CODERS.BAY

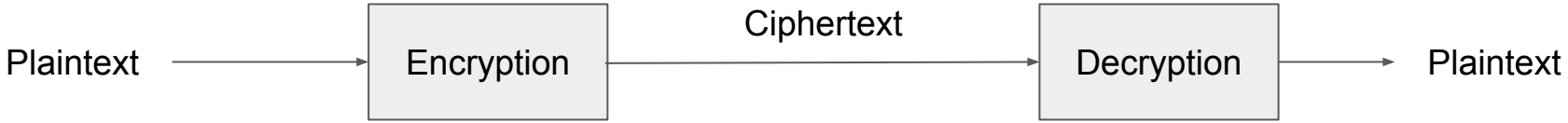
Kryptografie

Eine Einführung

Begriffe

- **Plaintext** – originale Nachricht.
- **Ciphertext** – Kodierte Nachricht.
- **Cipher** – Verschlüsselungsalgorithmus.
- **Key** – In der Chiffre verwendete Informationen, welche nur der Sender/Empfänger kennen.
- **Encrypt** – Verschlüsseln
- **Decrypt** – Entschlüsseln
- **Cryptography** – Studium der Verschlüsselungsprinzipien/ Methoden
- **Cryptanalysis** – Studium der Prinzipien / Methoden Entschlüsselung von Chiffretext ohne Kenntnis des Schlüssels
- **Cryptology** – Wissenschaftliches Gebiet von Kryptografie und Kryptoanalyse

Senden einer verschlüsselten Nachricht



Kerkhoffs’s principle (1883)

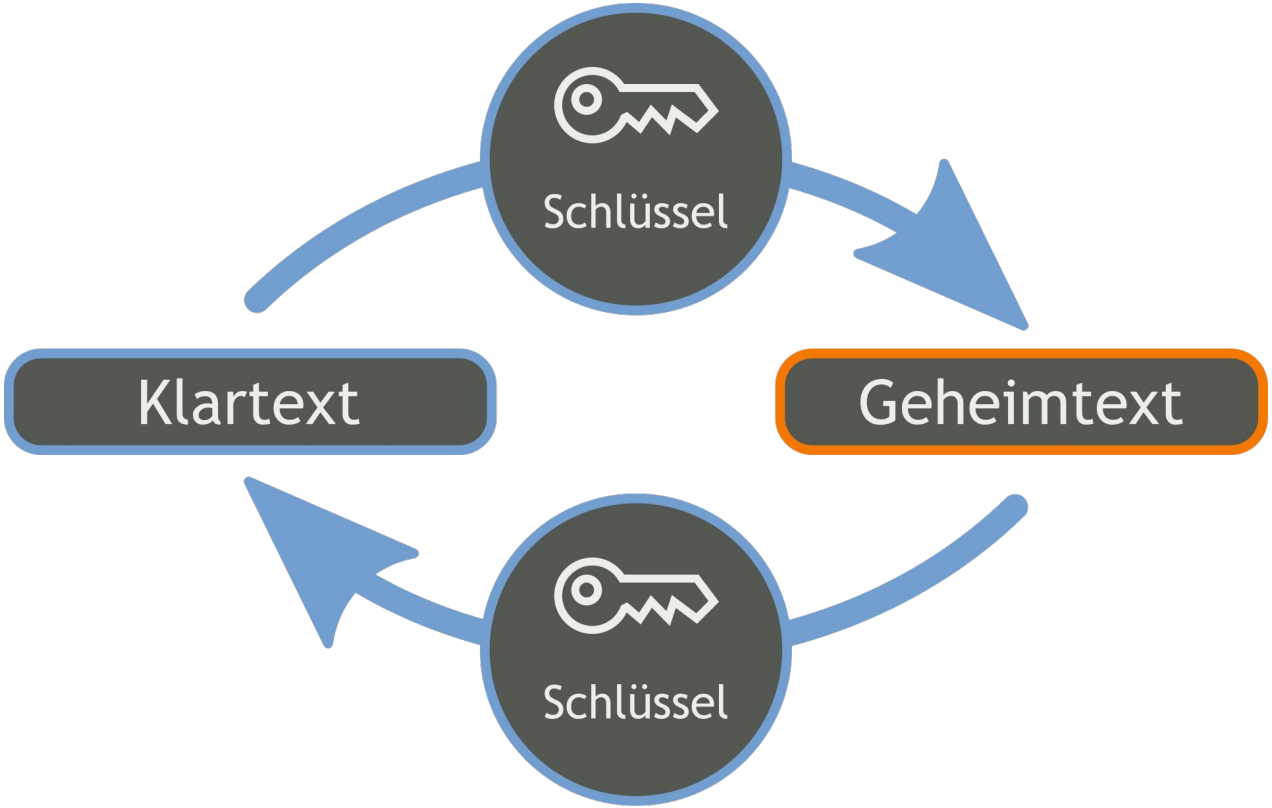
The system must not require secrecy.

