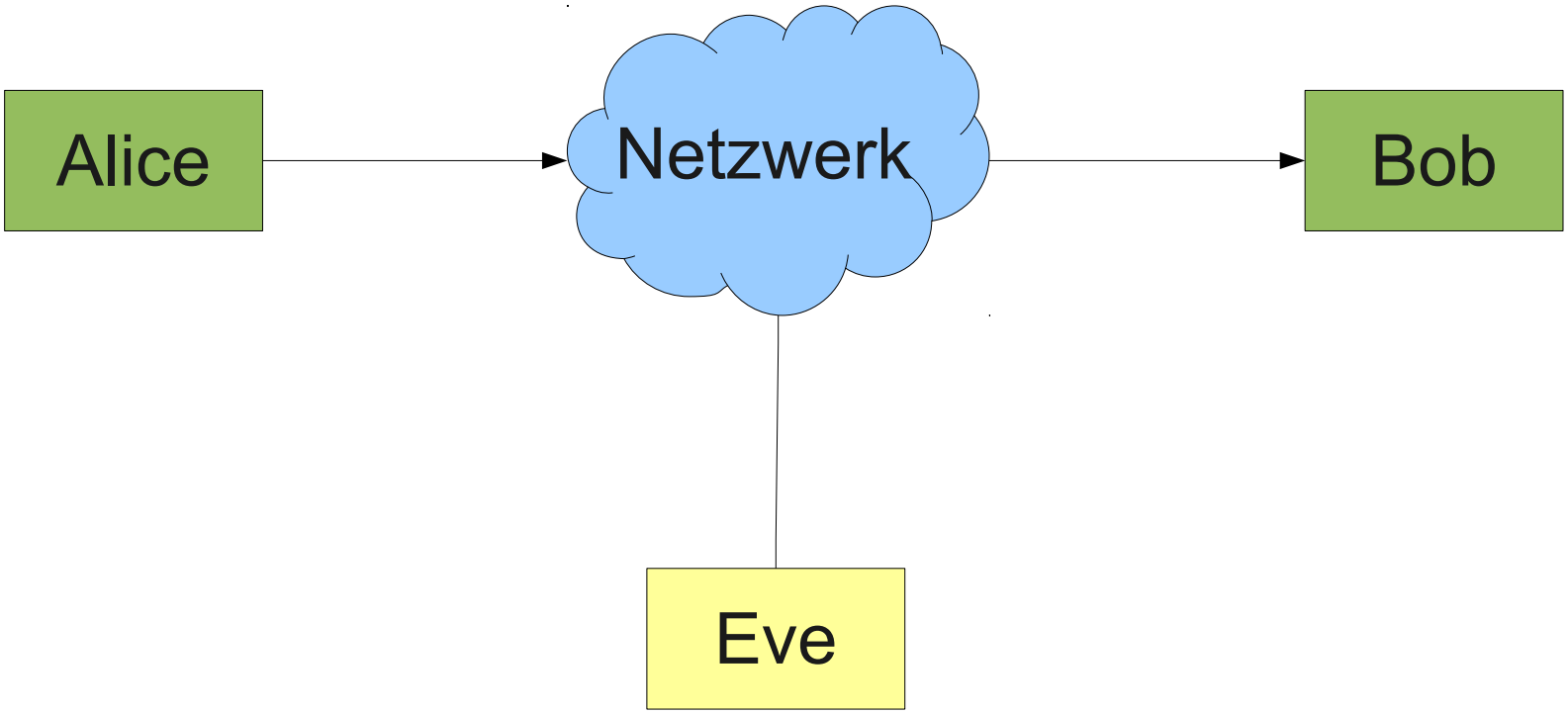
Grundlagen der Verschlüsselung und Authentifizierung (1)

Michael Fiedler
<michael.fiedler@informatik.stud.uni-erlangen.de>

Proseminar Konzepte von Betriebssystemkomponenten im SS 2010
Friedrich-Alexander-Universität Erlangen-Nürnberg

