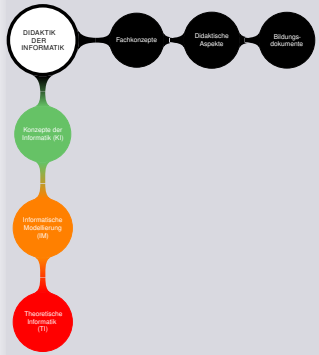


Seminar 9

Phänomenorientierte Kryptologie

Informatikfachdidaktik

Brigitte Zedler

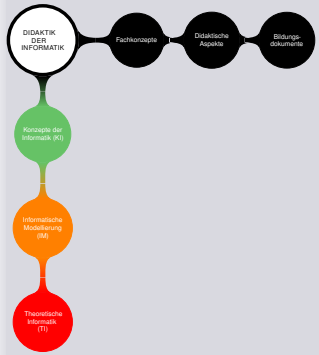
Seminar Didaktik der Informatik vom 4. Januar 2016

Version: b12c058
Stand: 2016-02-01 13:16
Bearbeitet von: zedler

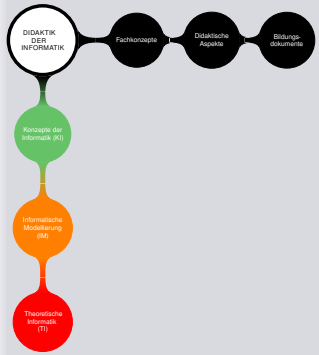
Fachgebiet Didaktik der Informatik
Bergische Universität Wuppertal

Kompetenzen – Seminar 9

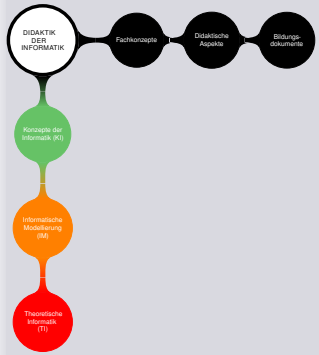
1. Einen Überblick über die Kryptologie schaffen
2. Lesen von Stereogrammen
3. Strukturiertes Feedback geben



Gliederung – Seminar 9



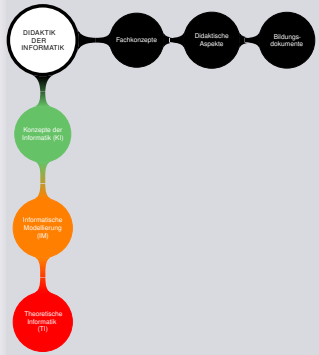
Spioncamp



ASCII - Codierung

Codierung

Die Buchstaben bleiben ***wo*** sie sind, aber nicht ***was*** sie sind. (Aber jeder kann nachschlagen, was sie bedeuten!) Man nennt so etwas einen *Code*. Mit einem Code soll nichts geheim gehalten werden.

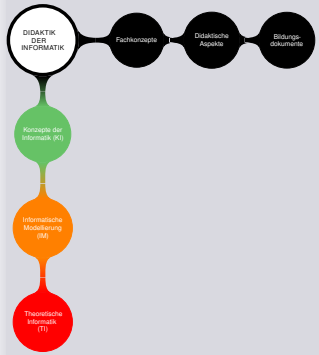


ASCII - Codierung

Codierung

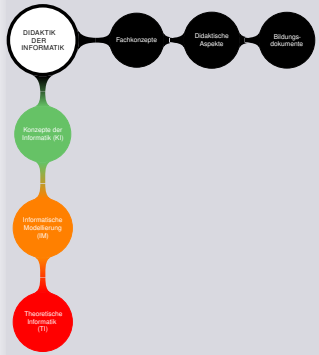
Die Buchstaben bleiben ***wo*** sie sind, aber nicht ***was*** sie sind. (Aber jeder kann nachschlagen, was sie bedeuten!) Man nennt so etwas einen *Code*. Mit einem Code soll nichts geheim gehalten werden.

