Lucerne University of
Applied Sciences and Arts
HOCHSCHULE
LUZERN
Informatik

Information Security Fundamentals
02 Kryptologie 1
symmetrische Verfahren / Hashfunktionen

Ausbildung

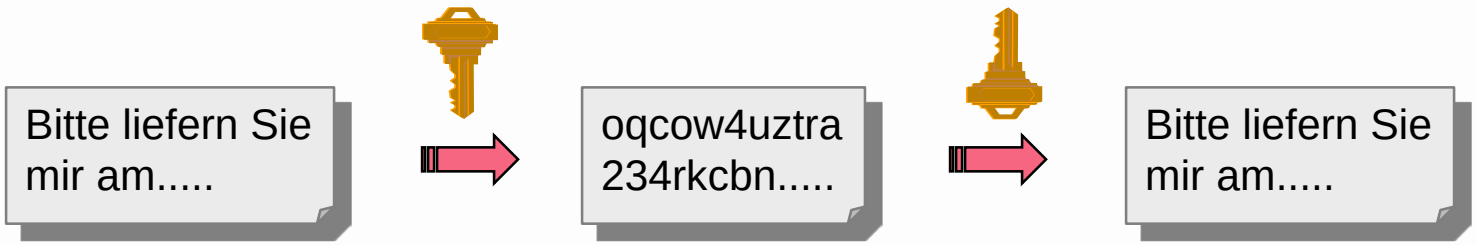
Prof. Konrad Marfurt
Studiengangleiter Wirtschaftsinformatik

T direkt +41 41 757 68 61
konrad.marfurt@hslu.ch

Rotkreuz 18.02.2017

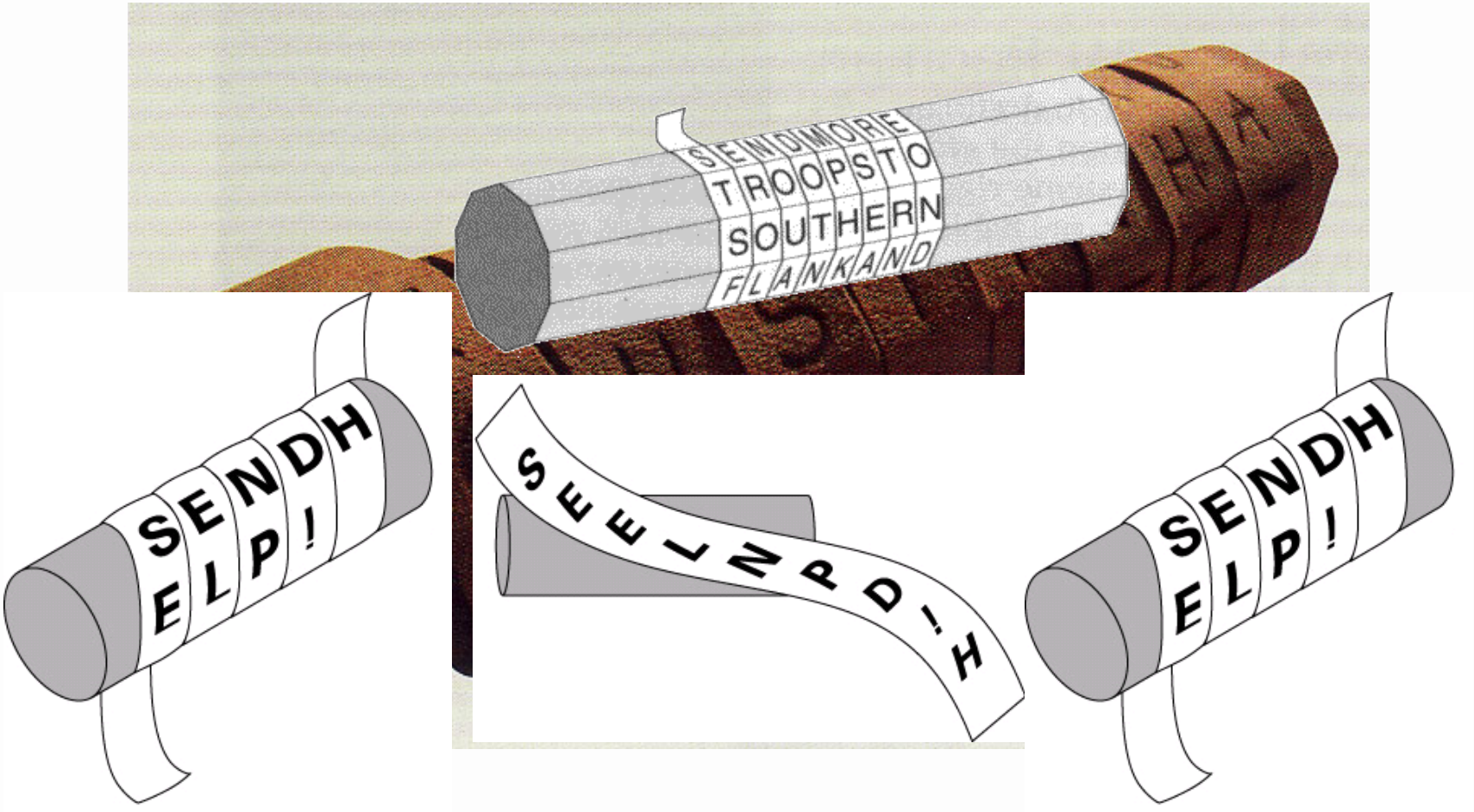
Kryptographie / **Verschlüsselung / Entschlüsselung**