18.05.2010

Motivation



Kryptologie

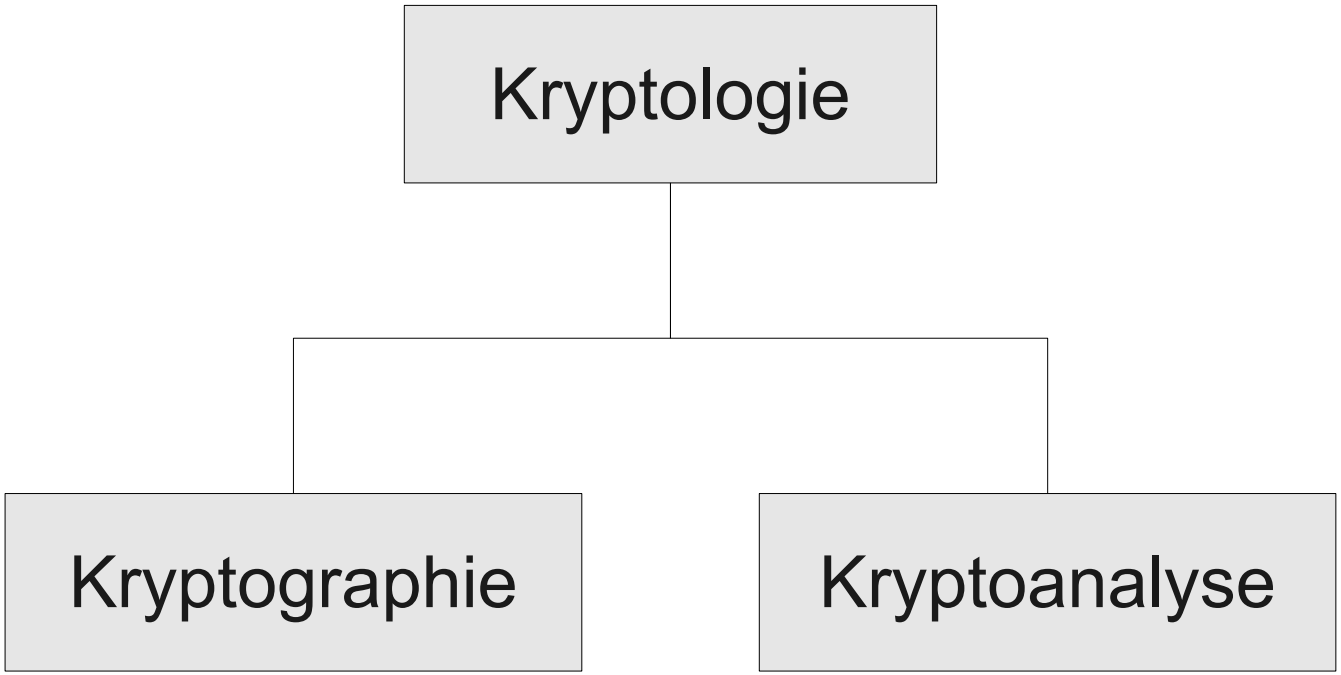


Abbildung: Kryptographie und Kryptoanalyse als Teilgebiete der Kryptologie