Die Sicherheit eines Kryptosystems darf nicht davon, abhängenden kryptografischen Algorithmus geheim zu halten.

Klassifikation

- Cryptographic hash: 0 Schlüssel und nicht umkehrbar.
- Symmetric: 1 Schlüssel
  - Symmetrische Verschlüsselung wird auch cipher oder chiffre gennant.
    - Es gibt Block und Stream Chiffren.
- Asymmetric: 2 Schlüssel, einen **public key** und einen **private key.**
  - Key agreement
  - Asymmetric encryption
  - Asymmetric signature

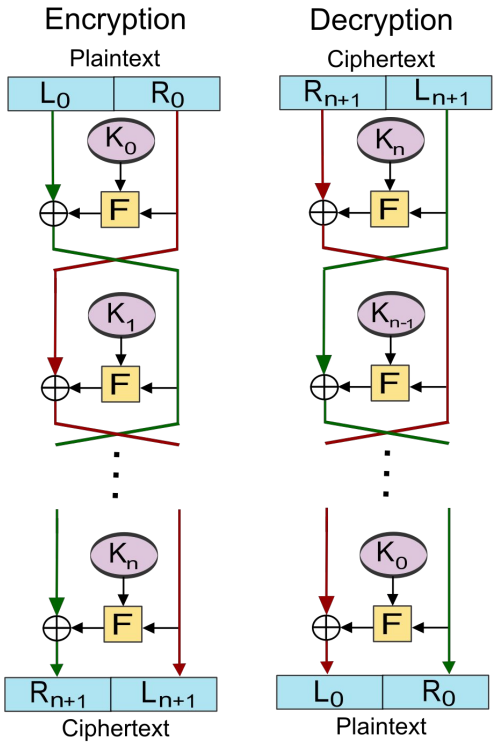
Symmetrische Verschlüsselung



Block Chiffren

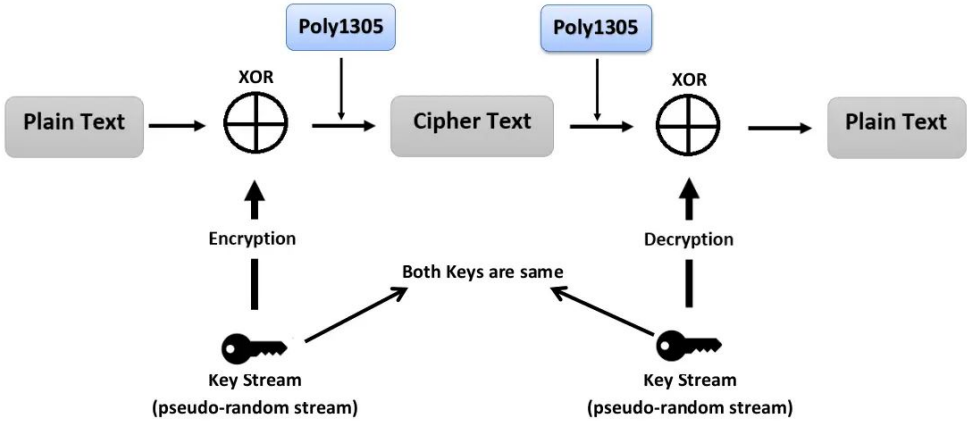
Blockchiffren verarbeiten Nachrichten in Blöcken, von denen jeder einzelne dann ver- und entschlüsselt wird. Beispiel: Feistelstruktur.