- Wissenschaft von der Geheimhaltung von Informationen durch Verschlüsselung
- Umwandlung einer Nachricht (Klartext) mit Hilfe eines Verfahrens (Krypto-Algorithmus) und eines Geheimnisses (Schlüssel) in eine scheinbar sinnlose Zeichenfolge (Geheimtext), die mit Hilfe des Schlüssels und des Umkehrverfahrens wieder in den Klartext umwandelbar ist.



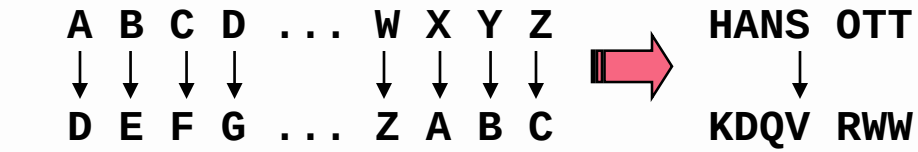
Skytale

- Älteste Methode
  - Spartaner im alten Griechenland

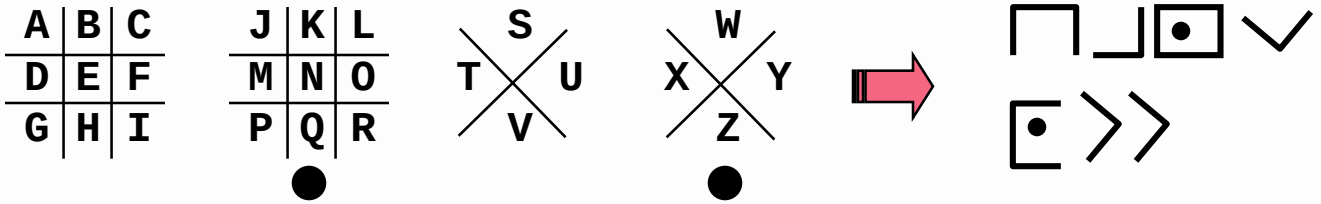


Zwei weitere Verschlüsselungsverfahren

Caesar-Chiffrierung:
Verschiebung der Zeichen im Alphabet



Freimaurer-Chiffre:
Abbildung von Zeichen in grafische Symbole



Fragen: Welches ist jeweils das Verfahren, was ist jeweils das Geheimnis, wie gross ist der „Schlüsselraum“?

