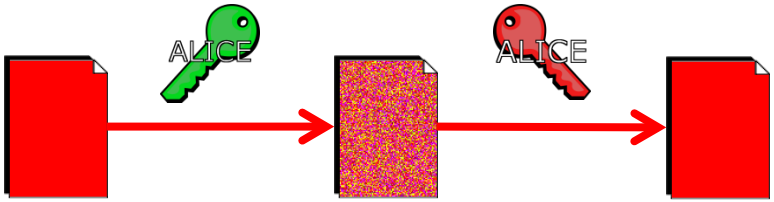
Asymmetrische Verschlüsselung/ Public-Key Verfahren

Privater Schlüssel (Private Key)

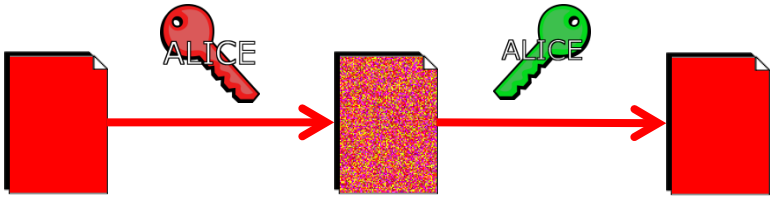
http://www.clker.com/clipart-neon-green-key.html

Öffentlicher Schlüssel (Public Key)

Immer möglich:

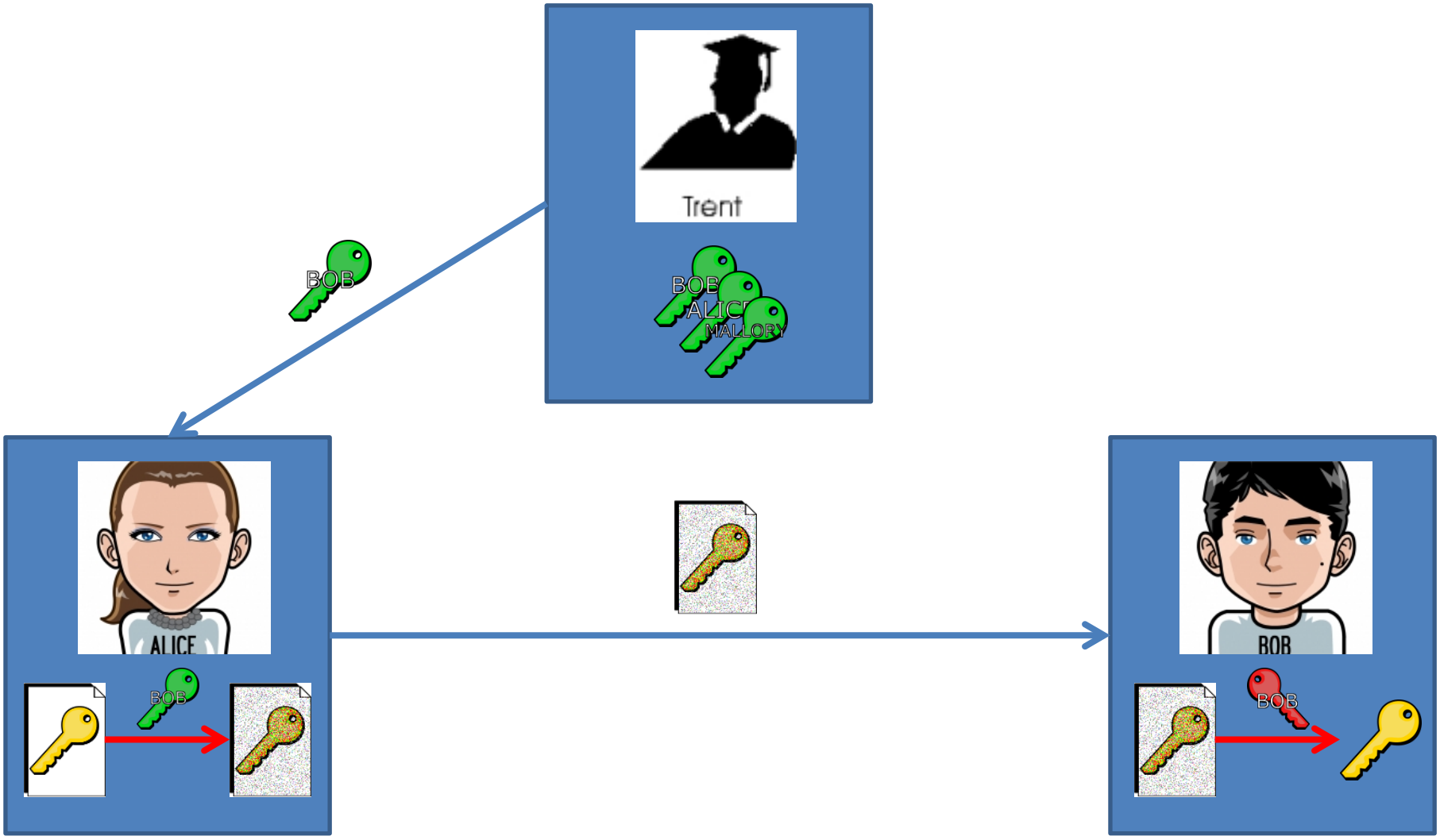


Manchmal möglich:

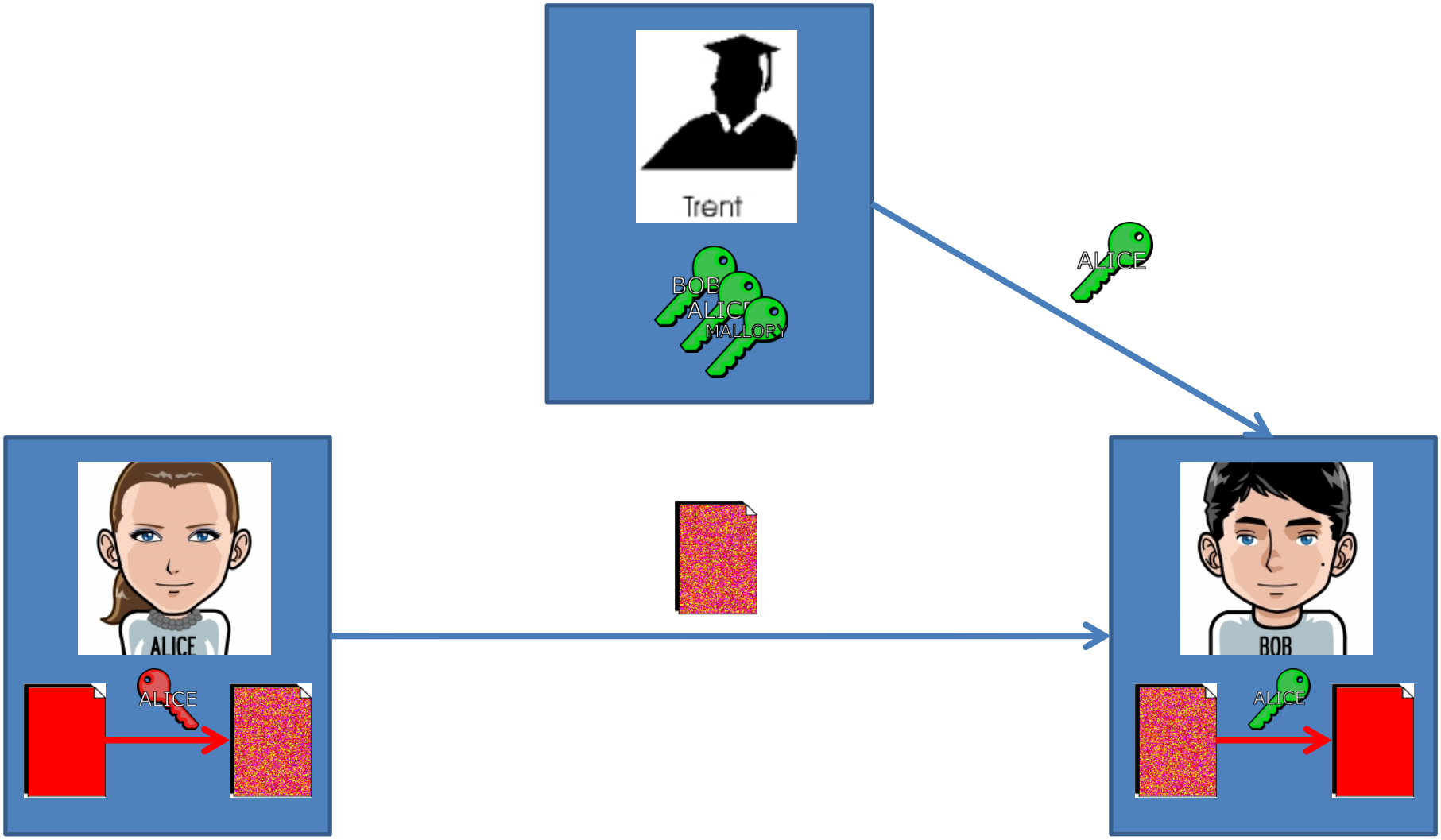


Aber: Public-Key Verfahren sind langsam

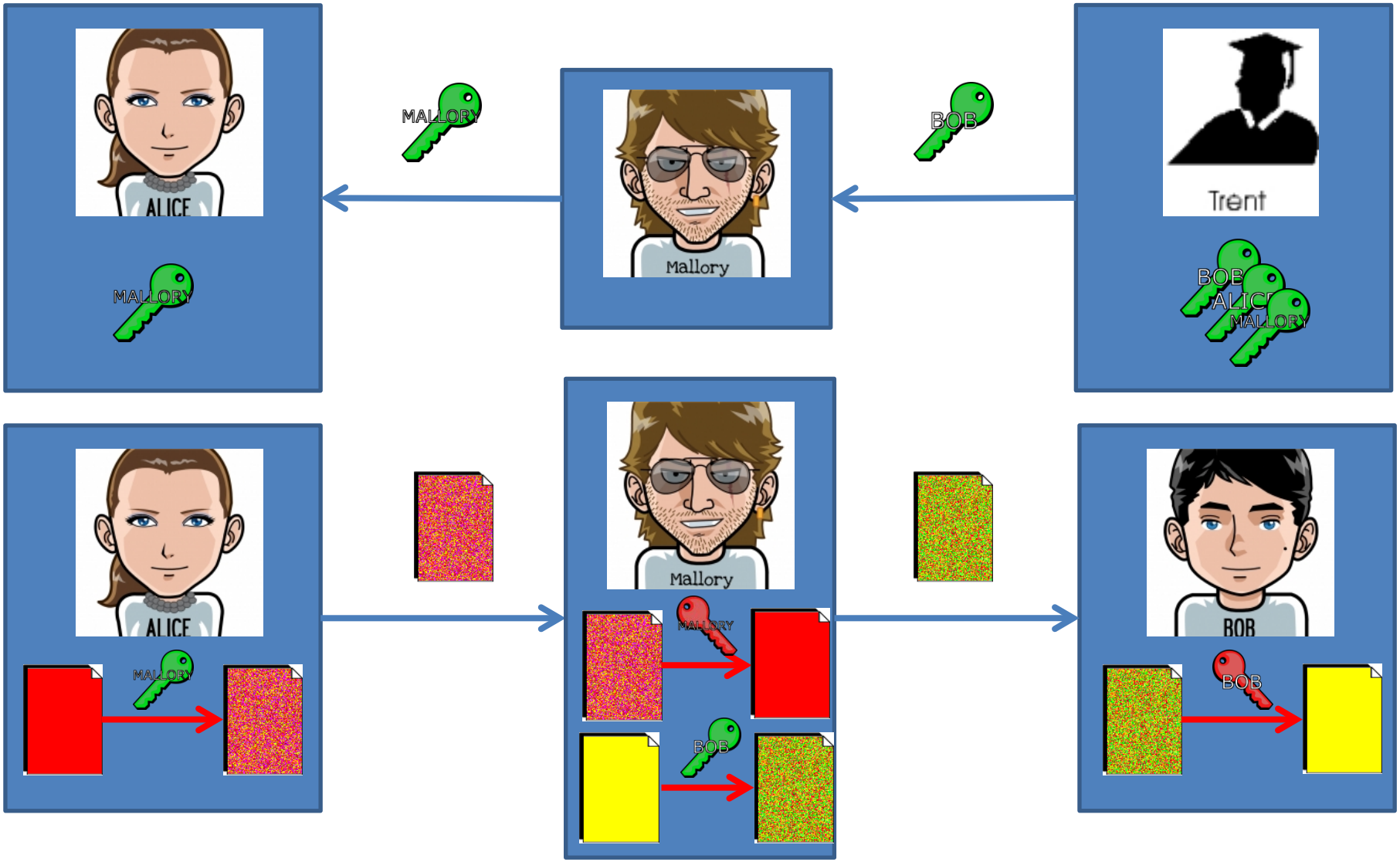
Schlüsselübertragung



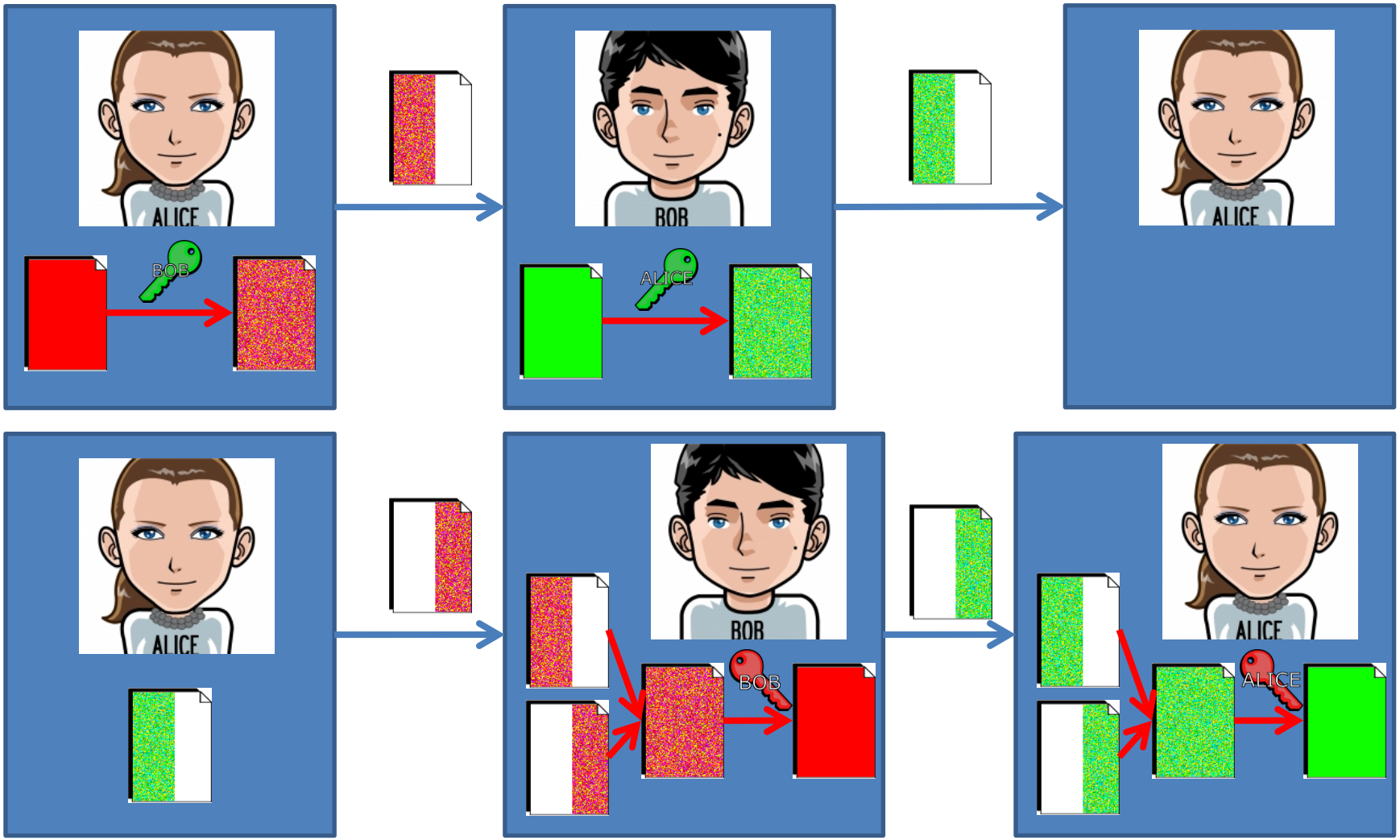
Digitale Signaturen



Man-in-the-Middle Angriff



Man-in-the-Middle Angriff: Lösung

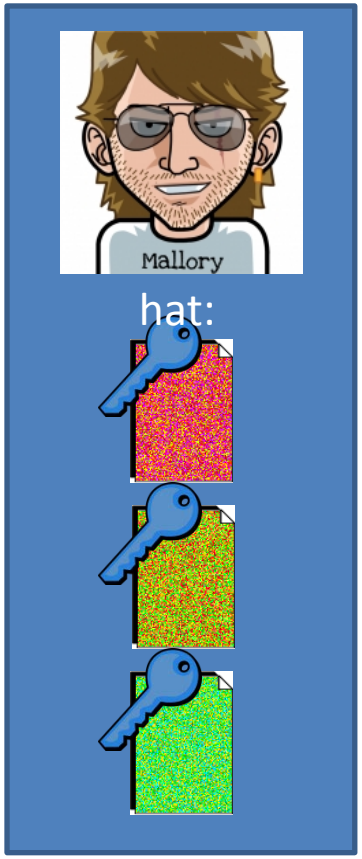


Angriffe

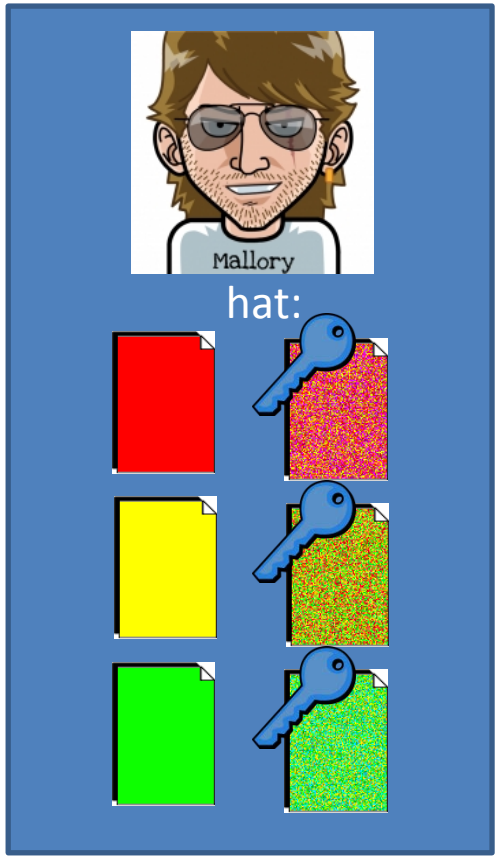
- Ciphertext only attack
- Known Plaintext attack
- Chosen plaintext Attack
- Adaptive Chosen Plaintext Attack
- Rubber-hose Cryptanalysis
- Social Engineering
- Häufigkeitsanalyse