Verschlüsselungsverfahren bzw. Kryptosystem

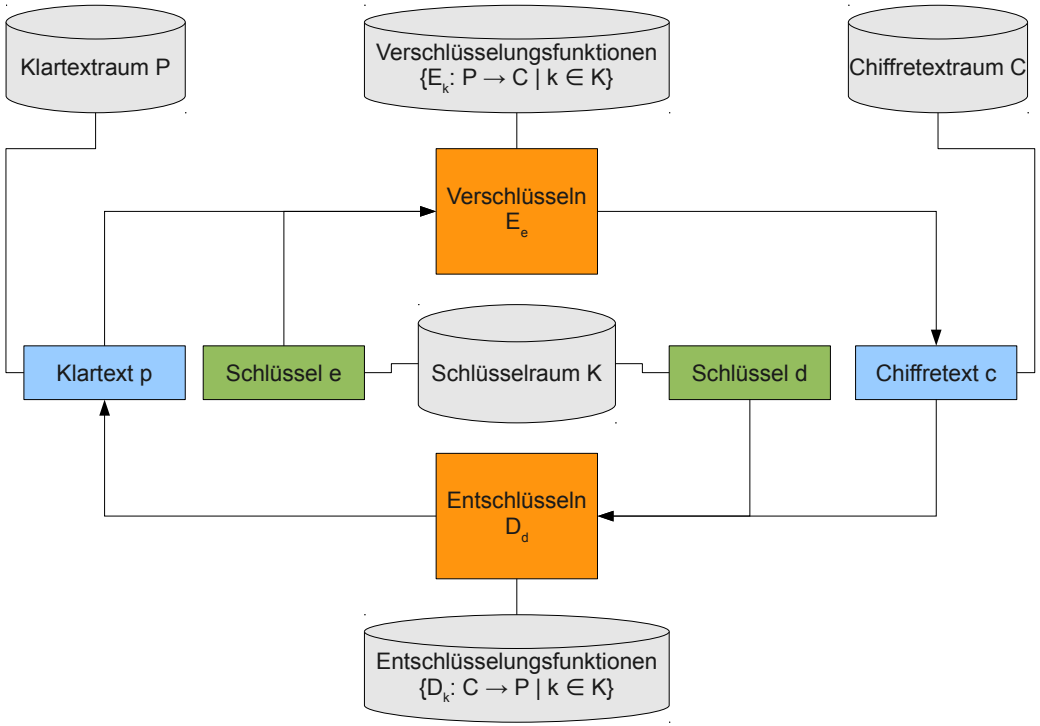
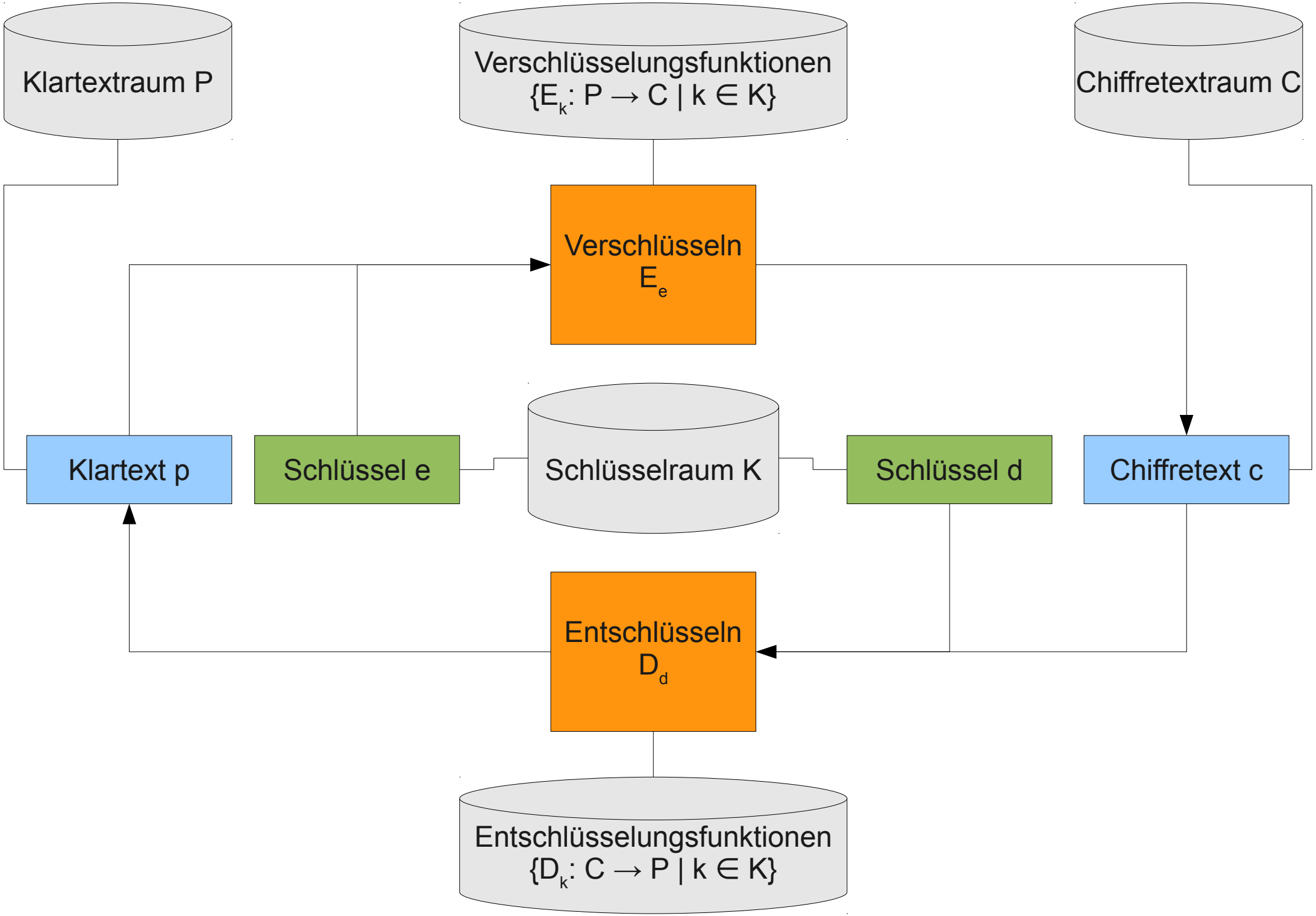