Merke: Gleiches Geheimnis zum Ver- und Entschlüsseln

Monoalphabetische Substitution

Überlegungsfragen:

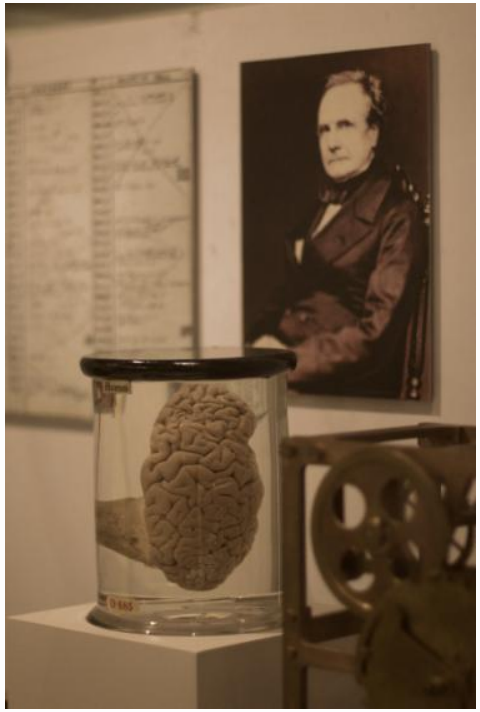
- Was ist die grundlegende Schwäche der vorangehenden Verfahren?
- Wie gehen Sie zur Entzifferung vor?
- Voraussetzungen für einen erfolgreichen Angriff

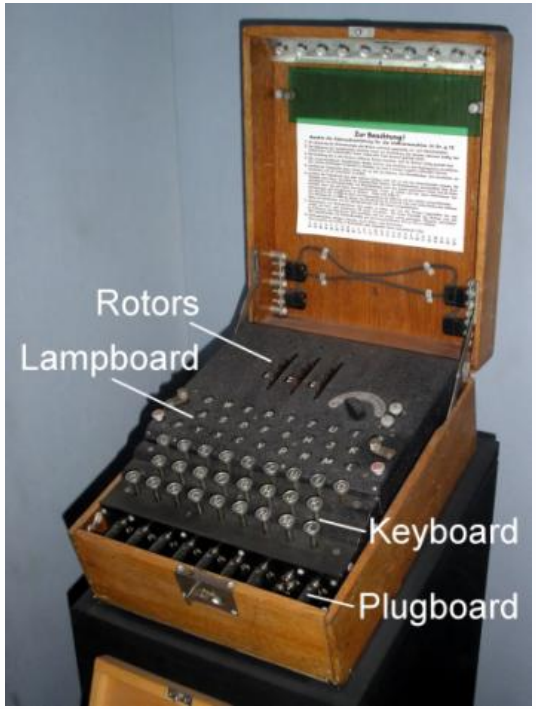
Fazit:

– Wenn das Verfahren bekannt ist, sind die Angriffe in den obigen Fällen nicht schwierig, weil die Anzahl möglicher «Geheimnisse» (Schlüssel) nicht sehr gross ist
– «Security by Obscurity» ist nicht immer ein gutes Konzept

Kerckhoffsches Prinzip:
Die Sicherheit eines Verschlüsselungsverfahrens soll auf der Geheimhaltung des Schlüssels und nicht auf der Geheimhaltung des Verschlüsselungsalgorithmus beruhen.

Polyalphabetische Substitution





Vigenère (1586)

Babbage (mitte 19. Jh)

Enigma (ab 1918)

Vernam Chiffre – One Time Pad

- Auch polyalphabetische Substitution ist nicht immun gegen Häufigkeitsanalysen
- Allerdings braucht es viel mehr Textvergleiche um einen Schlüssel zu ermitteln
- Wenn der Schlüssel wechselt, bevor viele Textvergleiche möglich sind, wird es schwierig
- Wenn Annahmen über den Klartext getroffen werden können, verringert sich der Aufwand (partially) known plaintext attack

Gilbert Vernam von AT&T

- er entwickelte 1917 eine sogenannte Stromchiffre, bei der ein beliebig langer nicht repetitiver Schlüssel auf einem Papierband mit dem Klartext kombiniert wird (einfachster Fall bitweises XOR)
- Jedes Band konnte nur einmal verwendet werden → **O**ne **T**ime **P**ad

Überlegungsfrage: Vor- und Nachteile dieses **Verfahrens**
Tipp: one-time pads sind *theoretisch* unknackbar!

