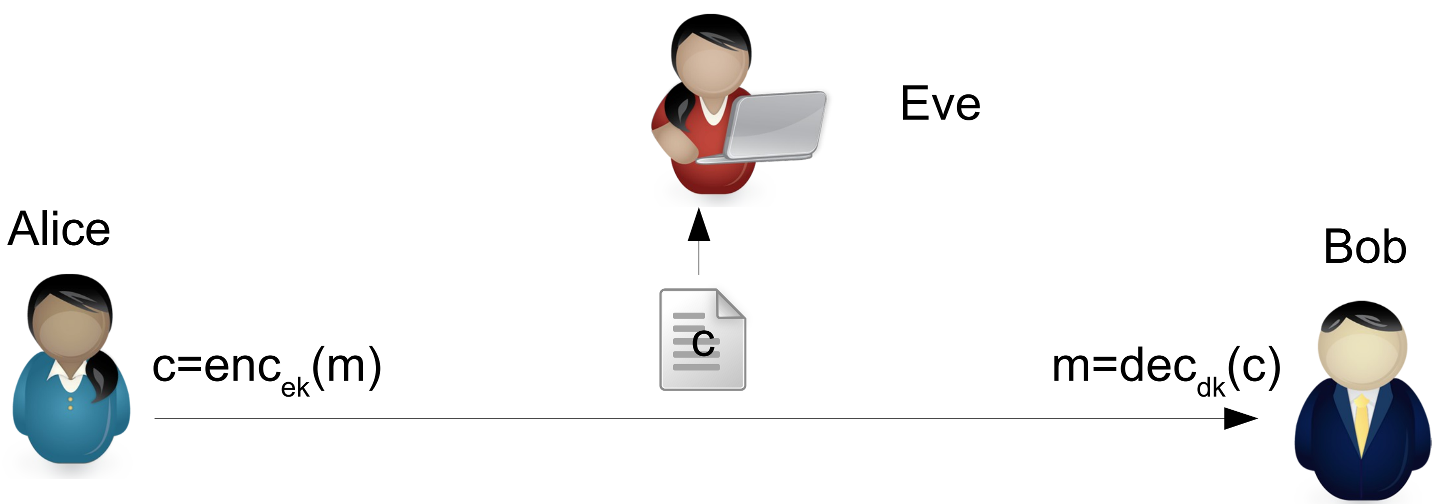
Themen zur Computersicherheit

Verschlüsselung

PD Dr. Reinhard Bündgen
buendgen@de.ibm.com

Kryptografisches System

- Alphabete $\Sigma_{1,}$ Σ_2
- Verschlüsselungsverfahren / Chiffre / englisch: cipher
  - enc: eK x $\Sigma_1^* \rightarrow \Sigma_2^*$, dec: dK x $\Sigma_2^* \rightarrow \Sigma_1^*$
  - Schlüssel (ek,dk) B eK x dK mit $dec_{dk}(enc_{ek}(m)) = m$ für alle m BΣ_1^*
  - verschlüsselt Klartext (plain text) zu Geheimtext (cipher text)



Angriffe auf ein Kryptografisches System

- Ziele eines Angriffs
  - finde Klartext zugegebenem Geheimtext
  - finde Schlüssel
- oft resultiert ein Angriff nur ein Teilziel
  - Eigenschaften des Geheimtextes
  - Eigenschaften des Schlüssels
- das allerdings von einem weiteren Angriff genutzt werden kann
- I.A braucht man zusätzliche Informationen über den Klartext oder Geheimtext um entscheiden zu können, ob ein Angriff erfolgreich war
- Seitenkanalangriffe
  - nutzen ein Informationsleck des Verschlüsselungsverfahrens
  - z.B Dauer der Berechnung, Strahlung, ...