Abbildung: Kryptosystem als Fünftupel $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, wobei $\forall e \in \mathcal{K} \exists d \in \mathcal{K} : \forall p \in \mathcal{P} : D_d(E_e(p)) = p$; angelehnt an [2]


Klartextraum P
Verschlüsselungsfunktionen
$\{E_k: P \rightarrow C \mid k \in K\}$
Chiffretextraum C
Verschlüsseln
E_e
Klartext p
Schlüssel e
Schlüsselraum K
Schlüssel d
Chiffretext c
Entschlüsseln
D_d
Entschlüsselungsfunktionen
$\{D_k: C \rightarrow P \mid k \in K\}$

Kategorisierung kryptographischer Algorithmen

	Anzahl Schlüssel[1]
symmetrisches Verfahren	1
asymmetrisches Verfahren	2
Hashfunktion	0

[1] für Ver-/Entschlüsselung bzw. Signatur/Überprüfung

Angriffsmethoden

Klassifikation nach Kenntnissen des Angreifers

- nur Chiffretext
- Chiffretext-Klartext-Paare
- gewählte Schlüsseltexte

Klassifikation nach Fähigkeiten des Angreifers

- aktiv
- passiv

Grundsätzliches Schema

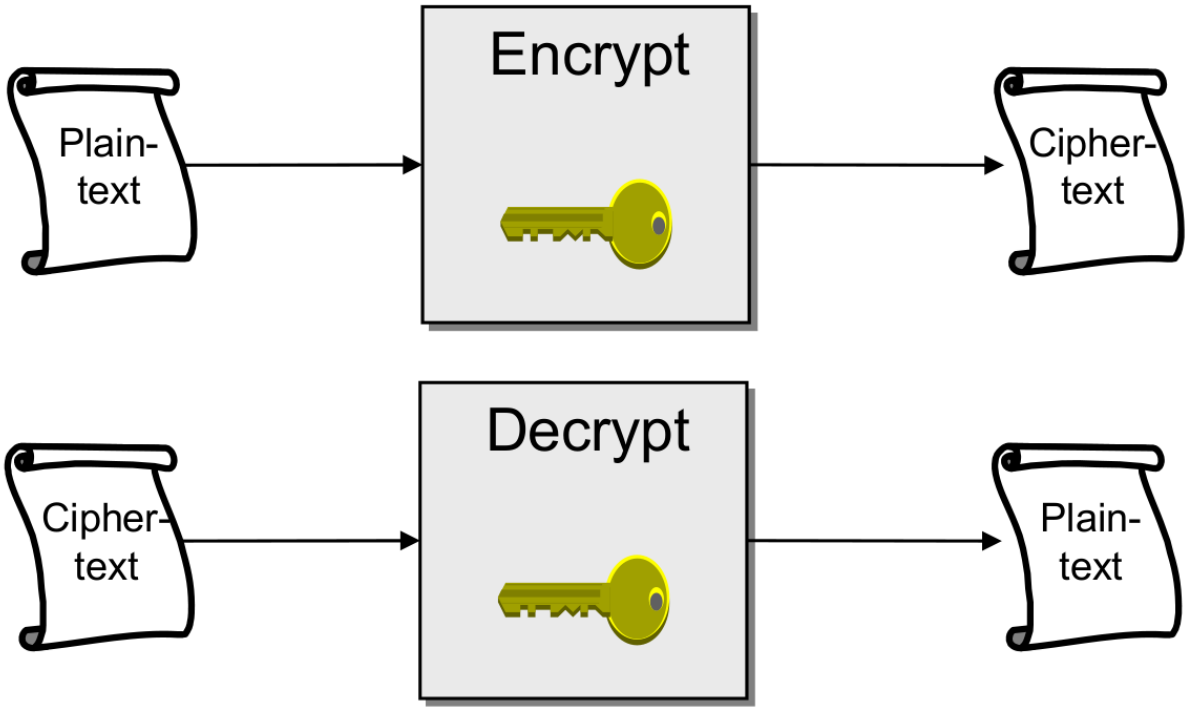


Abbildung: symmetrische Verschlüsselung; Ver-/Entschlüsselung mit demselben Schlüssel; Quelle: [3]

Chiffren

- **Blockchiffre**: Abbildung von Wörtern fester Länge ($\longrightarrow$ Blöcke) eines Alphabets auf Wörter derselben Länge und desselben Alphabets
- **Stromchiffre**: zeichenweise Abbildung

electronic code book mode (ECB)

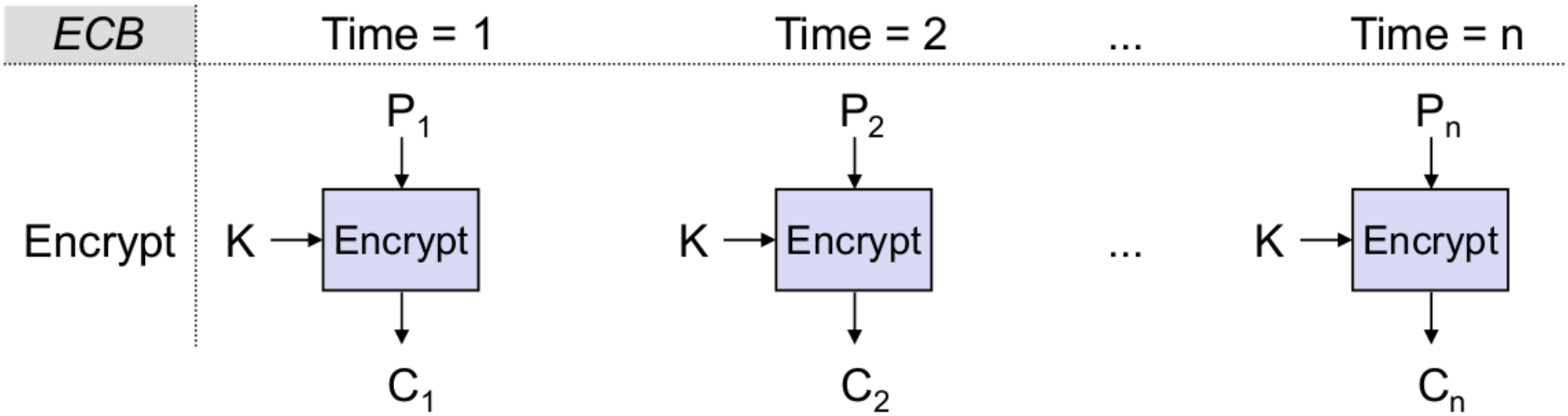


Abbildung: *electronic code book mode* (ECB); K: Schlüssel; P_i: Klartextblöcke; C_i: Chiffretextblöcke; Quelle: [3]

cipher block chaining mode (CBC)