Kryptoanalyse (auch Kryptanalyse)

Sie ist (natürlich) ebenso alt wie die Kryptographie
Kryptologie = Kryptographie + Kryptoanlyse

Sie umfasst das Studium von Methoden und Techniken, um Informationen aus verschlüsselten Texten zu gewinnen

→«Knacken des Codes»

- „Brechen“ = Entschlüsseln | Fälschen
  - vollständiges Brechen: finden des Schlüssels
  - universelles Brechen: finden eines äquivalenten Verfahrens

Arten der Kryptoanalyse

- Brute-Force
- Ciphertext-Only
- Known-Plaintext
- Chosen-Plaintext
- Chosen-Ciphertext

- Können Sie sich unter jeder Methode etwas vorstellen?
- Voraussetzungen / Randbedingungen (z.B. Häufigkeitsanalyse möglich?)

→ Im Lernschritt «Informationsdiebstahl» befassen wir uns mit konkreten Angriffen und Schlüsselstärken

Kryptographische Hashfunktionen

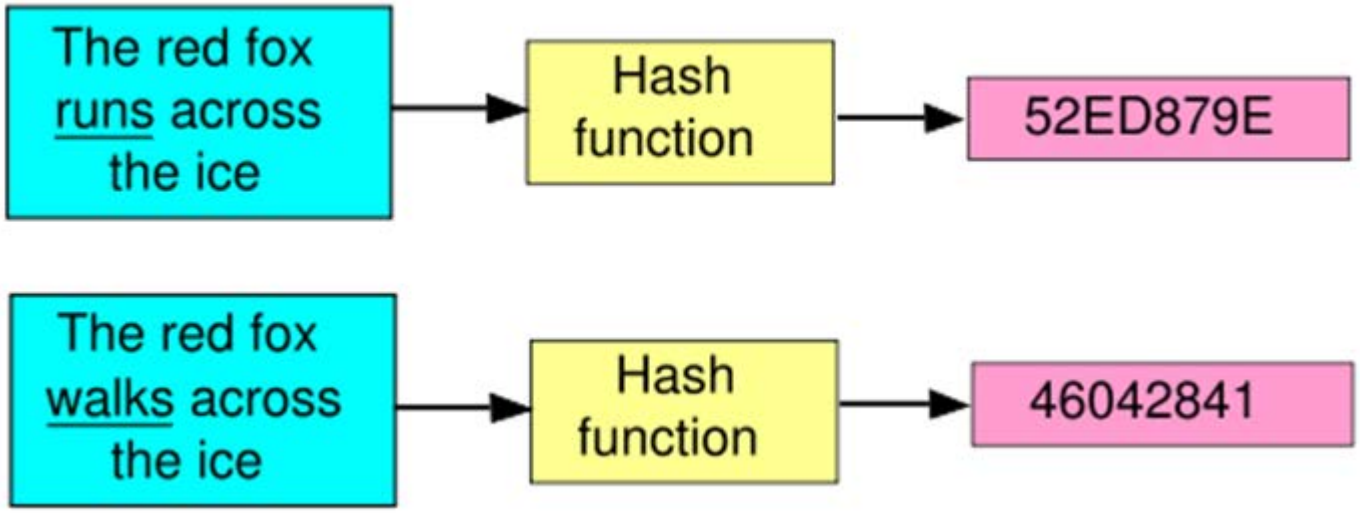
- Eine Hashfunktion berechnet aus beliebigen Binärdaten eine kondensierte Darstellung: Hashwert
- Vorstellungshilfe Fingerabdruck: wenig Information aber charakteristisch für eine (?) Person
- Dient z.B. als **M**essage **D**igest, also zur Charakterisierung einer Nachricht («alter Bekannter» MD5)
- Hashwerte basieren auf mathematischen Einwegfunktionen, die möglichst einfach zu berechnen sind, aber eine deutlich aufwändigere (oder gar keine) Umkehrung haben
  - Der Hashwert hängt von jedem Bit der Ausgangsdaten ab
  - Die Änderung eines Bits der Ausgangsdaten verändert viele (~50%) der Bits ihres Hashwertes (nicht voraussagbar)

- Sie werden häufig zum sicheren Speichern (nicht «verschlüsseln»!) von Passwörtern verwendet (→ Lernschritt Informationssicherheit)

