Verschlüsselung

Verschlüsselung und Entschlüsselung

Inhalt

- Geschichte
- Verschlüsselungsverfahren
- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung
- Hybride Verschlüsselung
- Entschlüsselung
- Anwendungsbeispiel

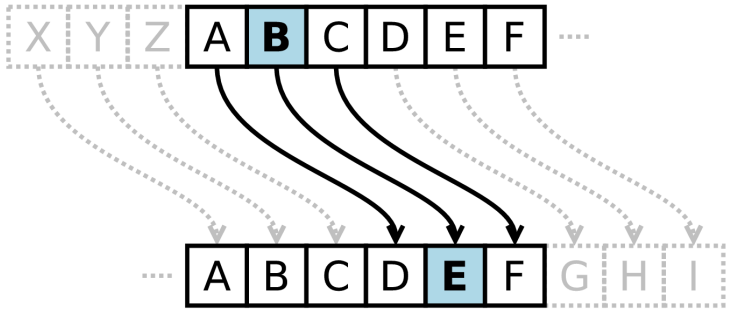
Geschichte der Verschlüsselung

- Skytale
- Cäsar-Verschlüsselung
- Enigma
- One-Time-Pad

Skytale

- Entwickelt im Jahre 500 v. Chr.
- Militärische Verschlüsselungsverfahren
- Eingesetzt von den Spartanern
- Holzstab mit Lederstreifen

Cäsar-Verschlüsselung



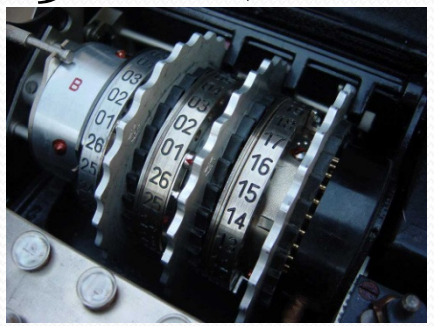
- Entwickelt ca. 50 v. Chr.
- Verschiebung der Buchstaben
- Leichte Entzifferung
- Wurde Weiterentwickelt (ROT-Verschlüsselung)

Enigma

- Entwickelt vom Arthur Scherbius (Elektroingenieur)
- Patentanmeldung 1918
- Rotorschlüsselmaschine
- Fertigstellung am 9. Juli 1923

Enigma (Aufbau u. Anwendung)

- Holzgehäuse (340 mm * 280 mm * 150 mm)
- Gewicht von ca. 12 kg



- Walzensatz von drei austauschbaren Walzen
- Vor jedem Funkspruch wurde die Startposition geändert.

One-Time Pad (Einmal-Block)

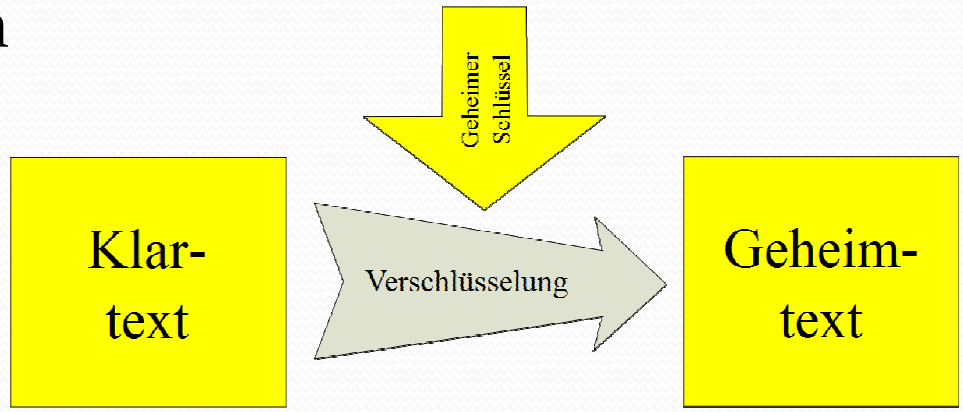
- symmetrisches Verschlüsselungsverfahren
- Schlüssel ist so lang wie die Nachricht selbst
- Schlüssel enthält zufällige Zeichen
- Bis heute sichere Verschlüsselung