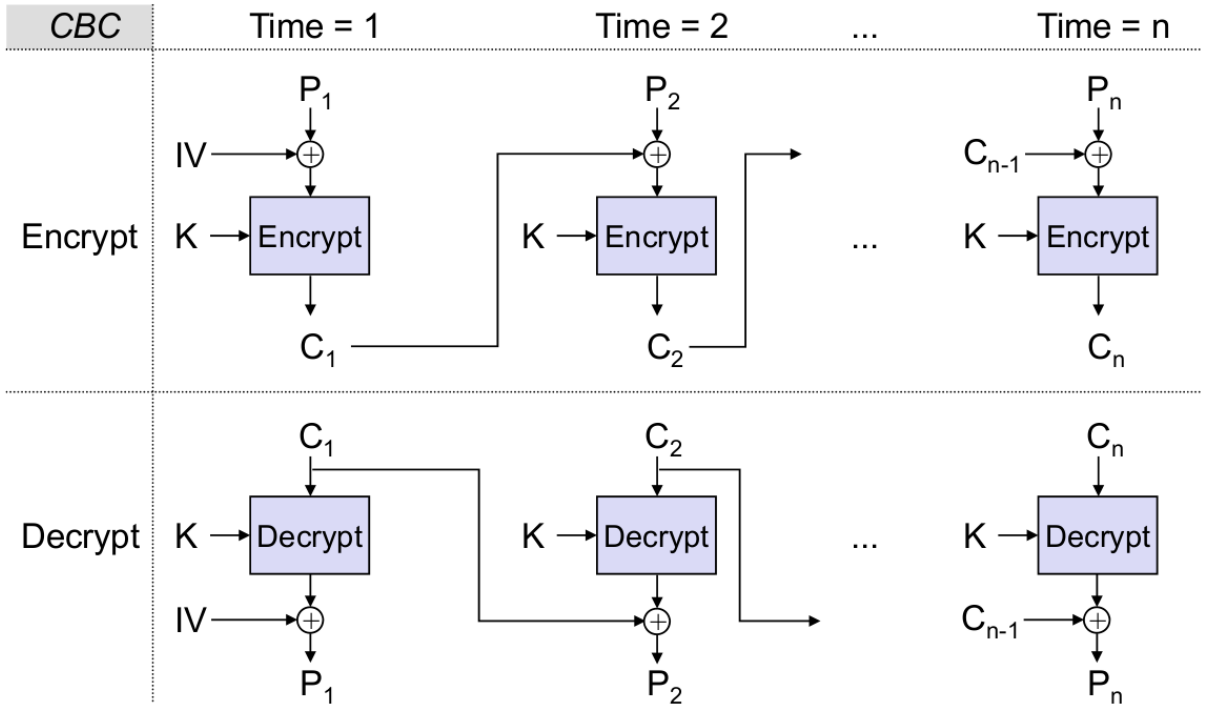


Abbildung: *cipher block chaining mode* (CBC); K: Schlüssel; P_i: Klartextblöcke; C_i: Chiffretextblöcke; IV: Initialwert für C_0; Quelle: [3]

ciphertext feedback mode (CFB)

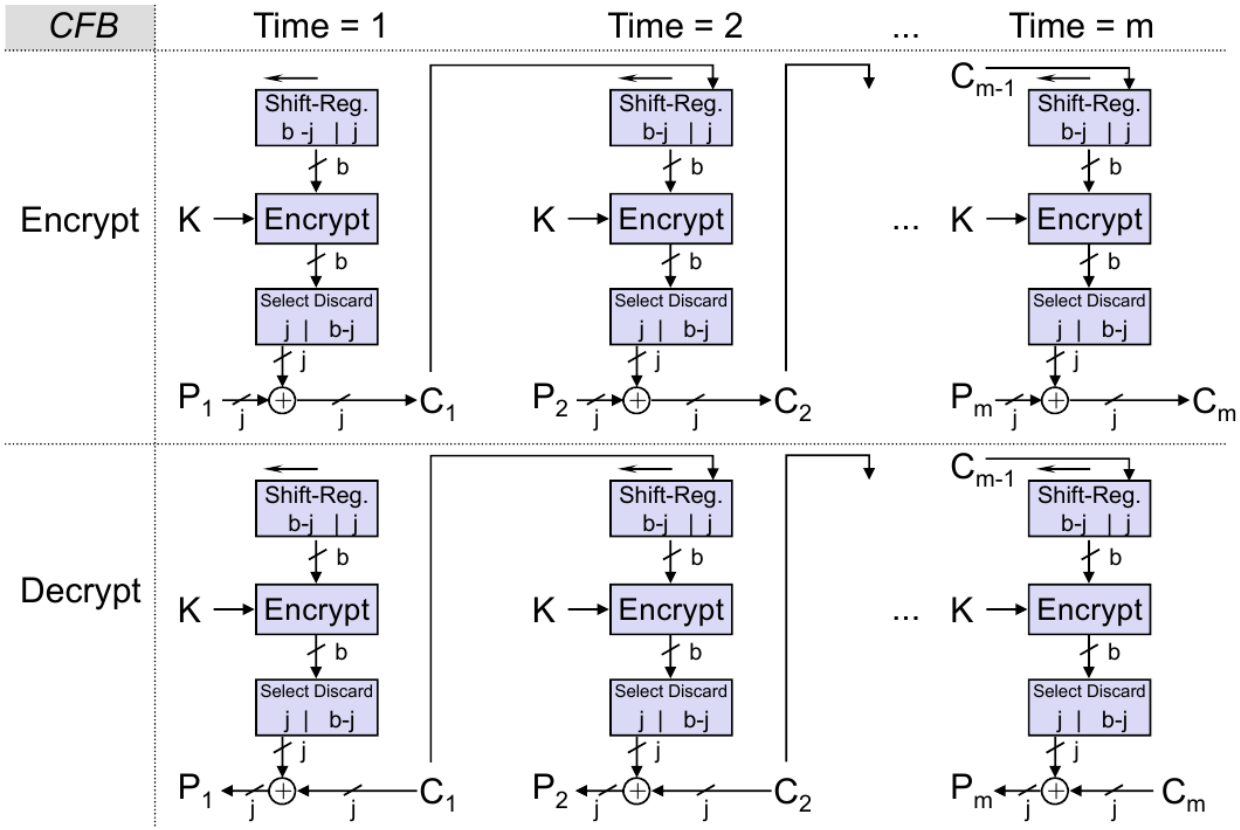


Abbildung: *ciphertext feedback mode*; Quelle: [3]