Ciphertext only attack

- Schwächster Angriff
- Immer möglich

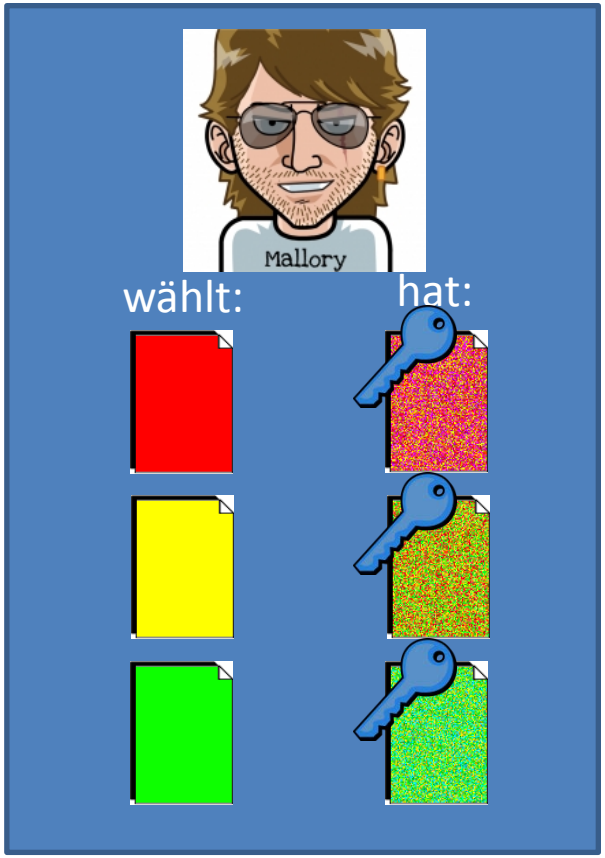


Known Plaintext attack



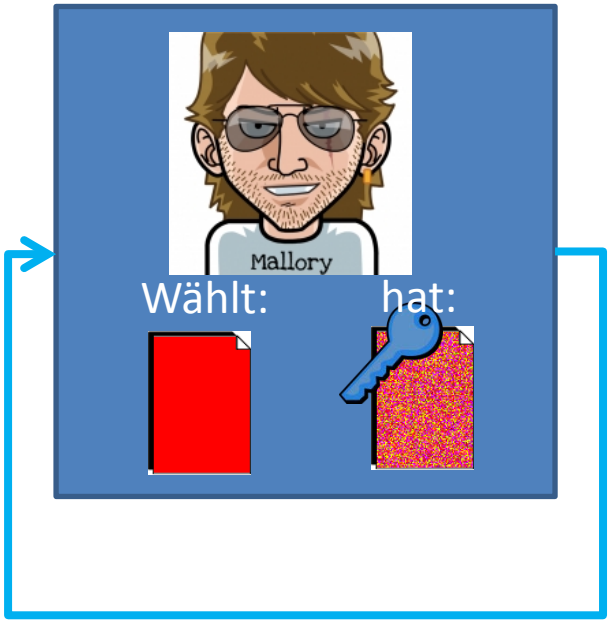
Chosen plaintext Attack

- Auch als Chosen Ciphertext möglich

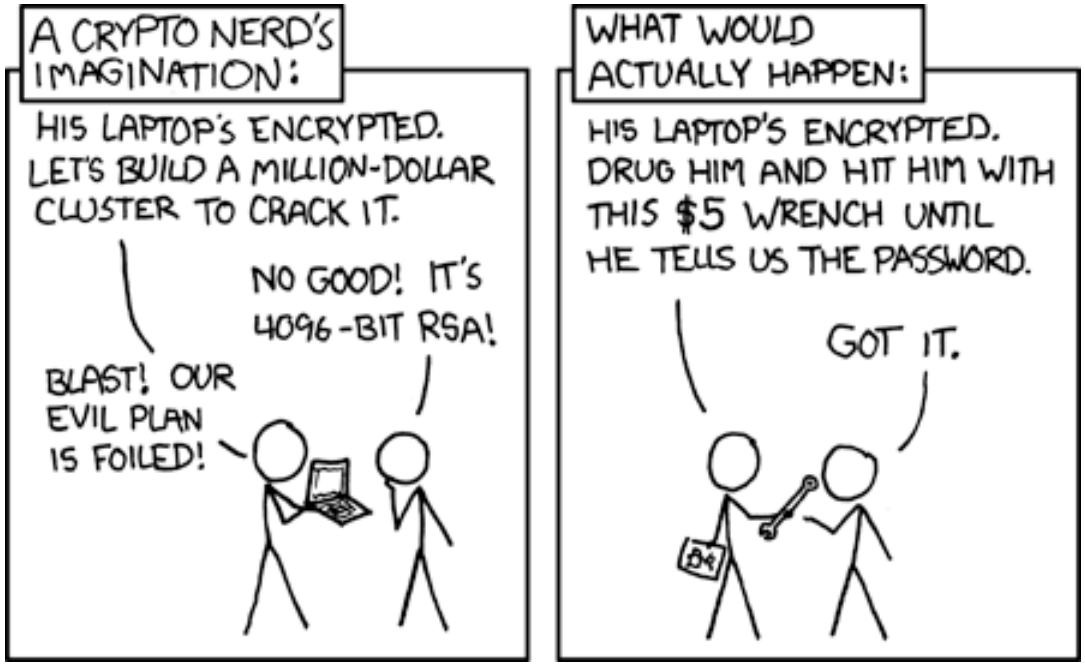


Adaptive Chosen plaintext Attack

- Bei Public-Key Verfahren immer möglich
- Auch als Adaptive Chosen Ciphertext möglich



Rubber-hose Cryptanalysis

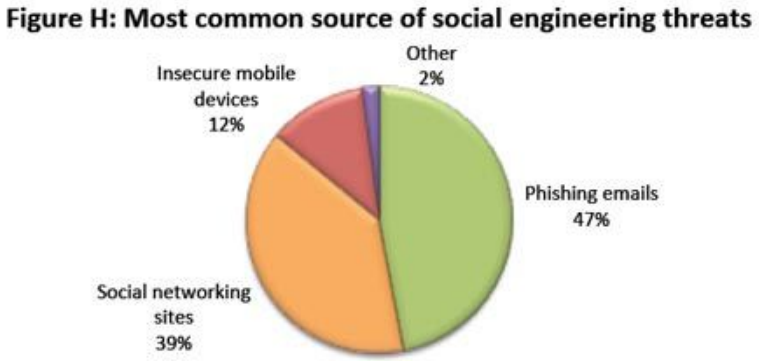


http://xkcd.com/538/

Actual actual reality: nobody cares about his secrets. (Also, I would be hard-pressed to find that wrench for $5.)

Social Engineering

Zielgenau zugeschnittene Angriffe nehmen zu. Zwei von drei deutschen Unternehmen wurden schon Opfer. Das hat Sicherheitsanbieter Check Point ermittelt.



http://www.cio.de/bild-zoom/2290486/1/689758/EL_13173081403541045799881/

http://magazine.thehackernews.com/images/Social-Engineering.JPG

Facebook Social Engineering Attack Strikes NATO

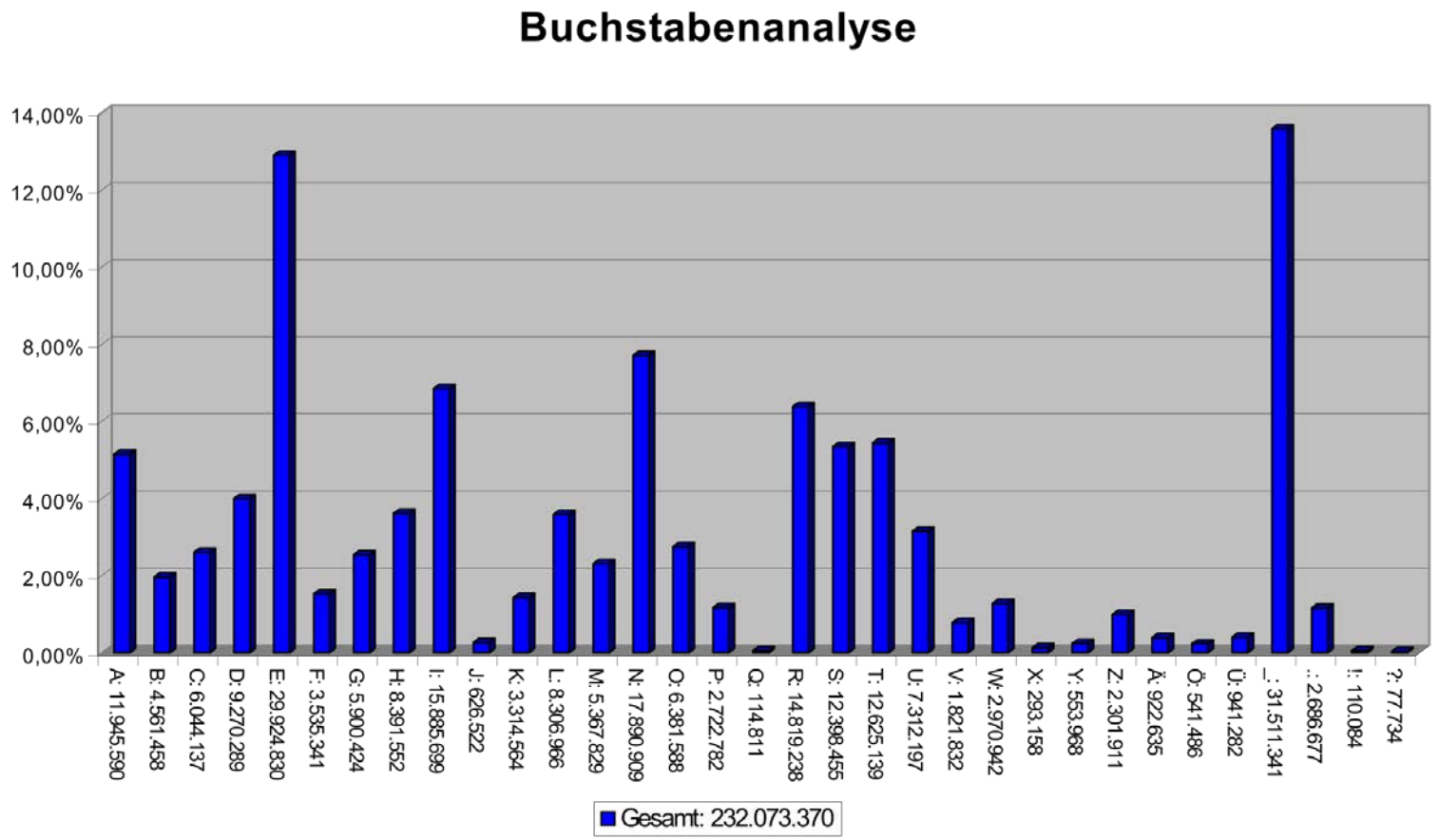
Top military commander in NATO targeted by attackers wielding fake Facebook pages. Some security watchers ask if Chinese culprits were involved.

By Mathew J. Schwartz InformationWeek
March 12, 2012 12:20 PM

The top military commander in NATO has been targeted by attackers wielding fake Facebook pages.

Attackers have been creating Facebook pages under the name of Admiral James Stavridis, NATO's Supreme Allied Commander Europe (SACEUR), in an attempt to lure his colleagues, friends, and family into connecting with the account and divulging private information, reported *The Observer* newspaper in Britain on Sunday.