Anforderungen an kryptographische Hashfunktionen

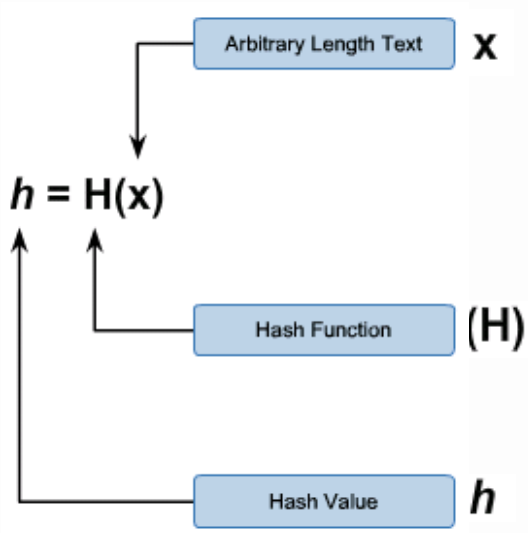
Es soll praktisch unmöglich sein,

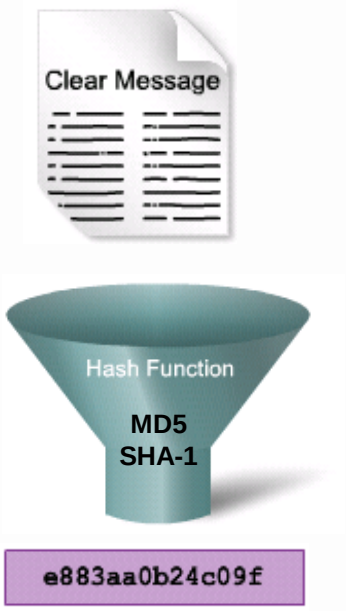
- zu einem gegebenen Hashwert h ein Dokument x mit H(x)=h zu finden (Einweg-Eigenschaft)
- zu einem Dokument d mit Hashwert h ein anderes Dokument x zu finden, so dass H(x) = h ist (schwache Kollisionsresistenz)
- zwei Dokumente x1 und x2 zu finden, welche den gleichen Hashwert liefern (starke Kollisionsresistenz)