Beispiele

- *data encryption standard* (DES)
- *triple data encryption standard* (triple-DES, 3DES, TDES)
- *advanced encryption standard* (AES), „Nachfolger“ von DES
- *international data encryption algorithm* (IDEA)
- ⋮

DES – Allgemeines

- Ende der 1970er: in USA zum Standard erhoben
- im Folgezeitraum Verbreitung

DES – Funktionsweise

- DES ist sog. Feistelchiffre (eine Blockchiffre) mit Alphabet $\{0, 1\}$ und Blocklänge 64
- 1 Bit pro Byte als Prüfbit (ungerade Parität) $\Rightarrow$ 56 Bit des Schlüssels frei wählbar
- Anzahl verschiedener Schlüssel: $2^{56} \approx 7,2 \cdot 10^{16}$
- Verschlüsselung eines Klartextwortes
  1. initiale Permutationen
  2. interne Blockchiffre
  3. S-Boxen (spezielle Funktionen)
- Entschlüsselung: Anwendung von DES mit umgekehrter Schlüsselfolge

DES – Sicherheit

- Schlüssellänge: 56 Bit (64 Bit incl. Paritätsbits)
- Anzahl schwacher Schlüssel: 64 von $7,2 \cdot 10^{16}$
- Angreifbarkeit durch verschiedene Verfahren, aber: Durchprobieren erfolgversprechender
- bei $10^6 \frac{\text{Verschlüsselungen}}{\mu s}$: 56-Bit-Schlüssel in ca. $10h$ auffindbar
- Erhöhung der Schlüssellänge durch mehrfache Anwendung ($\rightarrow$ 3DES)

Authentifizierung

- Nachweis von
  - Identität
  - Authentizität
- Unterteilung in
  - Teilnehmerauthentifizierung
  - Nachrichtenauthentifizierung

Teilnehmerauthentifizierung

Wodurch zeichnet sich ein Teilnehmer eindeutig aus?

- biologische Eigenschaften
- Besitz eines einzigartigen Objekts
- einzigartiges Wissen = Geheimnis

Nachrichtenauthentifizierung

- Was macht Dokumente authentisch?
  - Unterschrift
  - Echtheitsmerkmale

  $\longrightarrow$ charakteristische Information oder Fähigkeit des Erstellers
- „Geheimnis“ + „Dokument“ $\Rightarrow$ Authentizität
- Signaturverfahren

Kryptographische Protokolle

Kriterien für sinnvollen Einsatz:

- **Durchführbarkeit**: keine Abweichung von Spezifikation
  $\Rightarrow$ gewünschtes Ergebnis
- **Korrektheit**: Erkennen von Betrug

Passwortverfahren (Festcodes)

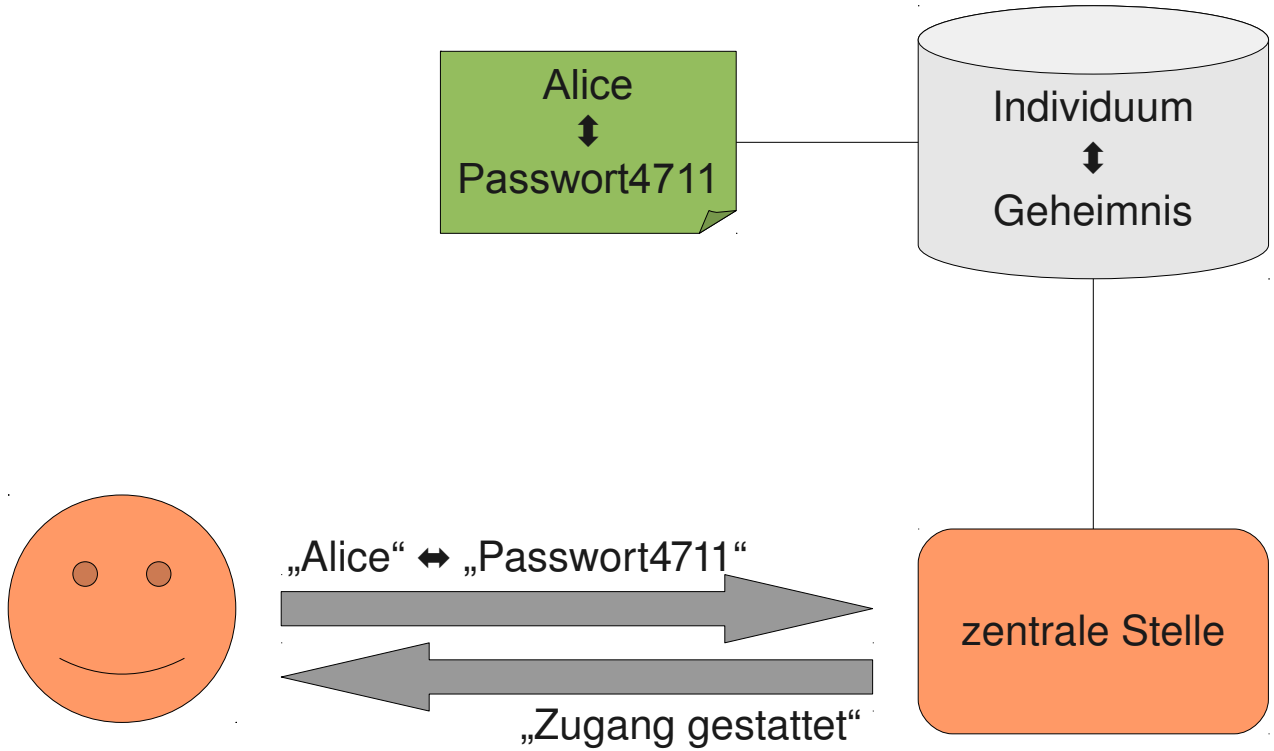


Abbildung: Passwortverfahren; nach [1]