Angriffsformen

- Art des Zusatzinformationsgewinns
  - Angriff mit bekanntem Geheimtext (cipher text only attack, COA)
    - Angreifer kennt einen oder mehrere Geheimtexte
  - Angriff mit bekanntem Klartext (known plaintext attack, KPA)
    - Angreifer kennt die zu einem oder mehreren Geheimtexten gehörigen Klartexte
  - Angriff mit gewähltem Klartext (chosen plain text attack, CPA)
    - Angreifer kann sich zu gewählten Klartexten die dazugehörigen Geheimtexte berechnen lassen
  - Angriff mit gewählten Geheimtext (chosen cipher text attack, CCA)
    - Angreifer kann sich zu gewählten Geheimtexten die dazugehörigen Klartexte berechnen lassen
- Zeitpunkt des Zusatzinformationsgewinns
  - direkter Angriff (offline, batch)
    - vor bekannt werden der Herausforderung
  - adaptiv (online, adaptive)
    - nach bekannt werden der Herausforderung

Orakel

- Angriffs-Orakel: Funktion die Verschlüsselungsaufgaben als „black box“ löst
  - COA-Orakel erzeugt zufälligen Geheimtext
  - KCA-Orakel erzeugt zufälligen Klartext mit zugehörigem Geheimtext
  - CPA-Orakel berechnet zugegebenem Klartext den Geheimtext
  - CCA-Orakel berechnet zu gegebenem Geheimtext den dazugehörigen Klartext
- IND-Orakel verschlüsselt zufällig einen von zwei gegebenen Klartexten und gibt den Gemeintext aus
- Orakel berechnet *nicht* die Lösung der Herausforderung

Ununterscheidbarkeit (indistinguishability)

Ununterscheidbarkeitstest:

- Angreifer befragt das Angriffs-Orakel
- Angreifer wählt 2 Nachrichten m_1, m_2
- IND-Orakel wählt ein mB{ m_1, m_2 }
- IND-Orakel gibt $c=enc_k(m)$ aus
- bei adaptivem Angriff befragt Angreifer das Angriffs-Orakel
- Angreifer gibt als Resultat seiner Angriffs b B { 1, 2 } aus

Der Test ist (im Sinne des Angreifers) bestanden, wenn $c = enc_k(m_b)$

Definition: Ein kryptografisches System ist gegen einen Angriff *sicher im Sinne der polynomiellen Ununterscheidbarkeit*, wenn der Angriff den Ununterscheidbarkeitstest nur mit einer Wahrscheinlichkeit von 0,5 besteht.

Definition: Ein kryptografisches System ist *perfekt sicher*, wenn es gegen beliebige Angriffe sicher im Sinne der polynomiellen Ununterscheidbarkeit ist.

Alternative Definition: Ein kryptografisches System ist *perfekt sicher*, wenn nach jedem Angriff, die a priori Wahrscheinlichkeit eines beliebigen Klartextes gleich der a posteriori Wahrscheinlichkeit des Klartextes ist.

One Time Pad

- **Definition** Das folgende Kryptosystem heißt *one time pad*:
  - Sei $\sum = \sum_1 = \sum_2 = \{0,1\}$, eK = dK = $\sum^*$,
  - m B $\sum^*$
  - k B $\sum^*$ ist ein Zufallsbitstring mit |k| = |m|
  - und $enc_k(m) = dec_k(m)$ = k џ m (џ bit-weises xor)
- **Satz** Das one time pad ist perfekt sicher, wenn jeder Schlüssel genau einmal zur Verschlüsselung einer Nachricht verwendet wird.
- **Achtung**: Ein Zufallsbitstring darf nur einmal als one time pad Schlüssel verwendet werden!
  - seien m_1, m_2, k B$\sum^*$, $|m_1| = |m_2| = |k|$, c_1=m_1 џ k, c_2 = m_2 џ k
  - dann ist c_1 џ c_2 = m_1 џ m_2
  - wenn m_2 bekannt: m_1 = c_1 џ c_2 џ m_2