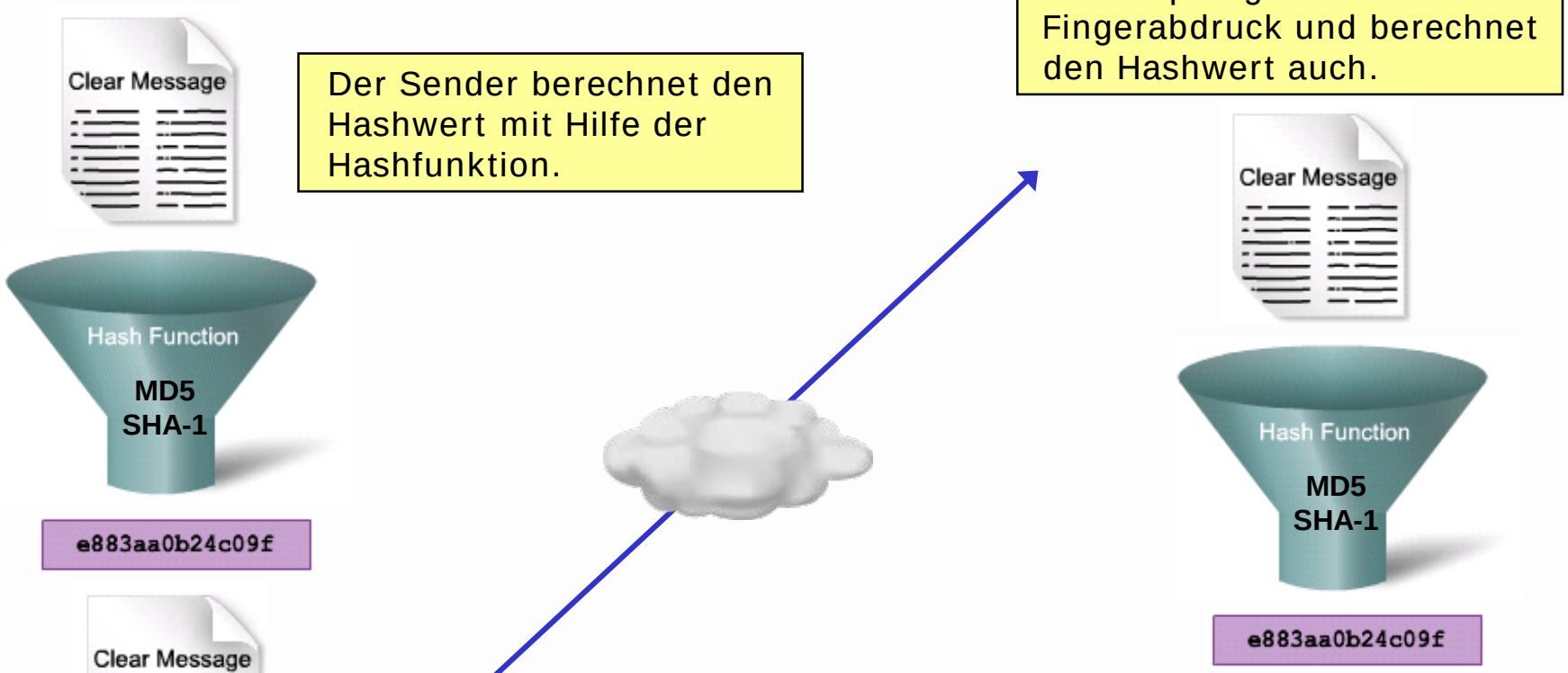
Hashwert graphisch illustriert

- Nachricht oder Datenpaket x bestimmen
- Hashfunktion H darauf anwenden
- «digest» fester Länge entsteht als h





Hashwert für Integrität



Der Sender berechnet den Hashwert mit Hilfe der Hashfunktion.

Dieser Fingerabdruck wird an die Nachricht geheftet und beides übermittelt.

Der Empfänger entfernt den Fingerabdruck und berechnet den Hashwert auch.

Wenn der berechnete und der übertragene Hashwert übereinstimmen, ist die Nachricht unversehrt.

Typische Verwendung von Hashes

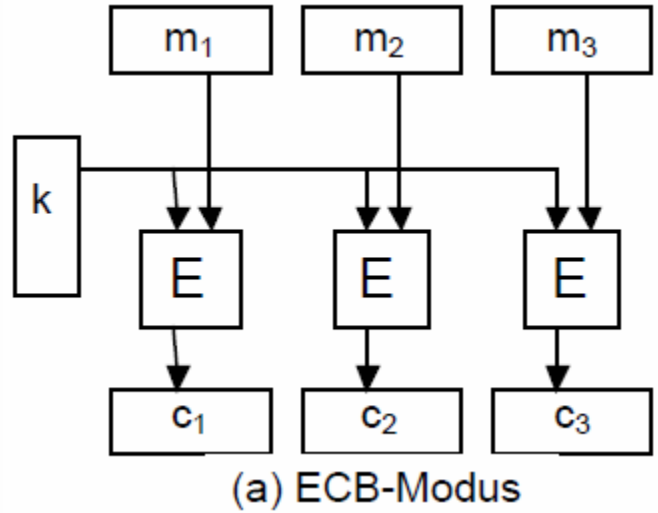
- Integrität einer Nachricht (z.B. eines Datenpakets bei IPSec) als sogenannte MACs (**M**essage **A**uthentication **C**odes)
- Beim Erzeugen von Einmalwerten für Authentisierungsprotokolle, damit nicht einfach ein Passwort übertragen wird (z.B. «digest» statt «basic» authentication beim Apache Webserver
- Zur Verifikation, dass eine heruntergeladene Datei unversehrt angekommen ist

- Einschränkungen:
  - Nur Integrität, nicht Vertraulichkeit geschützt
  - Anfällig für man-in-the-middle Angriffe
  - Die Authentizität ist nur gegeben, *wenn ein symmetrisches Geheimnis in die Bildung des Hashwertes einfliesst* (HMAC)
  - Die «Klassiker» SHA-1 und MD5 sind gelten heute nicht mehr als sicher!