Wechselcodeverfahren

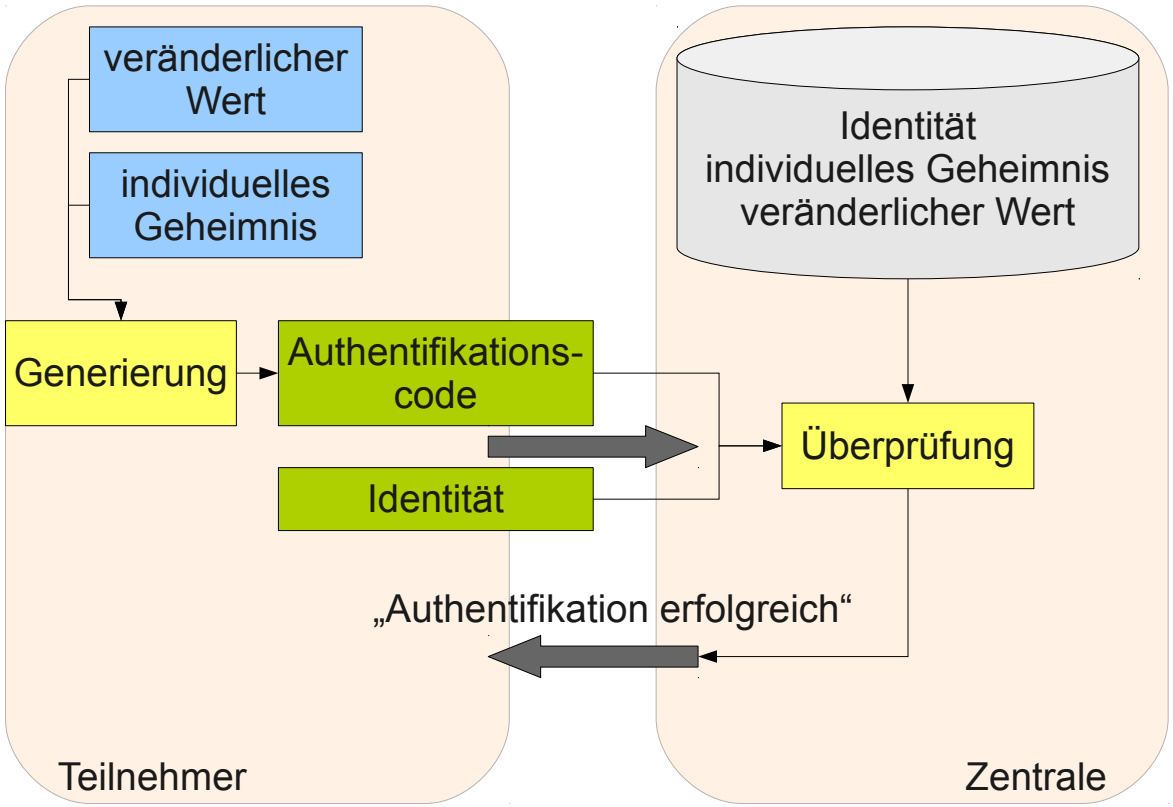


Abbildung: Wechselcodeverfahren; nach [1]