Feistelstruktur



Stream Chiffren

Diese Chiffren verarbeiten Nachrichten kontinuierlich bit- oder byteweise,



ChaCha20 Poly1305

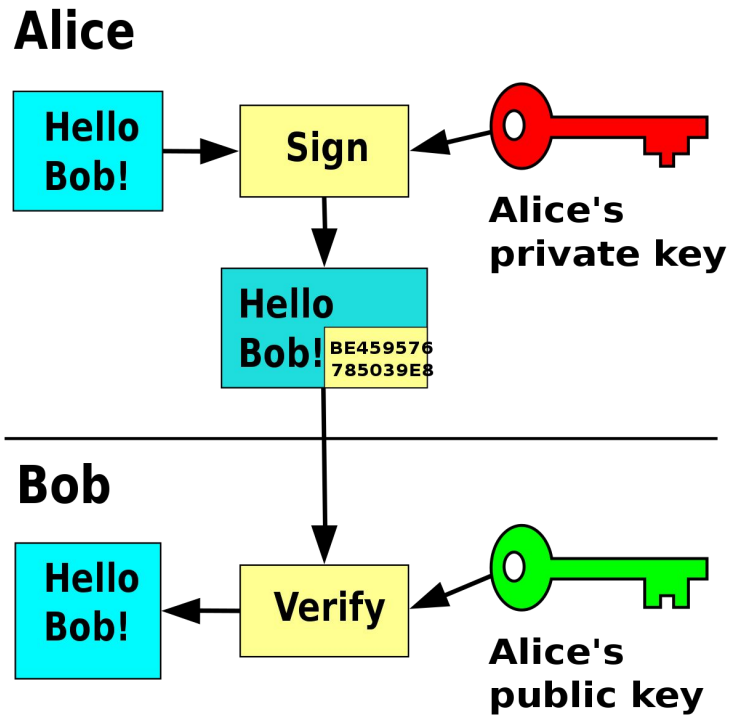
Source

Algorithmen

- Advanced Encryption Standard (AES)
- ChaCha20

Asymmetrische Verschlüsselung

Vom privaten Schlüssel kann (meistens) der öffentliche berechnet werden, aber nicht umgekehrt → one way function.