Häufigkeitsanalyse

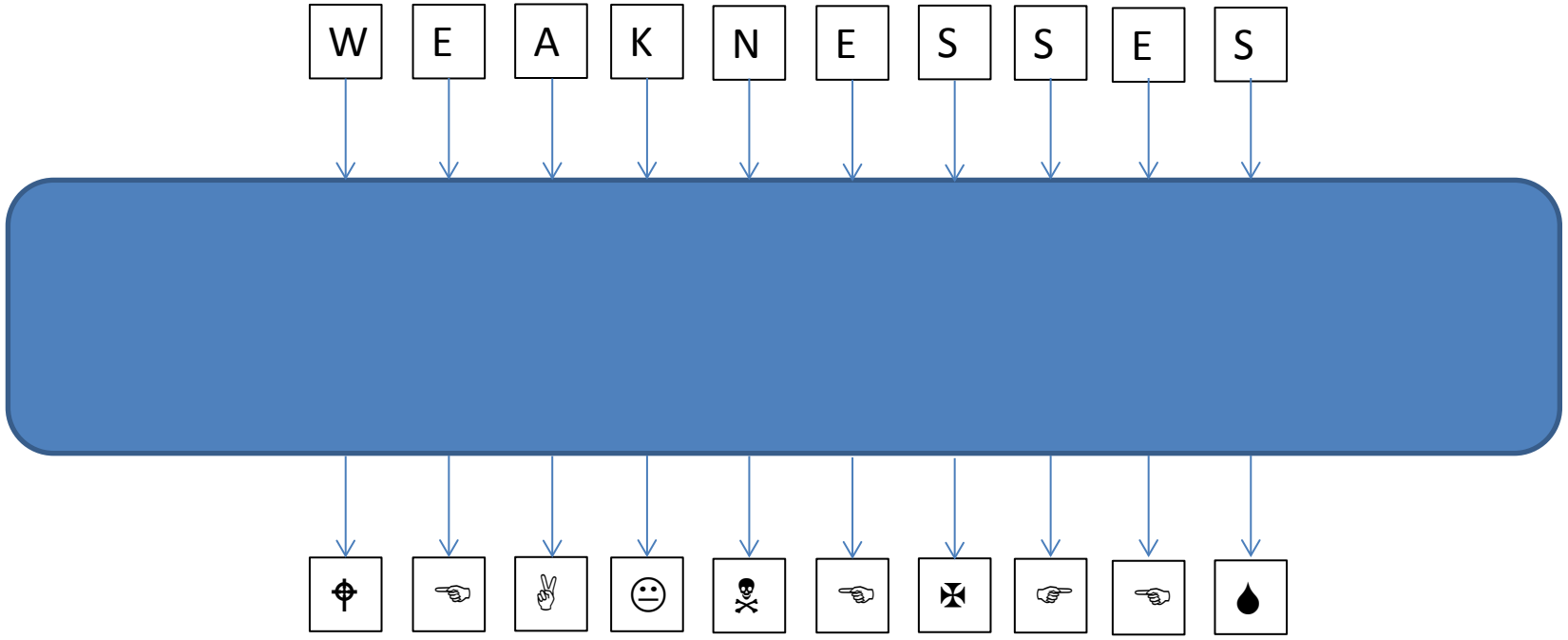


http://commons.wikimedia.org/wiki/File:Alphabet_haufigkeit.svg

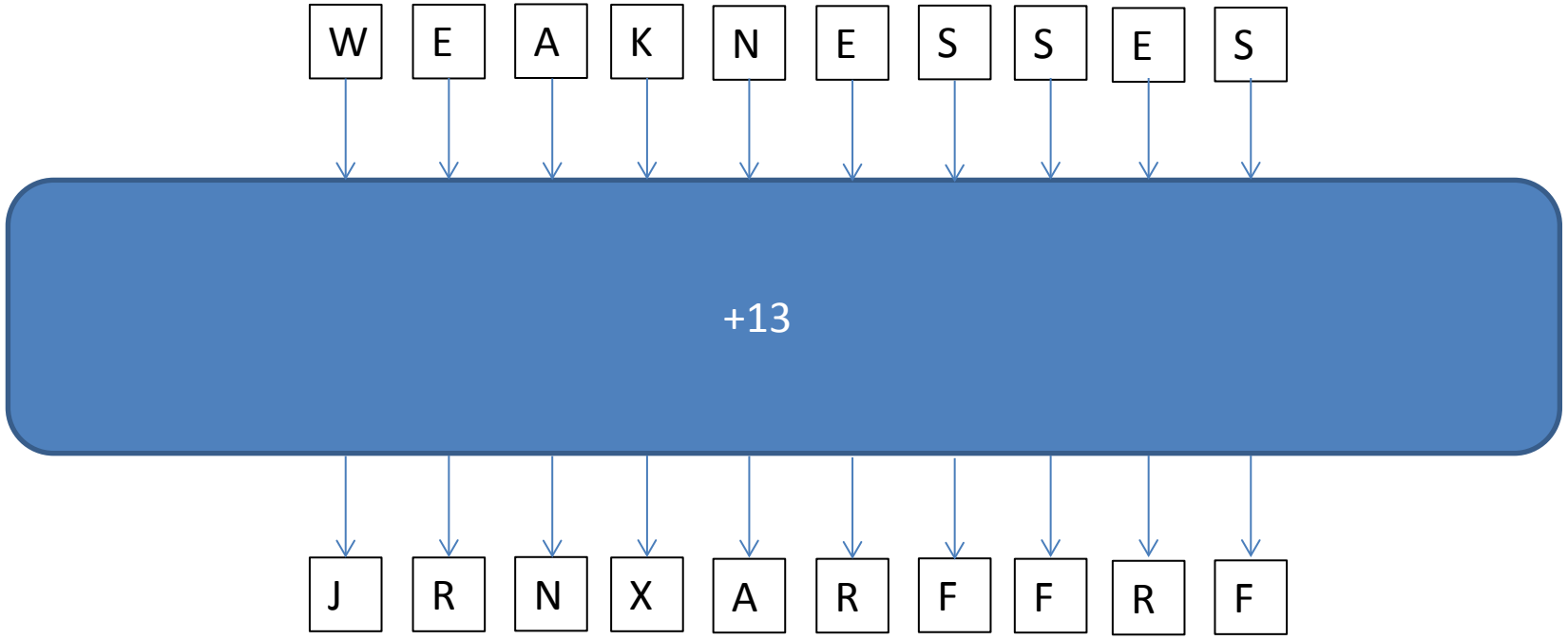
Ciphers

- Substitution Ciphers
- Transposition Ciphers
- Block Ciphers

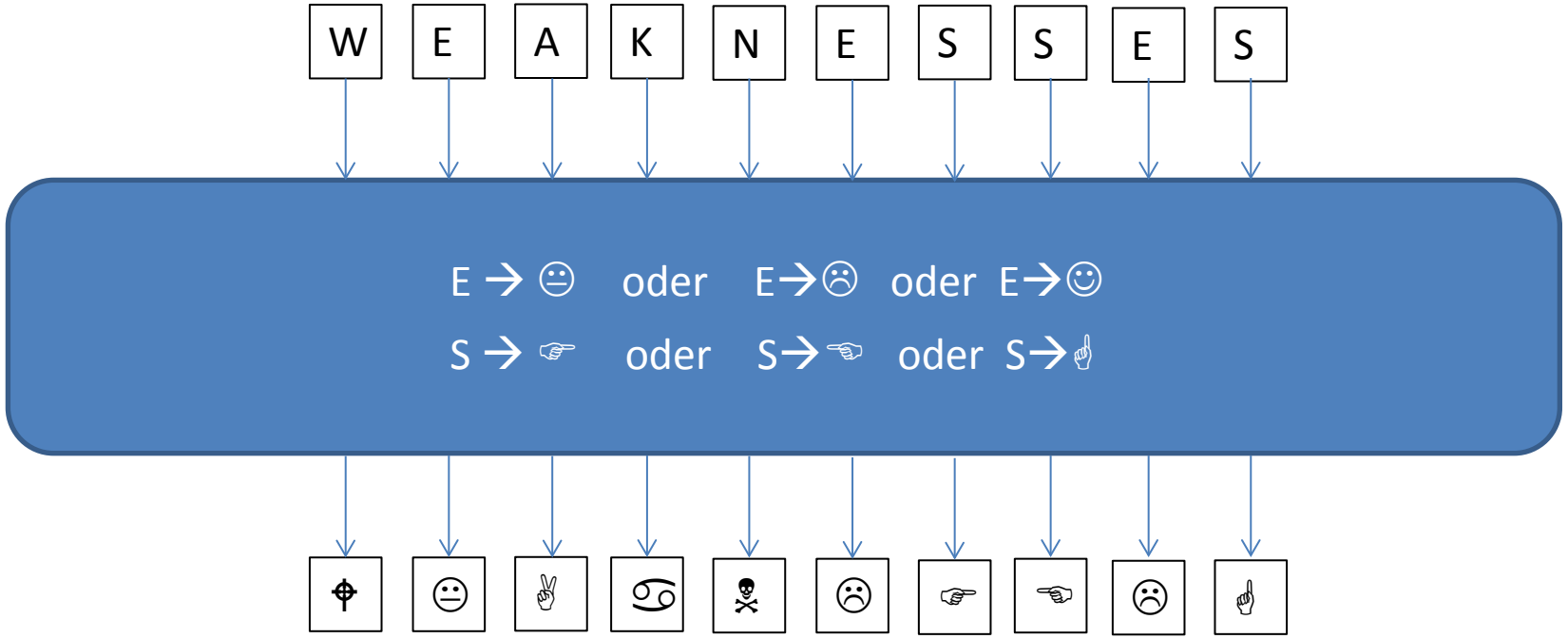
Substitution Ciphers



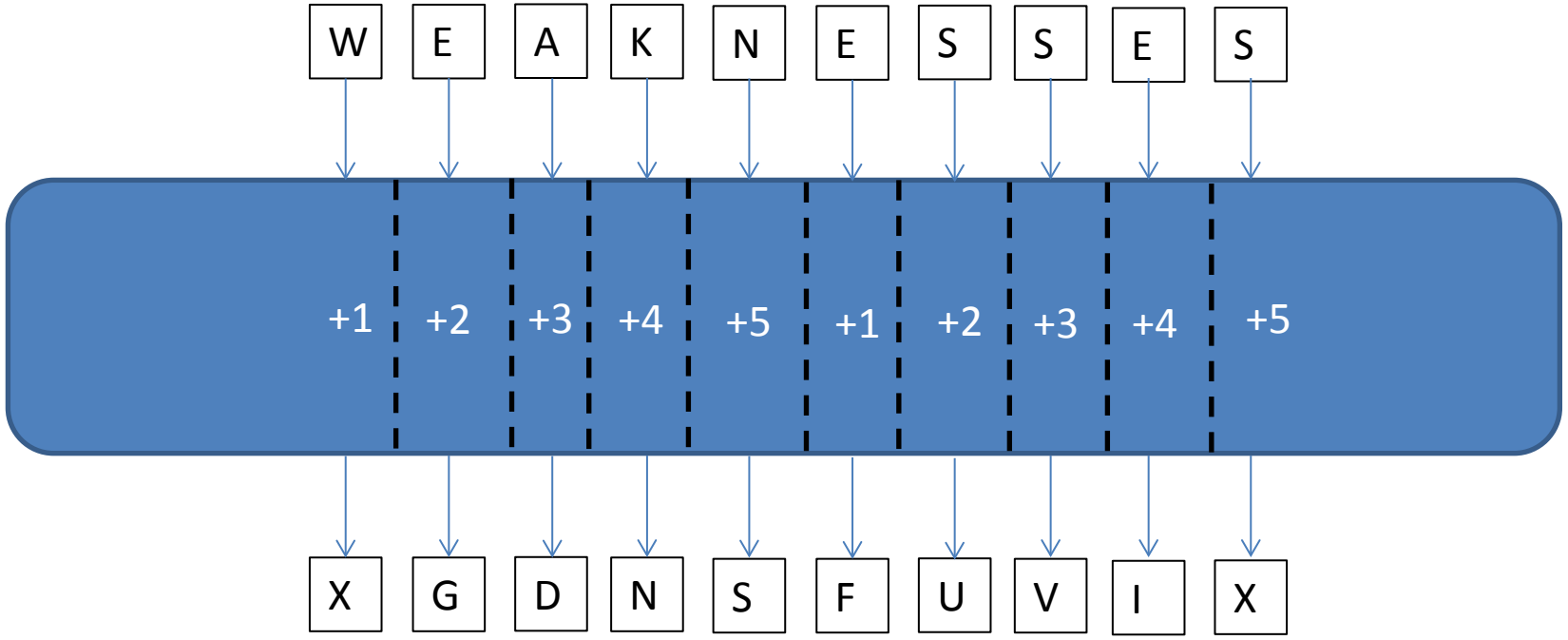
Simple Substitution Cipher



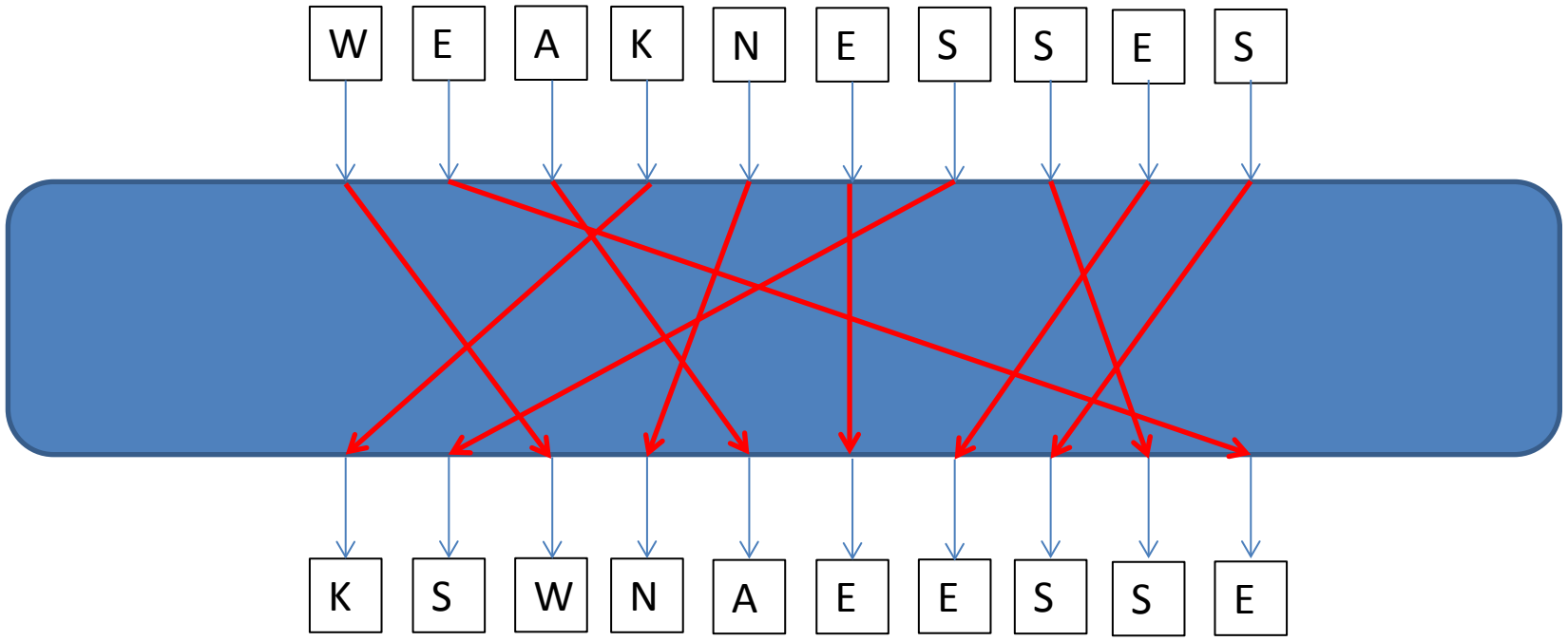