challenge and response

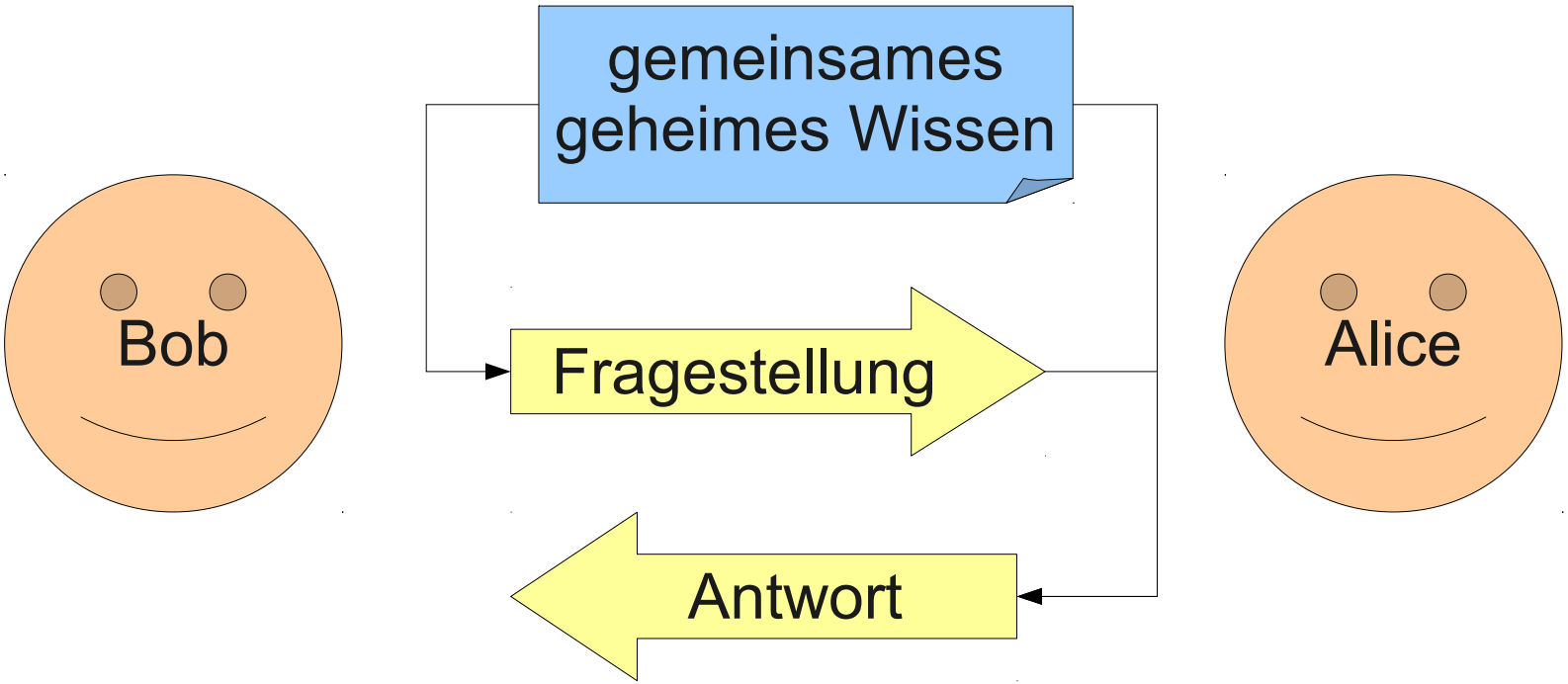


Abbildung: *challenge-and-response*-Verfahren; nach [1]

challenge and response: Beispiel POP3

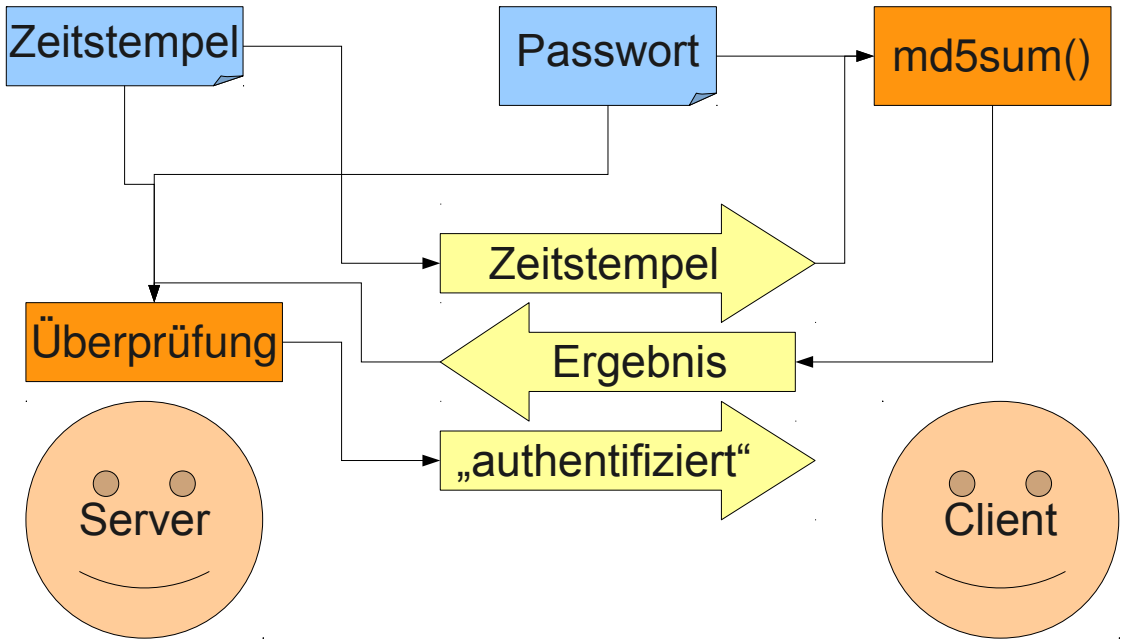


Abbildung: Authentifizierungsmöglichkeit bei POP3, siehe RFC 1460 (`http://tools.ietf.org/html/rfc1460`)

Zusammenfassung

- symmetrische Verschlüsselung
  - Blockchiffren (ECB, CBC, ...)
  - Stromchiffren (CFB, ...)
- Beispiel DES
- Authentifizierung
  - Passwortverfahren
  - Wechselcodeverfahren
  - *challenge and response*

Fragen?

Quellen


A. Beutelspacher, J. Schwenk, and K.-D. Wolfenstetter.
Moderne Verfahren der Kryptographie.
Vieweg, Brauschweig/Wiesbaden, 2nd, revised edition, 1998.


J. Buchmann.
Einführung in die Kryptographie.
Springer, Berlin/Heidelberg, 4th, extended edition, 2008.


F. Dressler and J. Kleinöder.
Vorlesungen Netzwerksicherheit/Systemsicherheit.
Website zur Vorlesung, WS 2007/08.