Historische Chiffren I

- Caesar Chiffren

a	b	c	d	...	v	w	x	y	z
↓	↓	↓	↓		↓	↓	↓	↓	↓
d	e	f	g	...	y	z	a	b	c

- Verschiebechiffren
  - $\sum = \sum_1 = \sum_2 = \{ s_0, s_1, \ldots, s_{n-1} \}$, ek = dk B {0, …, n-1}
  - enc_k: $s_i \,||\, m$ ڕ $s_{(i+k) \bmod n} \,||\, enc_k(m)$ für s_i B∑, m B∑*
  - dec_k: $s_i \,||\, m$ ڕ $s_{(i-k) \bmod n} \,||\, dec_k(m)$ für s_i B∑, m B∑*
  - Schlüsselraum: n verschiedene Schlüssel
  - Angriff: vollständige Suche
- Monoalphabetische Chiffren
  - $\sum = \sum_1 = \sum_2 = \{ s_0, s_1, \ldots, s_{n-1} \}$
  - ek=dk B { π B ∑ → ∑ | π ist Permutation }
  - enc_π: s||m ڕ $\pi(s)||enc_\pi(m)$ für s B∑, m B∑*
  - dec_π: s||m ڕ $\pi^{-1}(s)||dec_\pi(m)$ für s B∑, m B∑*
  - Schlüsselraum: |∑|! verschiedene Schlüssel
  - Angriff: statistische Analyse

Historische Chiffren II

Polyalphabetische Chiffren

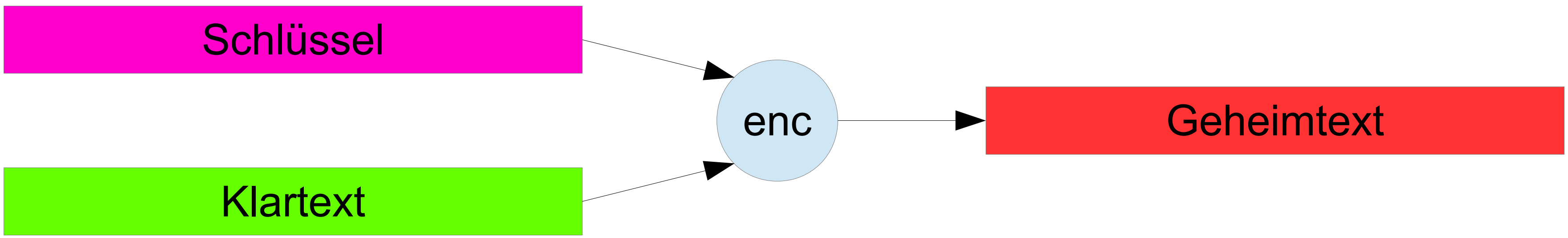
- Vigenère Chiffre (um 1500)
  - Sei $|\sum| = n$, ord: $\sum \rightarrow \{0,1,...,n-1\}$ bijektiv
  - $eK = dK = \sum^*$ mit $ek = dk = k$ B $\sum^*$ für alle Schlüssel
  - seien a, s B$\sum$ und k, m B $\sum^*$ dann ist
  - $enc_{a||k}(s||m) \quad = enc_{ord(a)}(s) \; || \; enc_{k||a}(m) = ord^{-1}((ord(s) + ord(a)) \bmod n) \; || \; enc_{k||a}(m)$
- Angriffe
  - Vigenère Chiffre galt lange Zeit als unentzifferbar
  - Bestimmung der Schlüssellänge (Kasiski)
    - gleiche Geheimtextstücke (die zu gleichen Klartextstücken gehören) haben einen Abstand, der ein vielfaches der Schlüssellänge beträgt
  - Bestimmung von sprachlicher Redundanz im Geheimtext (Friedman)
    - Friedmanscher Koinzidenzindex: Wahrscheinlichkeit dass zwei beliebig aus einem Text gewählte Buchstaben gleich sind (Ziehen ohne zurücklegen).
    - Für jede Sprache gibt es charakteristische Wahrscheinlichkeit, dass zwei aus einem Text gewählte Buchstaben gleich sind (folgt aus statistischer Buchstabenhäufigkeit)
    - Sei $|k|$ die gesuchte Schlüssellänge, f der sprachtypische Koinzidenzindex, g der Koinzidenzindex eines Zufallstextes (Gleichverteilung der Buchstaben), n die Länge des Textes, p die Anzahl der gezogenen Paare aus gleichen Buchstaben
    - theoretisch: $p = f \bullet n \bullet (n/|k| - 1) / 2 + g \bullet n \bullet (n - n/|k|) / 2$
    - $F = 2 \bullet p / (n \bullet (n-1))$ ist Approximation des Friedmanschen Koinzidenzindexes
    - => $|k| = (f - g) \bullet n / ((n-1) \bullet F – g \bullet n + f)$