Homophonic Substitution Cipher



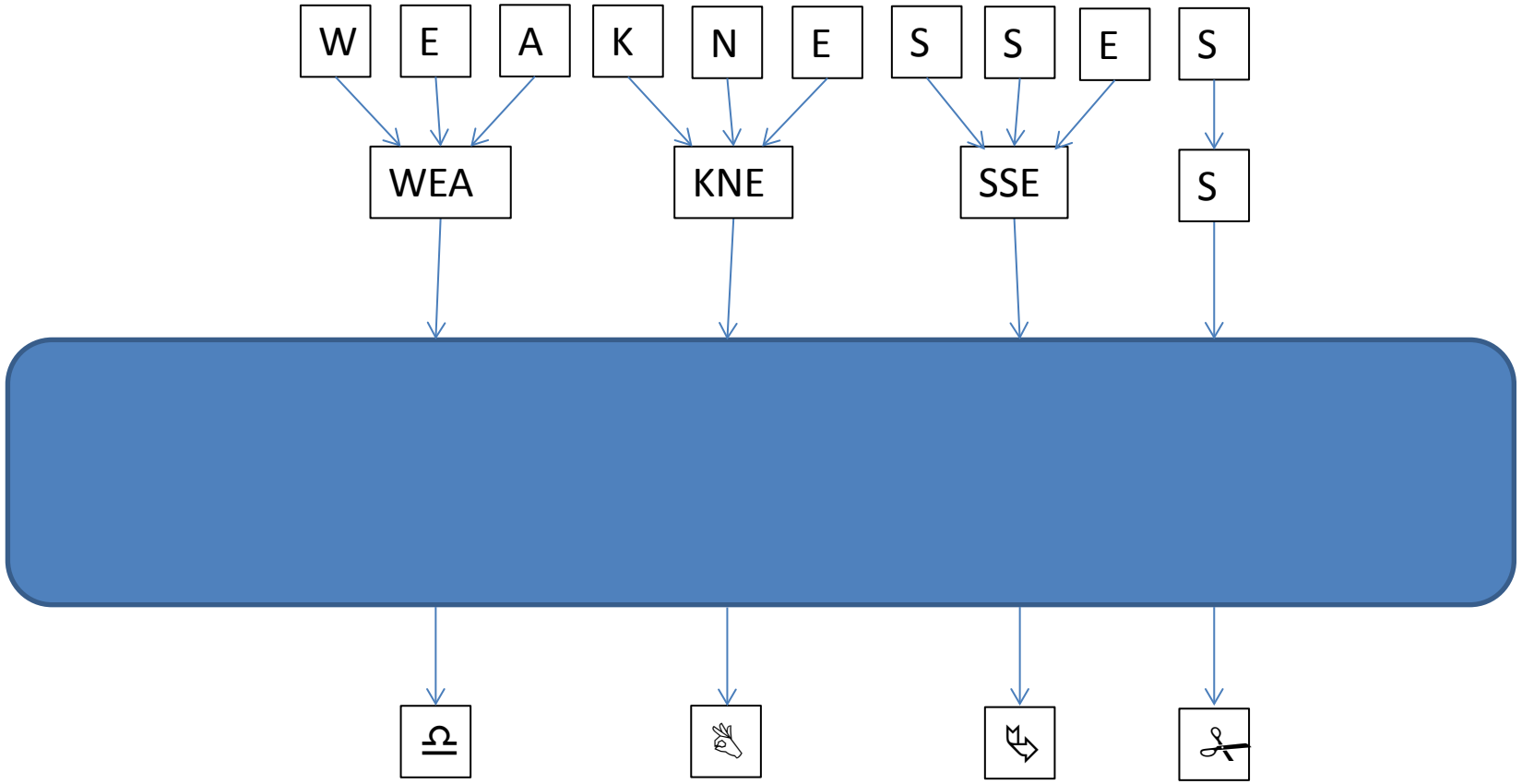
Polyalphabetic Substitution Cipher



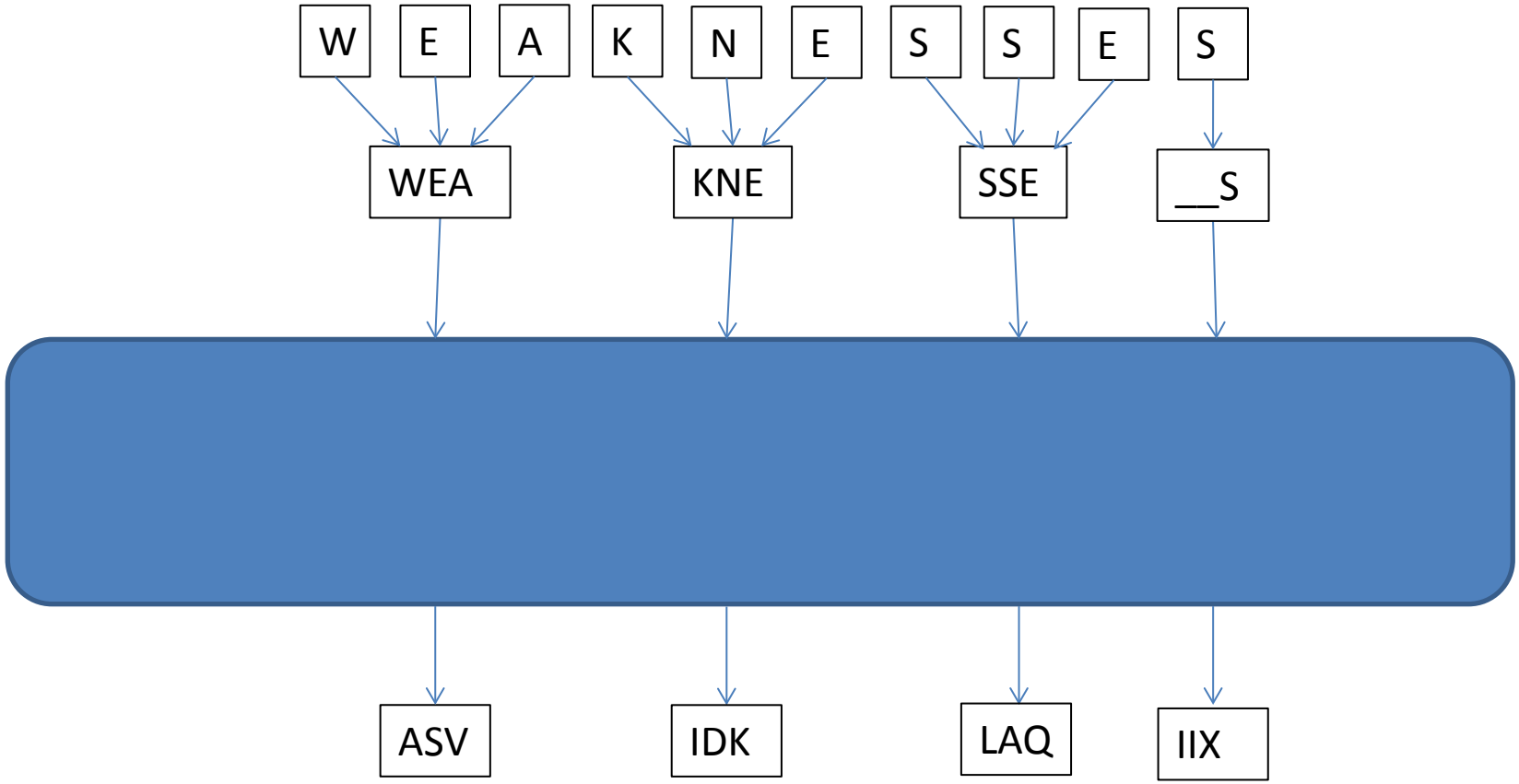
Transposition Ciphers



Block Ciphers



Kombination: Polygram Substitution Cipher

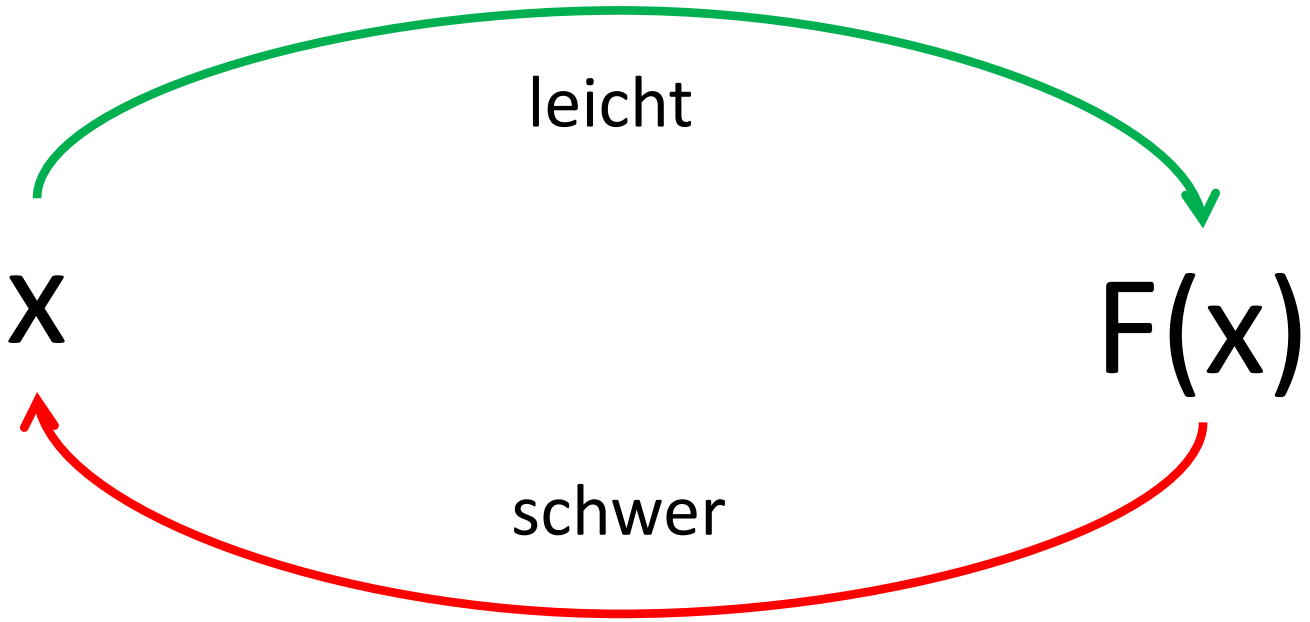


Kryptografische Funktionen

- One-Way Functions
- Trapdoor Functions
- Hash Functions
- Digitale Signaturen mit Hash Funktionen
- Kryptografische Hash Funktionen