Rivest–Shamir–Adleman (RSA); Variablen

d: privater Exponent

e: öffentlicher Exponent

p, q: Primzahlen

n: Modulus; Produkt von p und q

m: Klartext Nachricht

c: Ciphertext

RSA finden der Schlüssel

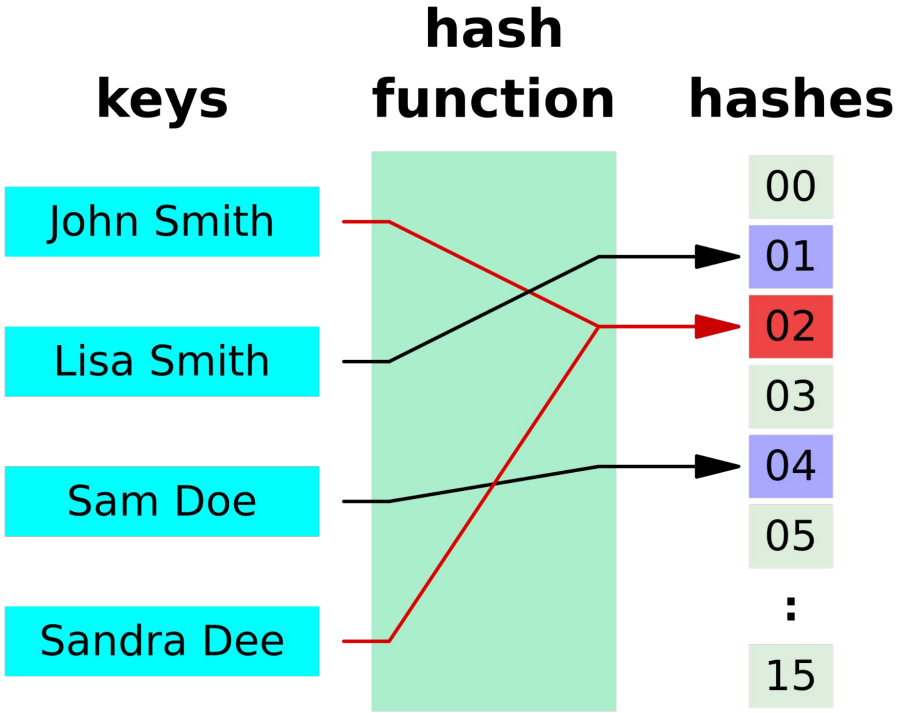
Finden der Schlüssel, Variablen

1. Finde zwei große Primzahlen p und q und berechne deren Produkt
2. Berechne die Totient Funktion $\phi(n) = (p-1) \cdot (q-1)$
3. Wähle zufällig e coprime zu $\phi(n)$
4. Zum Schluss: finde d, sodass $d = e^{-1} \ mod \ \phi(n)$
   a. Mit beispielsweise dem extended euclidean algorithm.
5. Der Benutzer e und n als public key und d als seinen private key.
6. p und q werden nicht mehr gebraucht und sollten gelöscht werden.

Algorithmen

- Rivest–Shamir–Adleman (RSA)
- Elliptic Curve Digital Signature Algorithm (ECDSA)

Hashing


keys
hash function
hashes
John Smith
Lisa Smith
Sam Doe
Sandra Dee
00
01
02
03
04
05
:
15

One Way Function

Hash Algorithmen sind sogenannte one way functions. Sie wandeln Werte in Hashes um, aber von einem Hash kann man nicht wieder zurück in einen Wert.

$$h = H(m)$$

H(m) berechnet den kryptografischen Fingerprint der Nachricht m. Die Funktion ist nicht injektiv. Jedoch ist sie surjektiv.

Bei gleichem Input muss immer der gleiche Hash erzeugt werden.

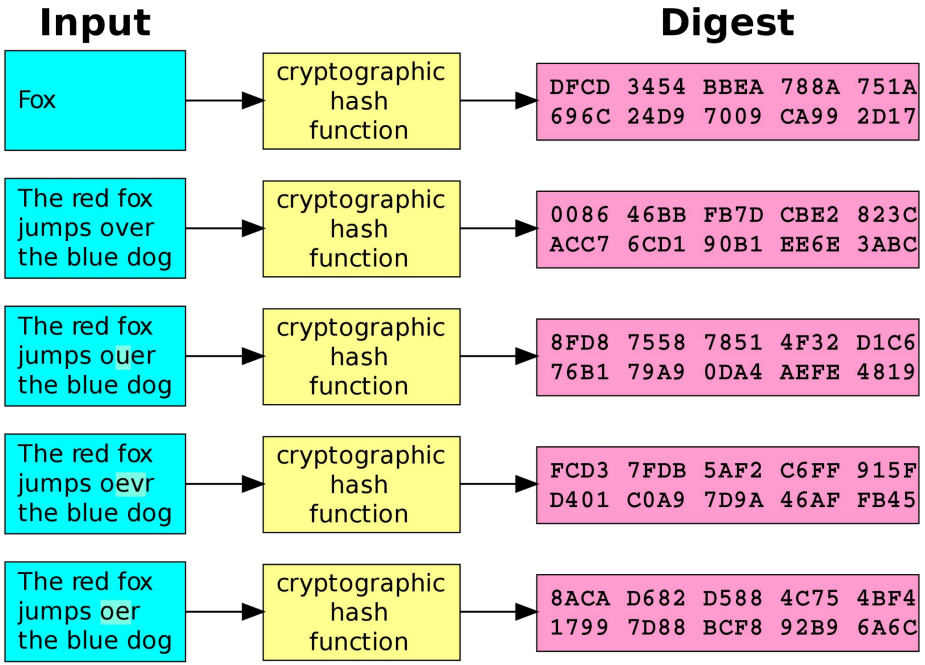
Kryptografische Hashfunktionen

Algorithmen:

- SHA – 3
- DSA

Eigenschaften:

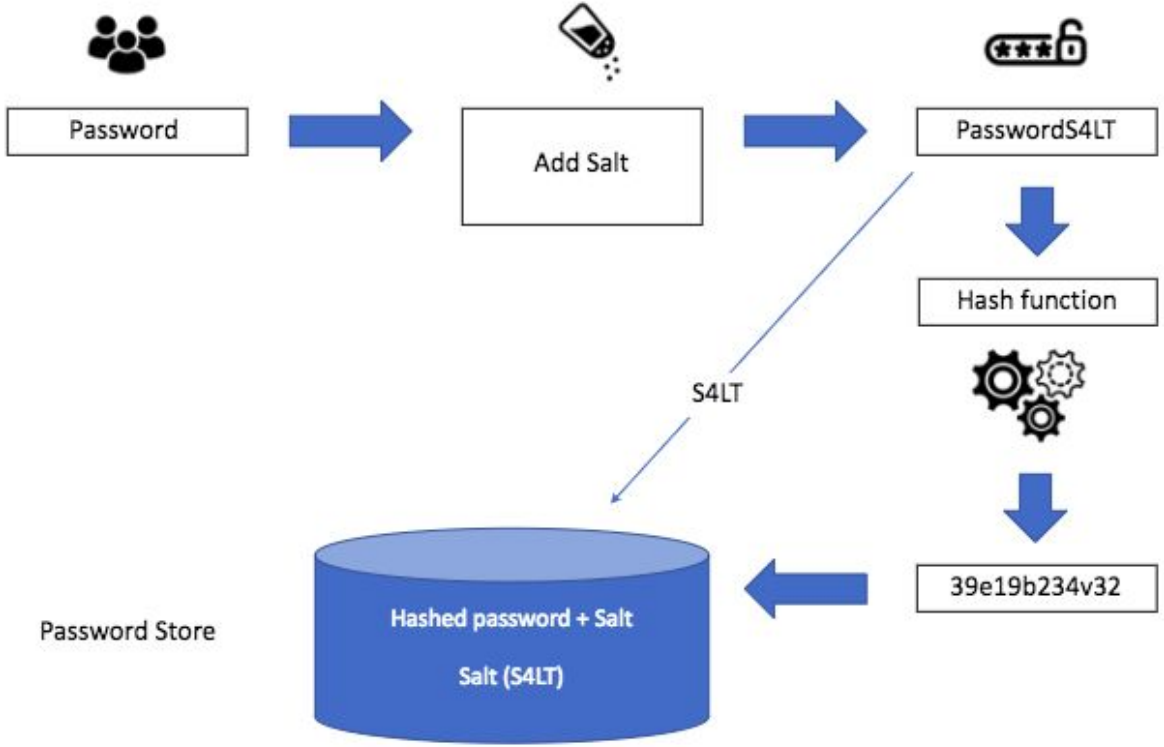
- Beliebige Eingabelänge
- Feste Ausgabelänge, z. B. 256 Bits
- Effizienz (bei Berechnung von h)
- One way Funktion
- Weak collision resistance
- Strong collision resistance
- Pseudozufälligkeit



Wozu benötigt man Kryptografisches Hashing?

- Digitale Signaturen
- Pseudonymisierung und Datenschutz
- Integritätsschutz (Erkennung von Manipulationen)
- Passwort-Speicherung

Salting



Source

Ausblick und Themen nach Wunsch

- Signaturen
- Elliptic Curve Signatures
- Transport Layer Security
- Zero knowledge
- Key Exchange
  - Quantum key distribution
- Angriffe auf Kryptosysteme