Historische Chiffren III

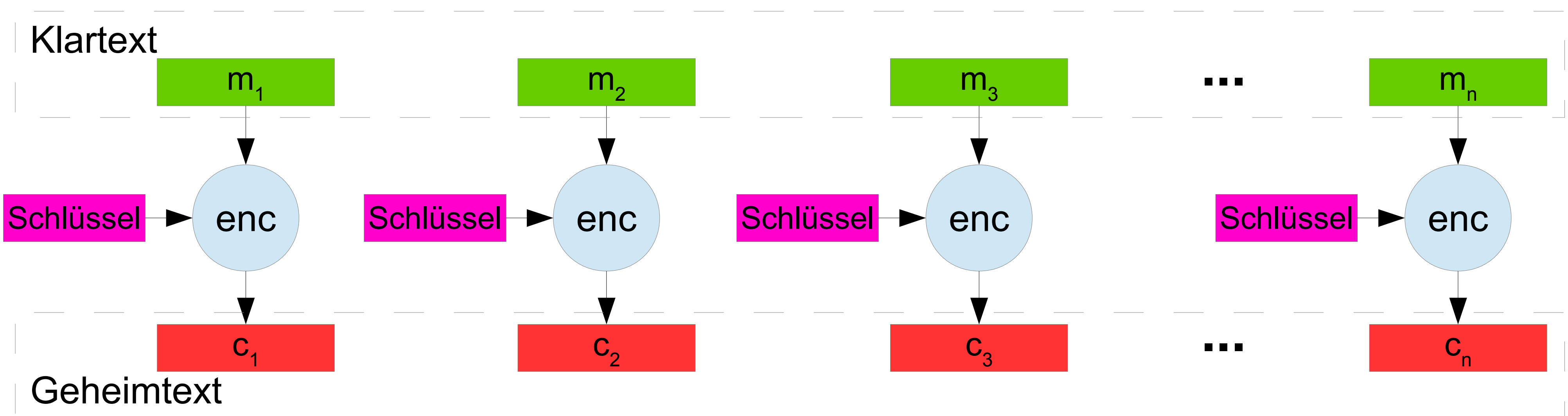
- die Enigma → getrennte Präsentation

Moderne Chiffren

- Stromchiffren
  - Verknüpfung eines Klartextes mit Schlüsselstrom
  - Verknüpfung: oft xor
  - Schlüssel: generiert mit Pseudozufallsgenerator (mit vereinbartem initialen Zustand)
  - Klartext kann beliebige Länge haben



- Blockchiffren
  - Verschlüsselung von Nachrichtenblöcken mit Hilfe eines konstanten Schlüssels
  - monoalphabetische Verschlüsselung auf großem Alphabet
  - Klartextlänge muss Vielfaches der Blocklänge sein



Symmetrische und asymmetrische Chiffren

- **Symmetrische Chiffren**
  - eK=dK (= K) und für alle Schlüssel (ek,dk) B eK x dK gilt ek = dk (=k)

- **Asymmetrische Chiffren**
  - für alle Schlüssel (ek,dk) B eK x dK gilt
    - ek ≠ dk und
    - dk kann nicht effizient aus ek berechnet werden
  - ek heißt auch öffentlicher Schlüssel (public key pk)
  - dk heißt auch privater Schlüssel (private/secret key sk)