One-Way Functions

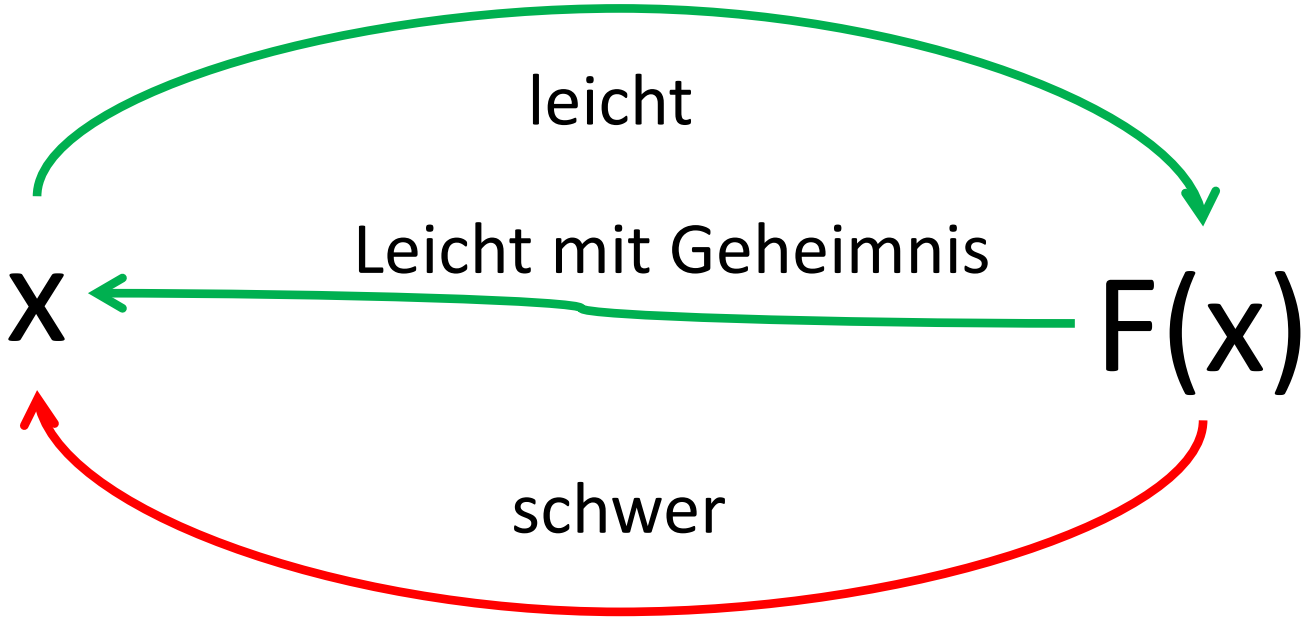
- Leicht zu berechnen
- Schwer umzukehren



z.B.:
Radizieren <-> Quadrieren

Trapdoor Functions

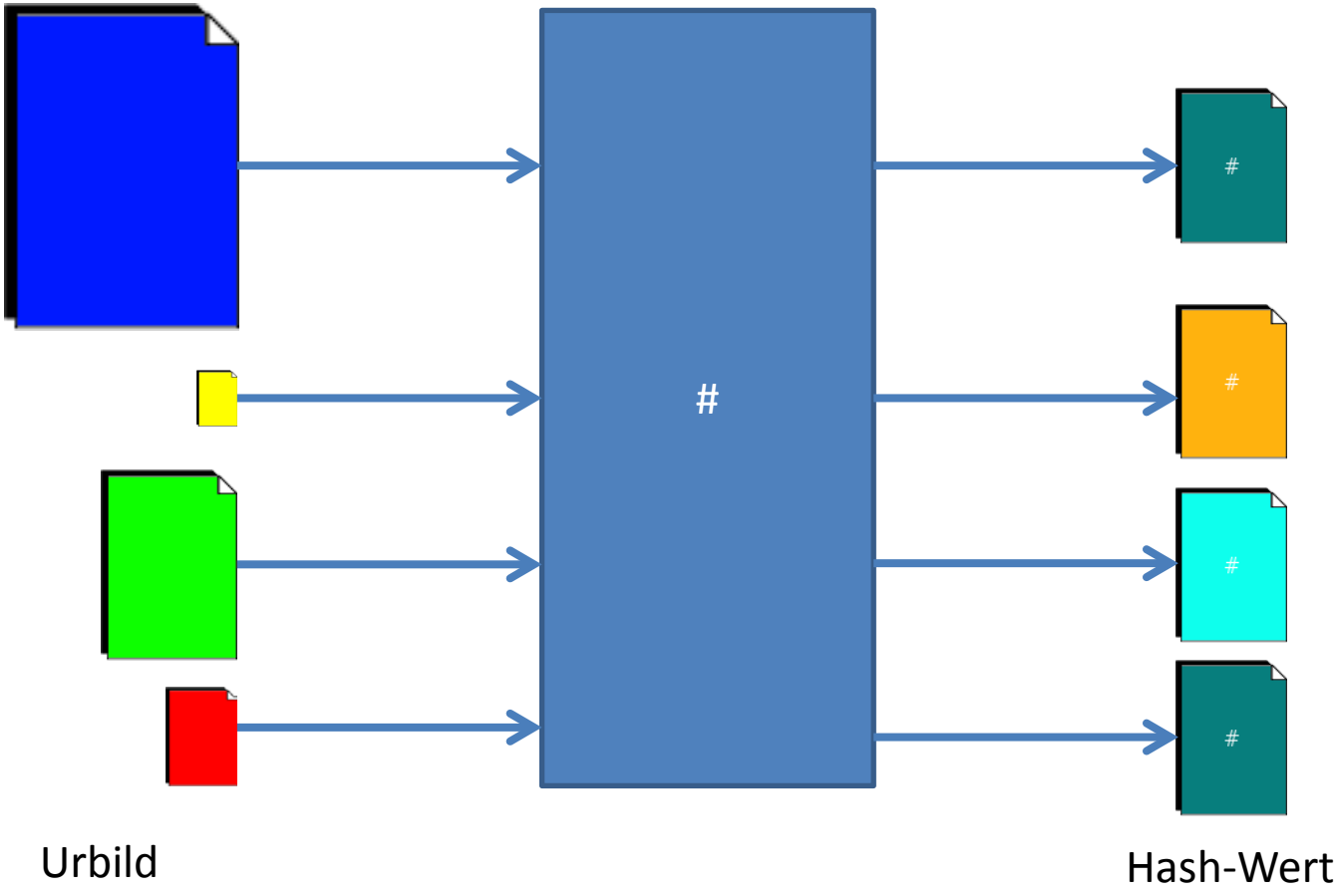
- Leicht zu berechnen
- Ohne Geheimnis schwer umzukehren



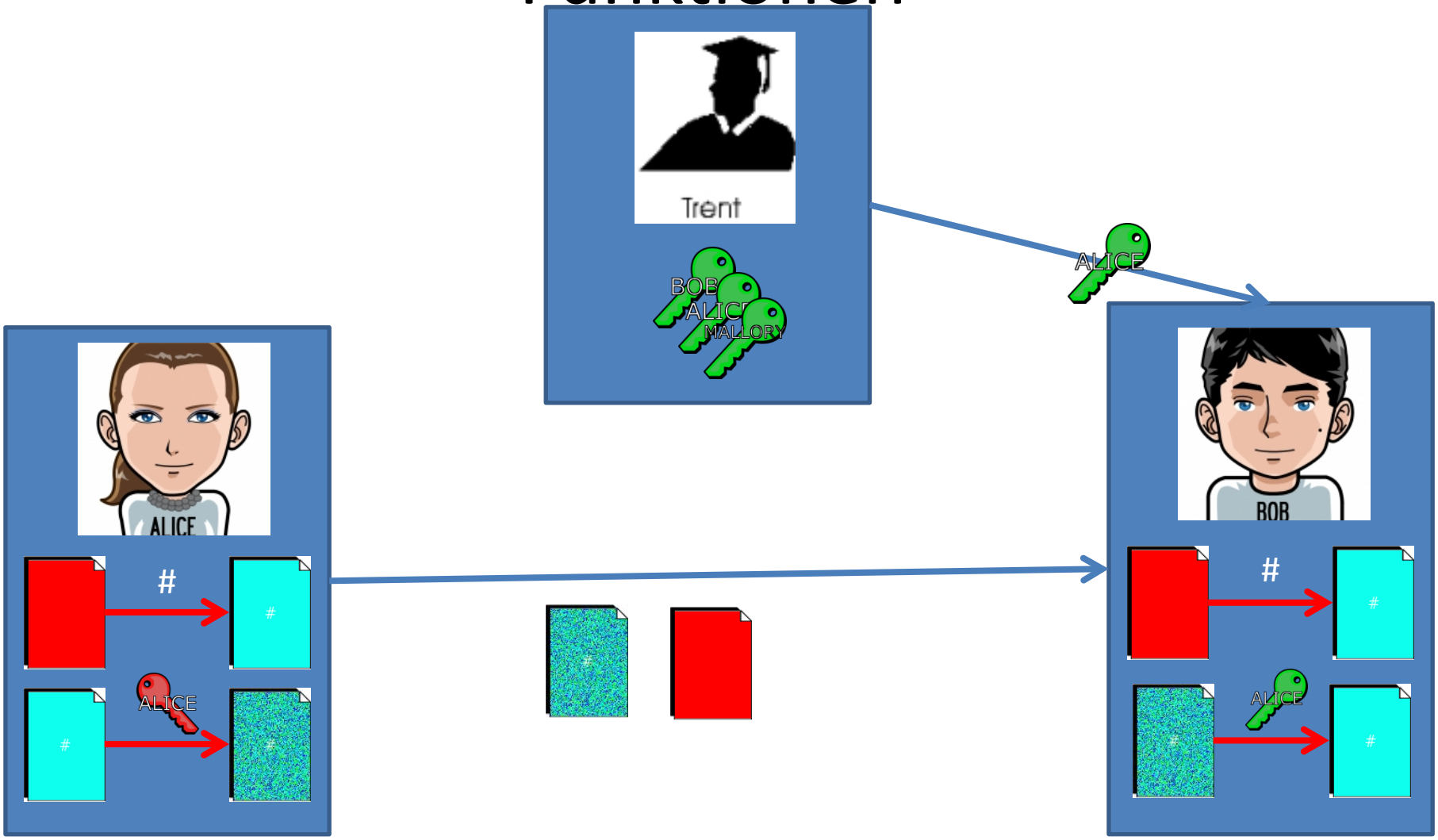
z.B.:
Primfaktorzerlegung <-> Multiplikation