Verschlüsselungsverfahren

- Einwegverschlüsselung
  - Mathematische Funktionen, welche schwer umgekehrt werden können (schwere Entschlüsselung)
  - Hashwert-Funktion
- Mehrwegverschlüsselung
  - Mehrere Schlüssel erzeugen das selbe Ergebnis (Beispiel: 2 * 4 = 8 und 24 : 3 = 8)
  - Ursprung der asymmetrischen Verschlüsselung

Symmetrische Verschlüsselung

- Verfahren
- Klassische Verfahren
- Moderne Verfahren



Symmetrische Verschlüsselung (Verfahren)

- Gleichen Schlüssel für die Ver- und Entschlüsselung
- Verschlüsselte Nachricht kann nur entschlüsselt werden, wenn beide Partner den selben Schlüssel verwenden.
- Schwierigkeit bei der Übergabe von Schlüssel

Symmetrische Verschlüsselung (klassische Verfahren)

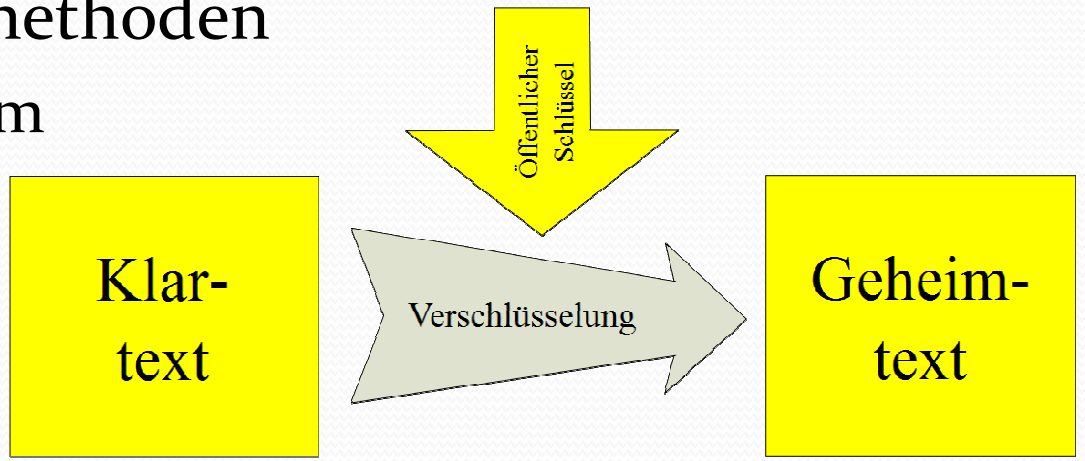
- Cäsar-Verschlüsselung
- DES - Data Encryption Standard
  - Vorgänger „Lucifer“ wurde von IBM entwickelt
  - Entwickelt von IBM in Zusammenarbeit mit der NSA
  - Schlüssellänge von nur 56 Bits
- One-Time-Pad

Symmetrische Verschlüsselung (moderne Verfahren)

- 3DES - Triple- Data Encryption Standard
  - Mehrfaches verwenden von DES mit zwei unterschiedlichen Schlüsseln
  - Schlüssellänge: 3 * 56 Bits = 168 Bits, effektiv aber nur 112 Bits
- AES - Advanced Encryption Standard
  - Nachfolger von DES / 3DES
  - Algorithmus ist frei verfügbar und darf ohne Lizenzgebühren eingesetzt
- Twofish
  - Nachfolger von Blowfish
  - Schlüssellängen: 128, 192 oder 256 Bit je nach Anzahl der Verschlüsselungsdruchgänge