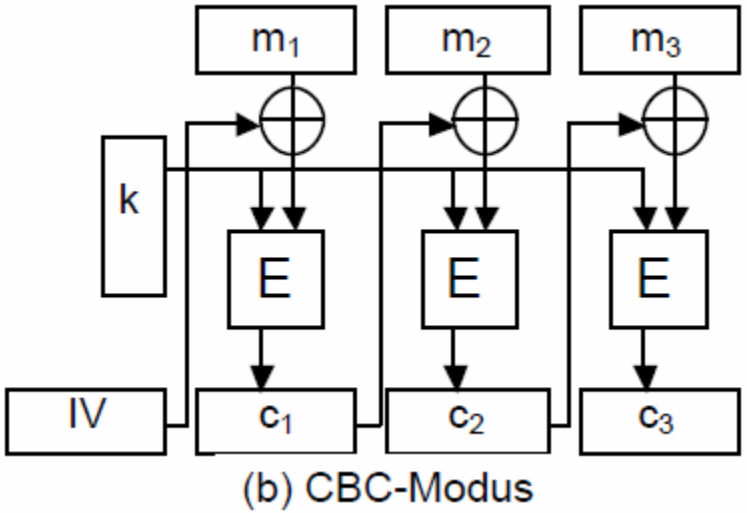
Blockchiffren

- Nachricht wird in Blöcke fixer Länge (zB 64 oder 128 Bit) aufgeteilt, bevor diese verschlüsselt werden
- Verschiedene Betriebsarten mit Vor- und Nachteilen

- Überlegungsfrage: wie wirken sich Übertragungsfehler zwischen Sender und Empfänger aus?



(a) ECB-Modus

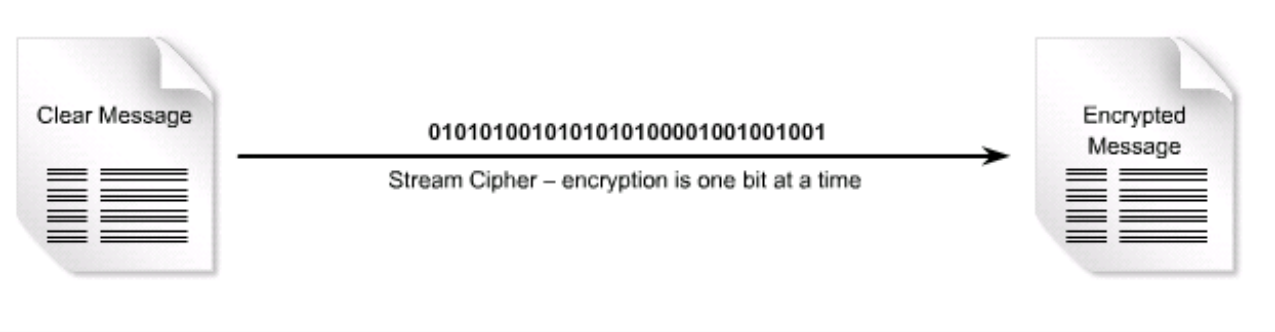


(b) CBC-Modus

Stromchiffren

- One-Time Pads (OTP) sind nicht knackbar, da der Schlüssel beliebig lang und nicht berechenbar ist, wenn er *wirklich* zufällig entsteht
- Ein Problem ist die Schlüsselmanagement: wie erhält der Empfänger den Schlüssel und wie bewahrt man den Schlüssel sicher auf?
- Das zweite Problem ist die Zufälligkeit. Wirkliche Zufälle gibt es bei einer algorithmischen Maschine nicht. Gute Zufalls- oder Primzahlen sind nicht einfach zu erzeugen, wie wir noch sehen

→Pseudozufallszahlen erzeugen mit einem «normalen» geheimen Schlüssel und mit einem «Initialisierungsvektor» für jeden neuen Strom



CrypTool 2 – Kryptologie für jedermann

- Open Source Projekt (ursprünglich aus Hochschul- und Finanzbereich) unter Apache-Lizenz
- Spannender Abenteuerspielplatz
- Selber erkunden, sich aber nicht verlieren
- Vorgefertigte Szenarien mit Toolbox erweiterbar
- www.cryptool.de

Viel Spass bei den Übungen!