Hash Functions

- Wandeln beliebig große Eingaben in gleichgroße Ausgaben um



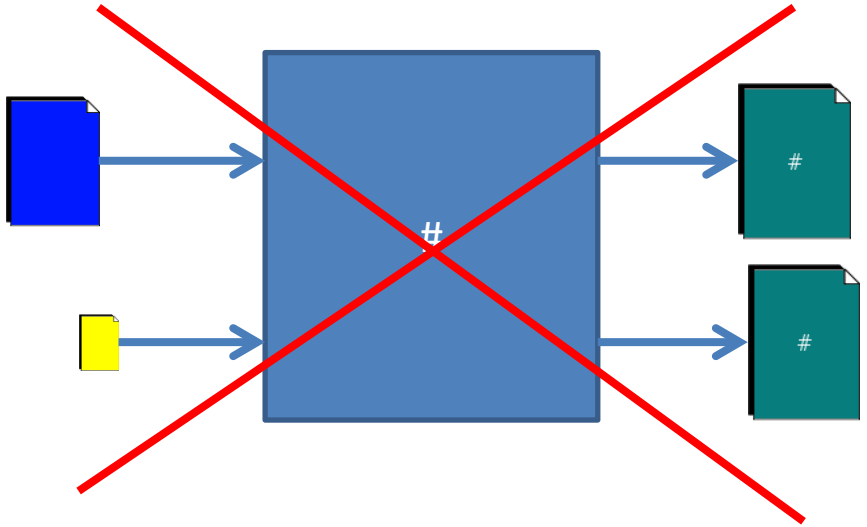
Digitale Signaturen mit Hash Funktionen



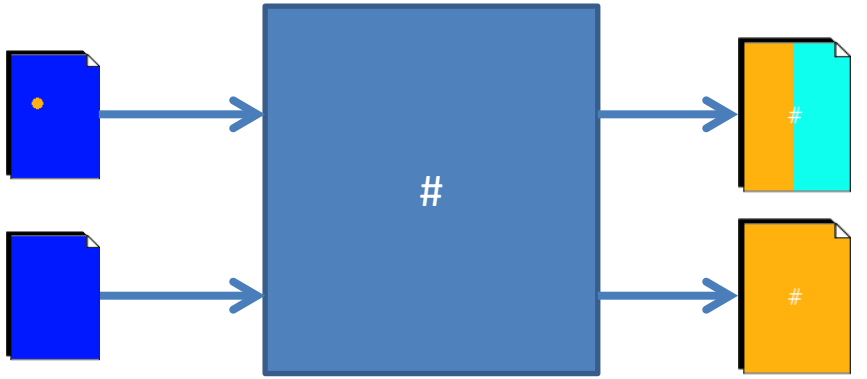
Kryptografische Hash Funktionen

Starke Kollisionsresistenz

(collision free)

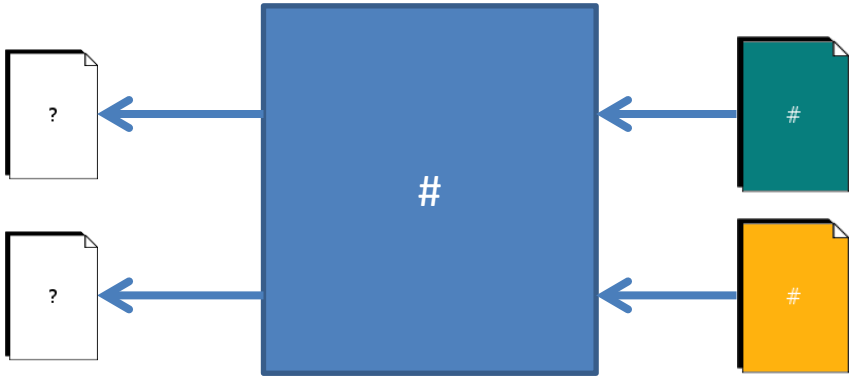


Chaos

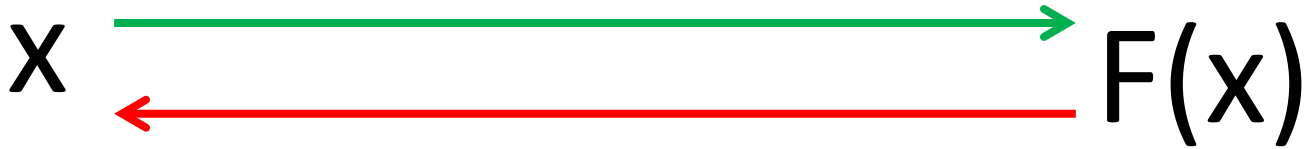


Kryptografische Hash Funktionen

Surjektivität



One-Way Eigenschaft



Mögliche Trapdoor Functions

Primfaktorzerlegung

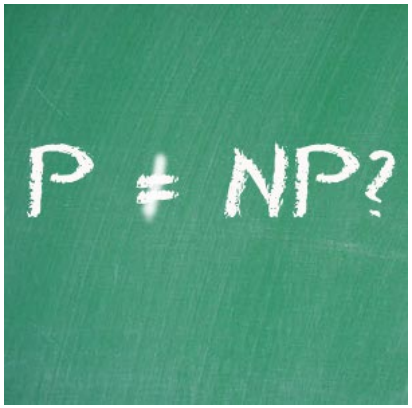
NP-Vollständige Probleme

Sichere Kryptografie?

Primfaktorzerlegung

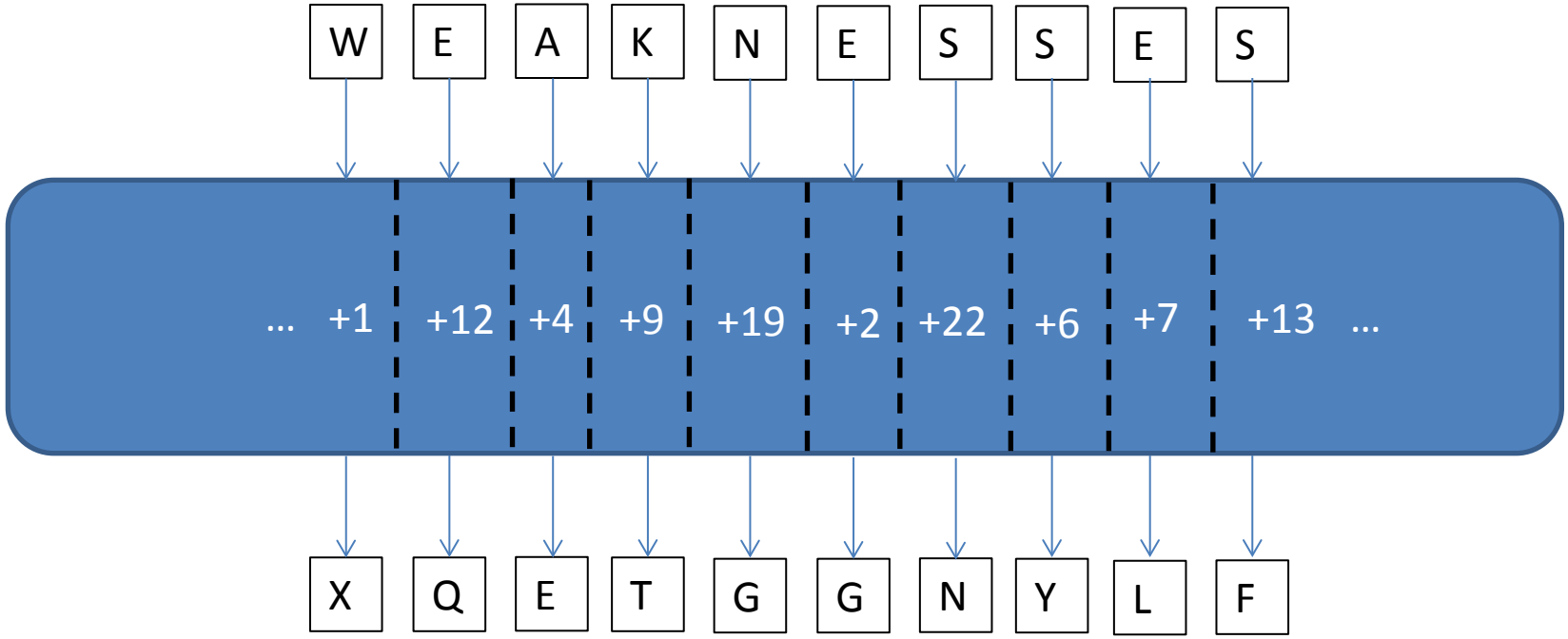
http://sparkedminds.in/worlds-most-expensive-computer/