Asymmetrische Verschlüsselung

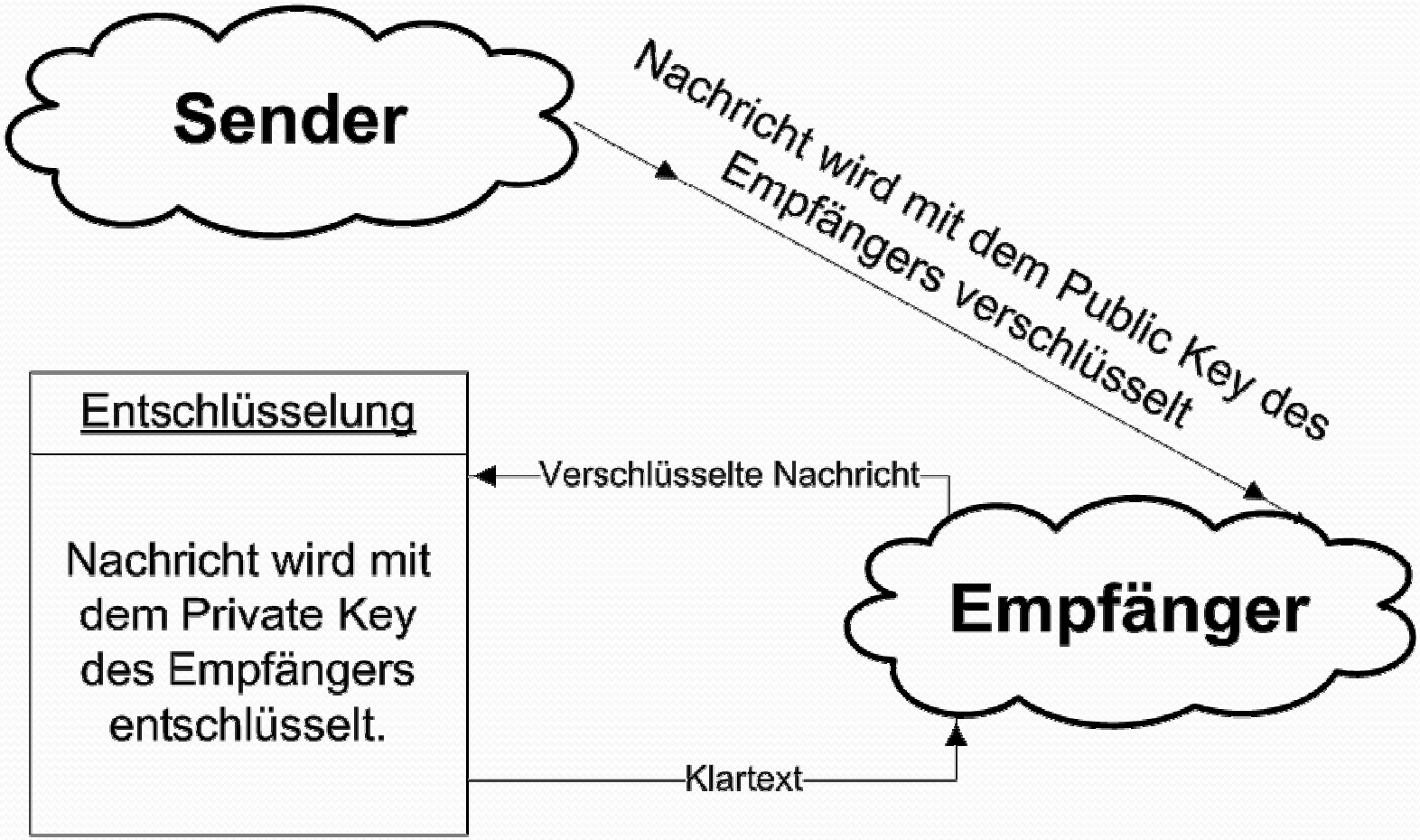
- Verfahren
- Ablauf
- Verschlüsselungsmethoden
  - RSA-Kryptosystem



Asymmetrische Verschlüsselung (Verfahren)

- Public Key – mit dem Public Key des Empfängers wird die zu sendende Nachricht verschlüsselt
- Private Key – dient zur Entschlüsselung der Nachricht, welche mit dem Public Key verschlüsselt wurde
- Algorithmus arbeitet sehr langsam

