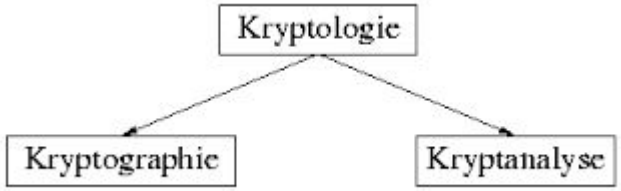
Kryptographie

Terminologie

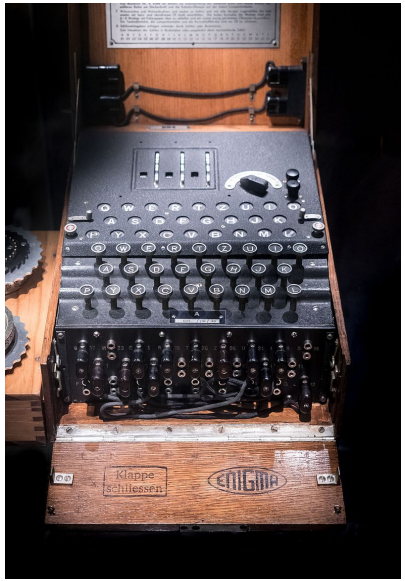
- Kryptologie
- Kryptographie
- Kryptoanalyse



- Authentizität
- Integrität
- Vertraulichkeit

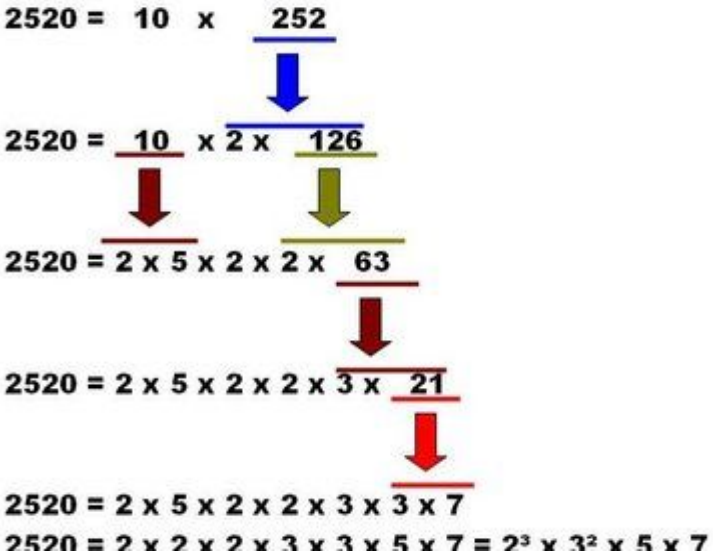
Geschichte der Kryptografie

- Epoche der Verschlüsselung mit Hand
  - Zeichenaustauschalgorithmen
- Epoche der Verschlüsselung mit speziellen Maschinen
  - Enigma
- Epoche der Verschlüsselung mit Computer
  - Data Encryption Standard
  - Public Key Kryptografie
  - Pretty Good Privacy
  - Advanced Encryption Standard



Mathematik

- Faktorisierung
  - Produkt aus großen Primzahlen
  - Berechnungsaufwand steigt stark



Symmetrische Verschlüsselung

- Beide Kommunikationspartner verwenden gleichen Schlüssel
- Schlüssel für Verschlüsselung und Entschlüsselung

Vorteil: Hohe Geschwindigkeit für Ver- und Entschlüsseln von Nachrichten

Nachteile: Schlüssel muss auf sicherem Weg überbracht werden

Implementierungen:

- DES (Data Encryption Standard)
- AES (Advanced Encryption Standard)
- OneTime-Pad (theoretisch unbrechbare Verschlüsselung)