NP-Vollständige Probleme



http://www.techpoweredmath.com/wp-content/uploads/2010/08/p-np.jpg

Sichere Kryptografie: One-time Pads

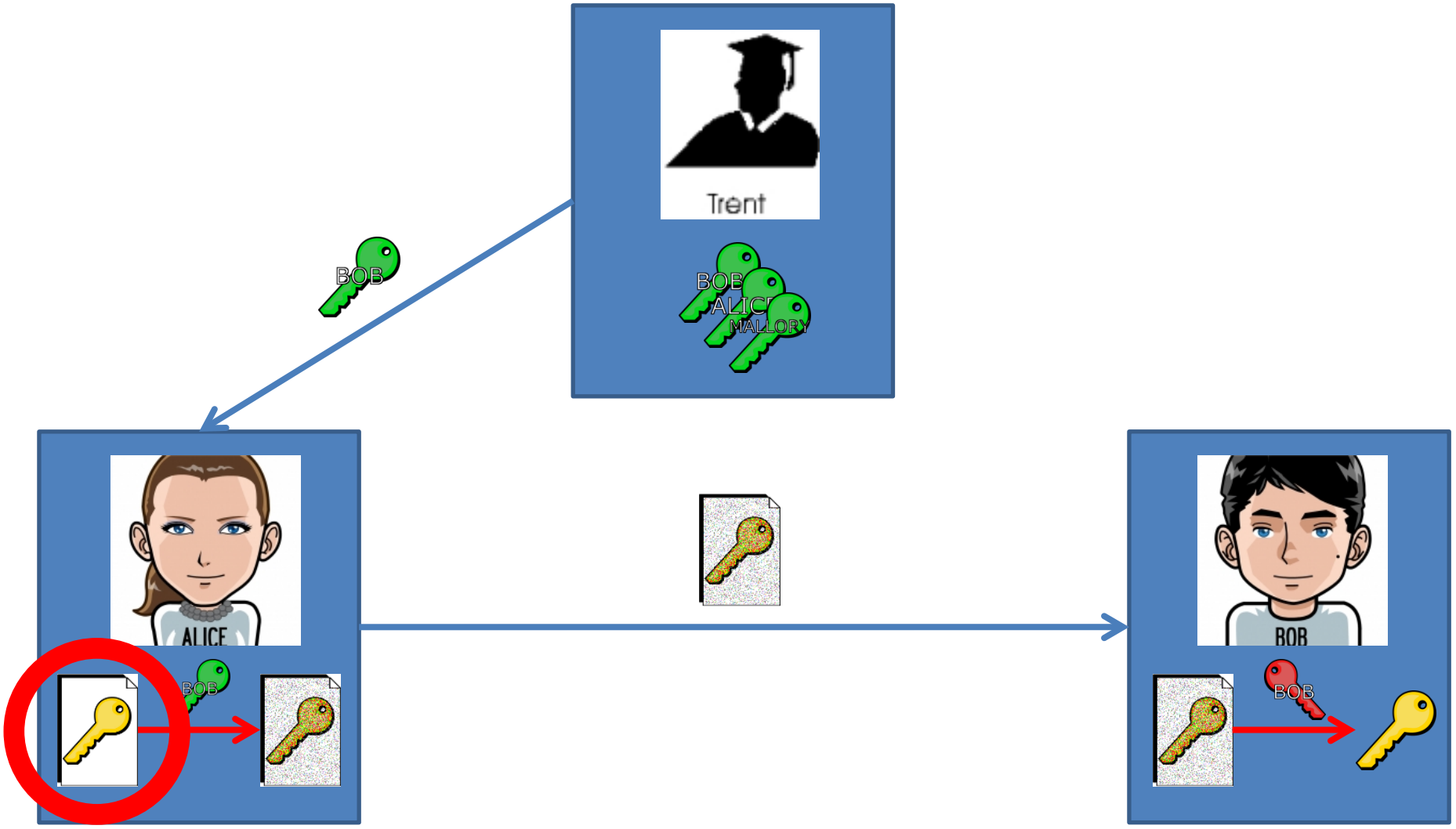


XQETGGNYLF → WEAKNESSES
XQETGGNYLF → PHILOSOPHY

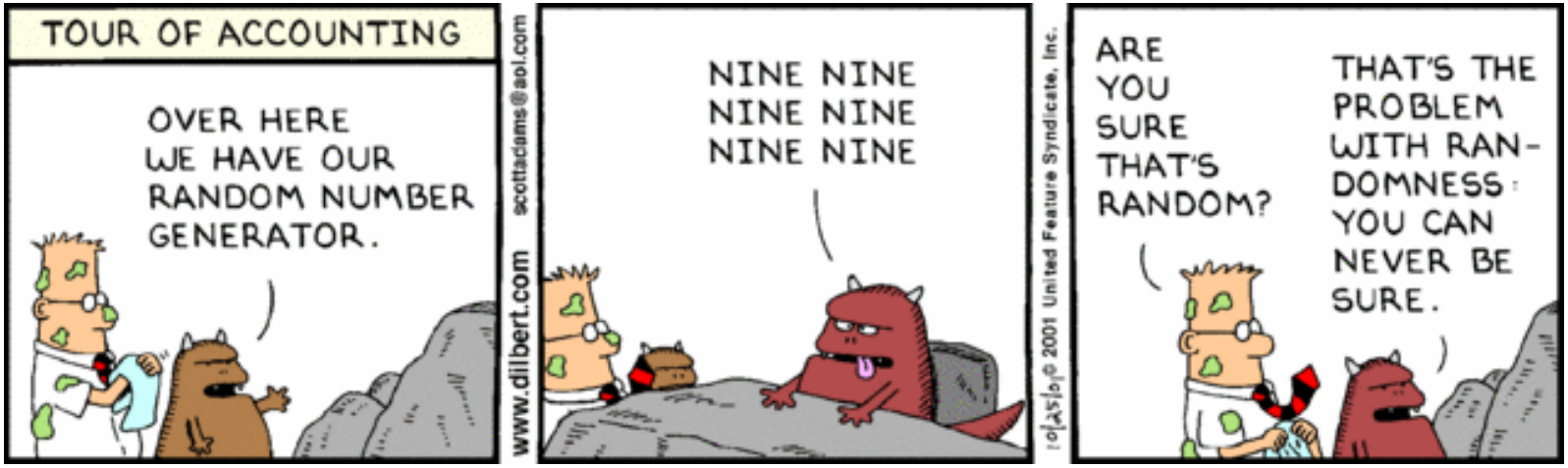
Zufallszahlengenerierung

- Wozu Zufallszahlen?
- Zufälligkeit
- Pseudozufallszahlen
- Kryptografische Zufallszahlen
- Echte Zufallszahlen

Wozu Zufallszahlen?

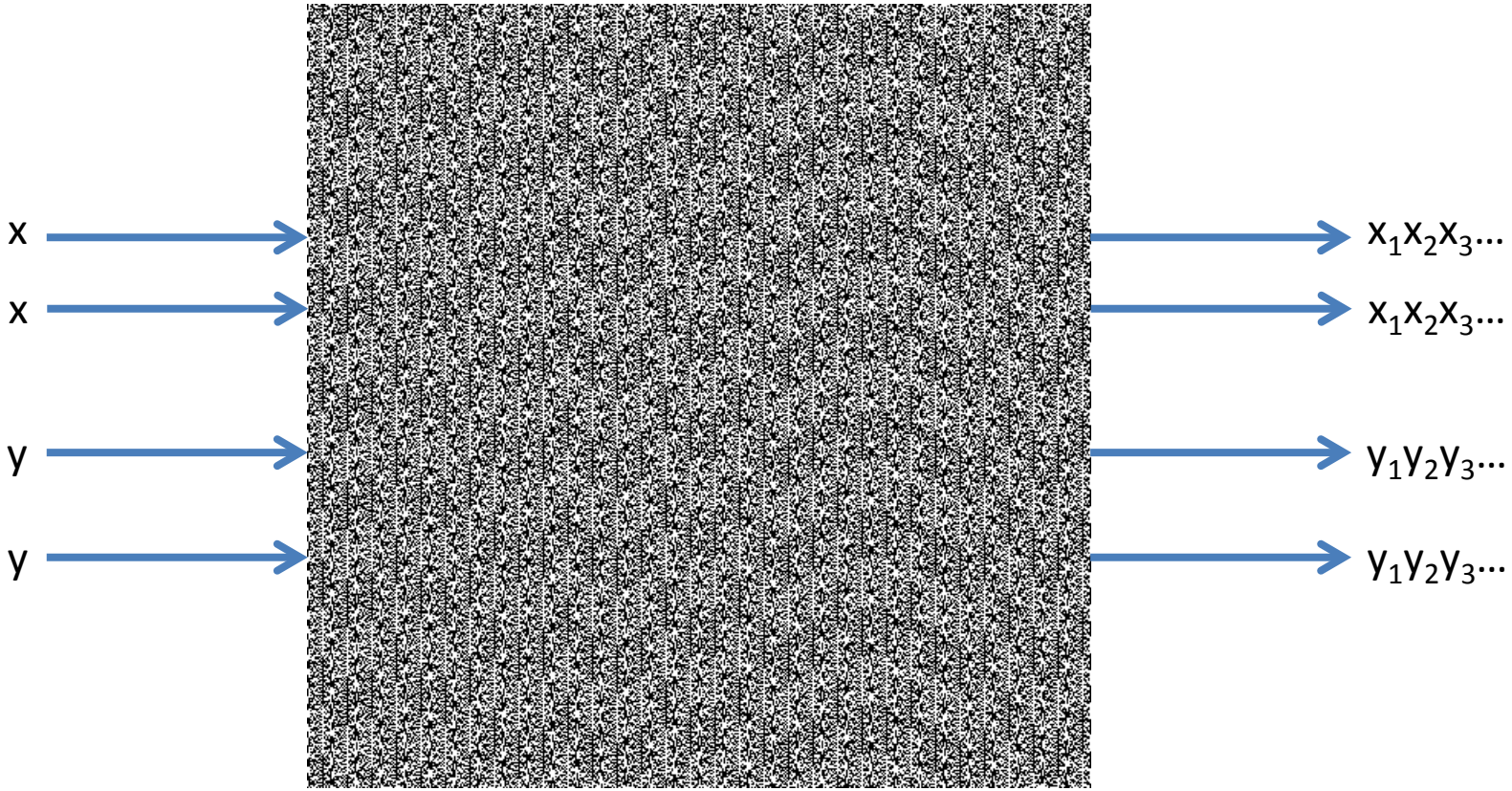


Zufälligkeit



Pseudozufallszahlen

1. Die Zahlen sehen zufällig aus.

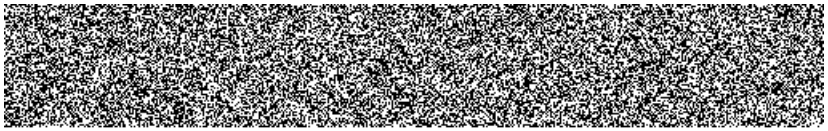


http://www.random.org/analysis/#visual

rand() in PHP unter Windows

Kryptografische Zufallszahlen

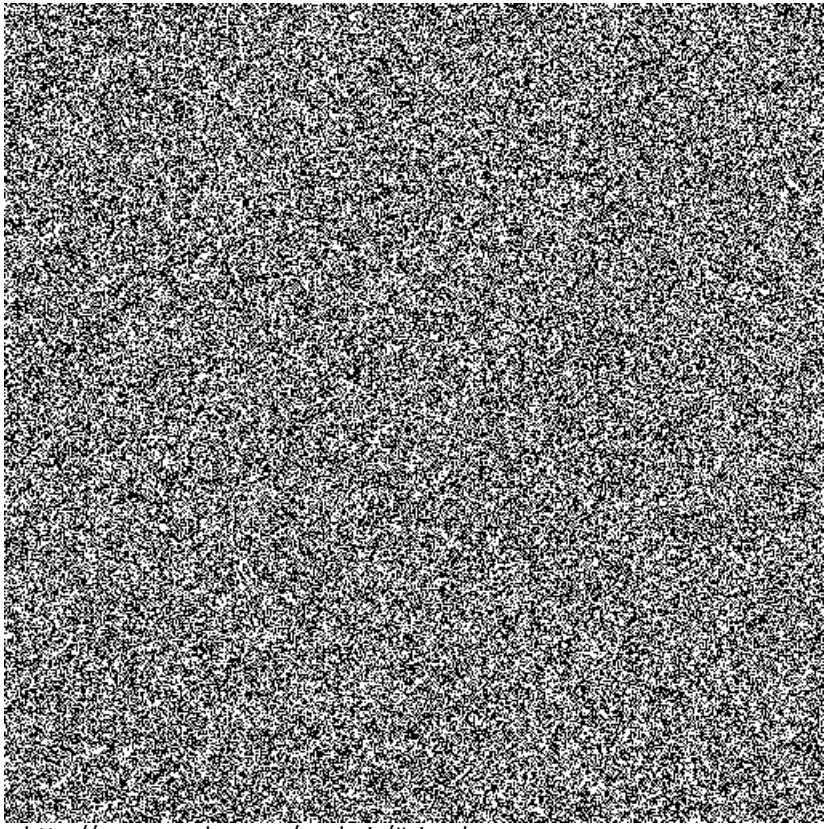
2. Die Zahlen sind unvorhersehbar.



?

Echte Zufallszahlen

3. Die Zahlen sind nicht verlässlich reproduzierbar.



http://www.random.org/analysis/#visual

Random.org (Atmosphärisches Rauschen)

Zusammenfassung

- Einleitung und Begriffsklärung
- Public Key Verfahren
- Angriffe
- Ciphers
- Kryptografische Funktionen
- Zufallszahlengenerierung