Asymmetrische Verschlüsselung (Ablauf)



Asymmetrische Verschlüsselung (Verschlüsselungsmethoden)

- RSA-Kryptosystem
  - Wurde 1977 von **R**ivest, **S**hamir und **A**dleman am MIT entwickelt
  - Erste asymmetrische Verschlüsselungsverfahren
  - Zur Verschlüsselung werden Primzahlen verwendet

Asymmetrische Verschlüsselung (Algorithmus-Beispiel)

- Erzeugung des öffentlichen und privaten Schlüssels
  - $p = 11$ und $q = 13$ für die beiden Primzahlen.
  - RSA-Modul ist $N = p \cdot q = 143$.
  - Die eulersche φ-Funktion nimmt damit den Wert $\varphi(N) = \varphi(143) = (p-1)(q-1) = 120$ an.
  - Die Zahl e muss zu 120 teilerfremd sein. Wir wählen $e = 23$. Damit bilden $e = 23$ und $N = 143$ den öffentlichen Schlüssel.
  - Es gilt: $e \cdot d + k \cdot \varphi(N) = 1 = ggT(e, \varphi(N))$ bzw. im konkreten Beispiel: $23 \cdot d + k \cdot 120 = 1 = ggT(23, 120)$ Die Gleichung wird mit Faktoren d = 47 und k = − 9 erweitert. d ist der private Schlüssel, während k nicht weiter benötigt wird.

Hybride Verschlüsselung

- Kombination der Asymmetrischen Verschlüsselung und Symmetrischen Verschlüsselung
- Die Nachricht wird symmetrisch mit einem zufällig generierten Session-Key verschlüsselt
- Der Session-Key, welcher für die Entschlüsselung benötigt wird, wird asymmetrisch verschlüsselt

- PGP - Pretty Good Privacy

Entschlüsselung

- Kryptoanalytiker
  - Marian Rejewski
  - Alan Turing
- Rainbow-Tables
  - Datenbank mit Hashwerten

Entschlüsselung (Kryptoanalytiker)

- Marian Rejewski
  - 16. August 1905 bis 13. Februar 1980
  - Polnischer Mathematiker und Kryptologe
  - Entschlüsselung der Schlüsselmaschine Enigma

- Alan Turing
  - 23. Juni 1912 bis 7. Juni 1954
  - Britischer Logiker, Mathematiker und Kryptoanalytiker
  - Grundlagen für die künstlicher Intelligenz

Entschlüsselung (Rainbow-Tables)

- Datenbank in unterschiedlichen Größen
- Größe von mehreren Terabyte je nach Anzahl der enthaltenden Zeichen
- Verwendung für verschieden Hashwerte (MD5, SHA1, LM Hashes, …)
- Schnelles finden der Hashwert und dazugehörigen Klartext

Anwendungsbeispiel

- Kleine Datenbank zum herausfinden von Windowskennwörtern
- Ophcrack – Opensource-Projekt
- http://sourceforge.net/projects/ophcrack/

Quellen

- http://lehrerfortbildung-bw.de/werkstatt/mo/m3/net/schluessel/l_asym.htm
- http://ls1-www.cs.uni-dortmund.de/~hildebra/Seminare/Presentations/sii/asymm.pdf
- http://www2-fs.informatik.uni-tuebingen.de/~reinhard/krypto/sommer/node1.html
- http://www.pohlig.de/Unterricht/Inf2002/Tag55/33.9_One_Time_Pad.htm
- http://www.simonhuwiler.ch/m101/index.php?to=moderne&kat=history
- https://wiki.koeln.ccc.de/index.php?title=Rainbowtables
- http://www-ivs.cs.uni-magdeburg.de/bs/lehre/wise0102/progb/vortraege/rosenow/rejewski.html
- http://www.turing.org.uk/turing/
- Bilder: http://commons.wikimedia.org/wiki/Hauptseite