Asymmetrische Verschlüsselung

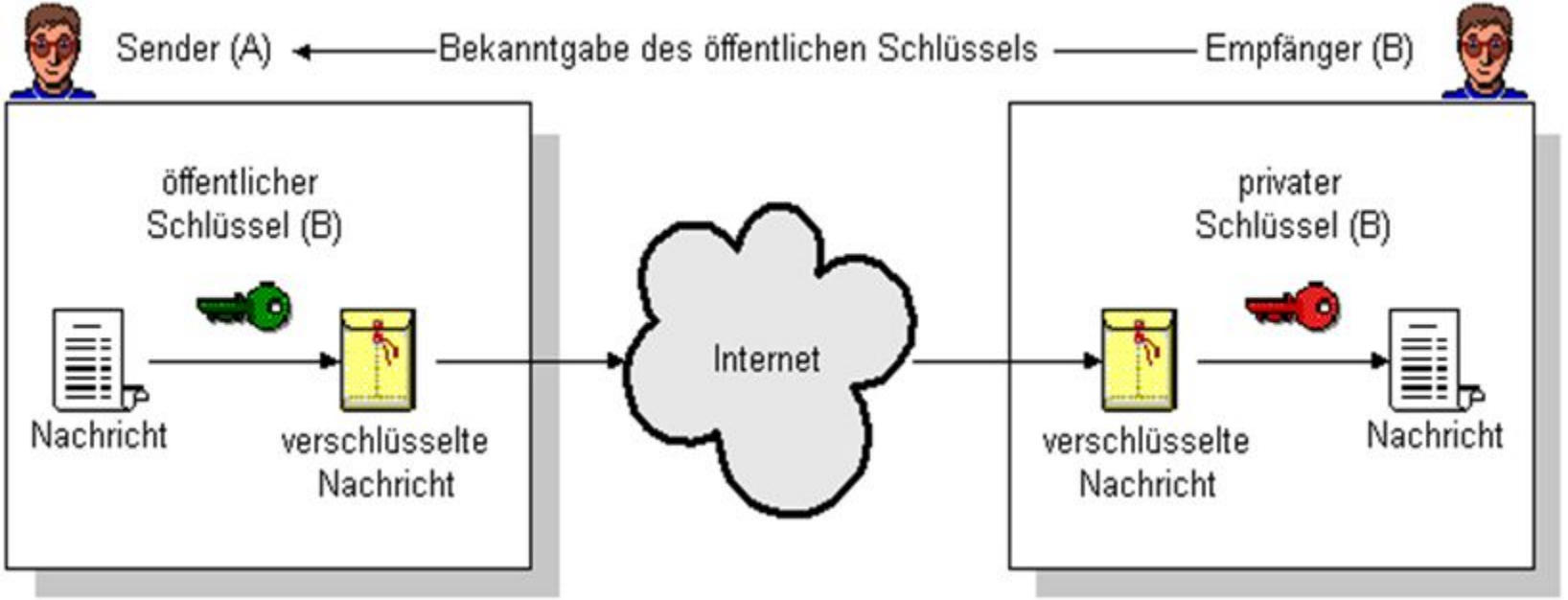
- Sowohl öffentlicher, als auch privater Schlüssel
- Verschlüsselung mit öffentlichem Schlüssel, Entschlüsselung allerdings **nur mit privatem Schlüssel** möglich
- Vorteile:
  - Hohe Sicherheit
  - Kein Schlüsselverteilungsproblem, da öffentlicher Schlüssel für jeden einzusehen ist
  - Authentifizierung durch elektronische Unterschriften (digitale Signatur) möglich
- Nachteile:
  - Asymmetrische Verschlüsselung ist wesentlich langsamer als symmetrische Verschlüsselung

Implementierungen:

- RSA (Rivest, Shamir, Adleman)

Asymmetrische Verschlüsselung

Beispiel:



Hashfunktionen

- Mathematische Funktion um Integration von Daten sicherzustellen
- Eingangsdaten können beliebig lang sein => Hashwert hat immer eine feste Größe

- Sicherstellung von Integration durch Prüfsummen
- Hashfunktionen sind nicht invertierbar, es gibt also für zwei Datensätze nicht gleiche Hashwerte

Implementierungen:

- MD5 (Message Digest Algorithm, gilt mittlerweile als unsicher)
- SHA-1 / SHA-256 (Secure Hash Standard)

Kryptoanalyse

Untersuchung des kryptographischen Verfahrens:

Versuchen...

1) ...das Verfahren / Algorithmus zu analysieren
2) ...den Schlüssel zu finden (Worst Case!)

oder

3) ...die Daten zu entschlüsseln

Kryptoanalyse

mit den Zielen:

-> potentielle Schwächen finden

-> in bestehende Systeme einzudringen

-> Schutzmechanismen auszuhebeln

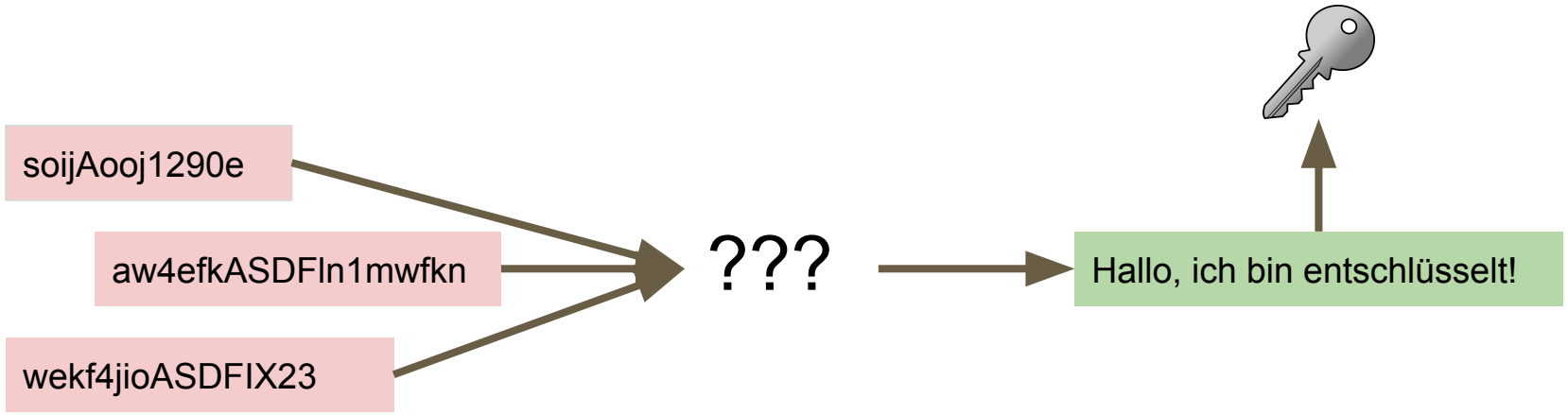
Kryptoanalyse

“Die Sicherheit darf nicht der Algorithmus, sondern die Geheimhaltung des Schlüssels”

August Kerckhoff

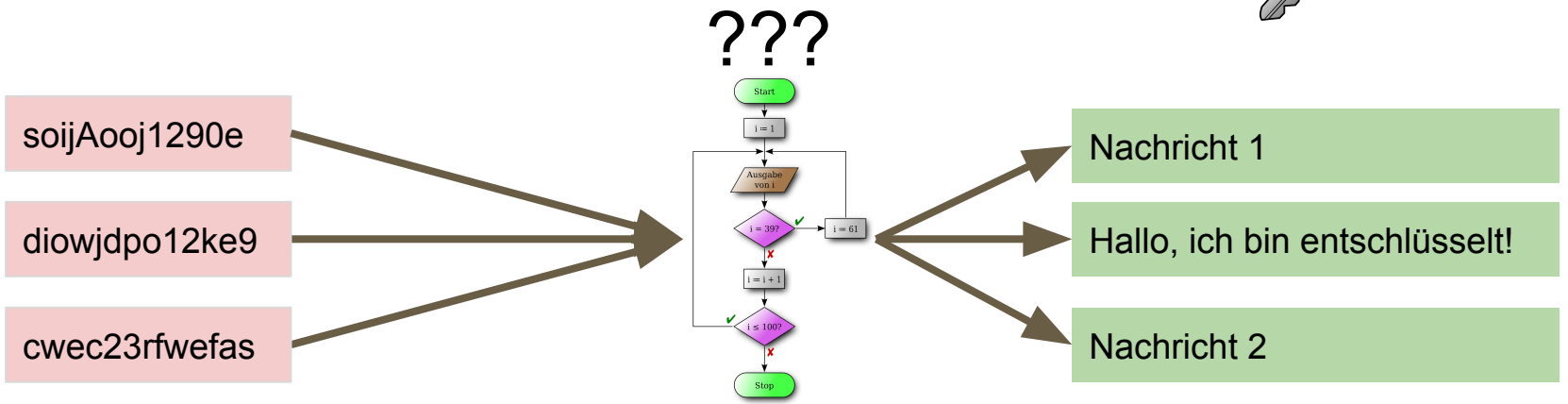
Kryptoanalyse

Die Angriffsverfahren: Ciphertext-Only (=nur verschlüsselter Text)



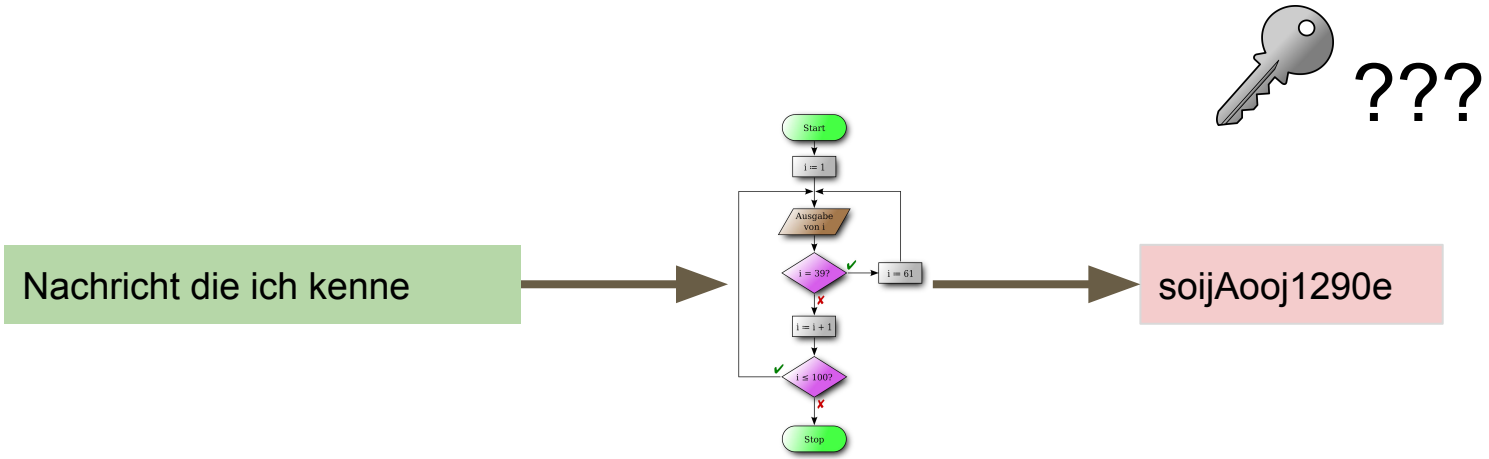
Kryptoanalyse

Die Angriffsverfahren: Known-Plaintext (=Geheim & Klartext)



Kryptoanalyse

Die Angriffsverfahren: Choosen-Plaintext (=Geheimtexte erzeugen)



Kryptoanalyse

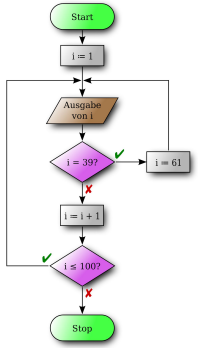
Die Angriffsverfahren: Choosen-Ciphertext (=Klartexte erzeugen)

???

soijAooj1290e

diowjdpo12ke9

cwec23rfwefas



Nachricht 1

NAchricht 2

Nachricht 3