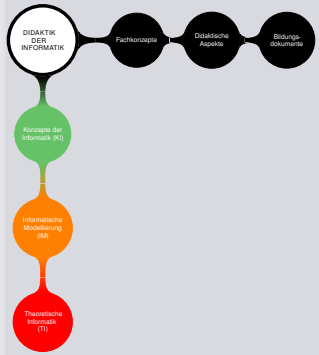
- Maschinenlesbare Codierung
- Thema Coderaum
- Hammingdistanz? Informationsgehalt?
- Problem: Codelänge



Steganographie

Die Buchstaben bleiben ***was*** sie sind, aber man erkennt nicht, ***wo*** die Nachricht ist. Das ist eigentlich gar keine Verschlüsselung, man nennt das *Steganographie*. (Das Wort Steganographie ist abgeleitet von den griechischen Wörtern *steganos* = bedeckt und *graphein* = schreiben.)





Steganographie

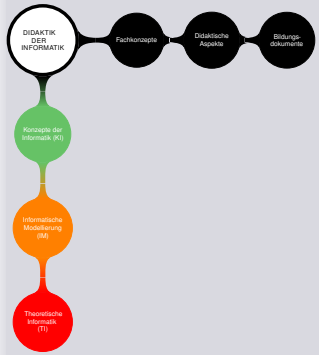
Die Buchstaben bleiben ***was*** sie sind, aber man erkennt nicht, ***wo*** die Nachricht ist. Das ist eigentlich gar keine Verschlüsselung, man nennt das *Steganographie*. (Das Wort Steganographie ist abgeleitet von den griechischen Wörtern *steganos* = bedeckt und *graphein* = schreiben.)

- Im alten Rom trugen Sklaven Nachrichten unter den Haaren verborgen
- Verborgene Nachrichten in Zeitungsartikeln oder Büchern
- Codierte Nachrichten in unauffälligen Zeichnungen
- Stereogramme
- Nachrichten in Metadaten von Bildern
- Schadsoftware in Bildern

Steganographie

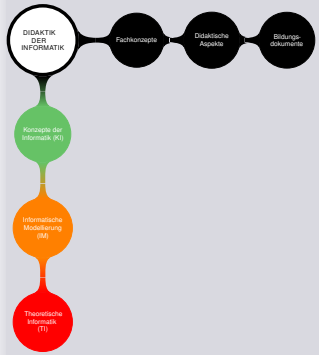
Fragen

- Relevanz für aktuelle Informatik?
- wichtige Aspekte (übersehen)?
- Bearbeitungsdauer der Station zu Stereogrammen?



Secret Sharing

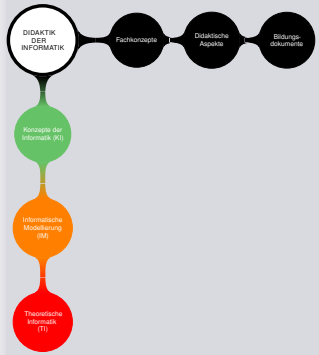
Die Nachricht wird durch ***Zerlegen*** unkenntlich gemacht. Erst das ***Zusammensetzen*** macht sie wieder lesbar.
Diese Art der Verschlüsselung heißt *Secret Sharing*.



Secret Sharing

Die Nachricht wird durch ***Zerlegen*** unkenntlich gemacht. Erst das ***Zusammensetzen*** macht sie wieder lesbar.
Diese Art der Verschlüsselung heißt *Secret Sharing*.

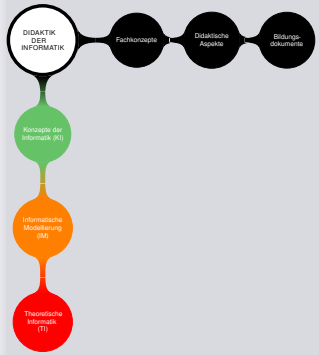
- Beispiel Schatzkarte
- Verschlüsselung: Teilen in zwei
- One-Time-Pad
- Alleinstellungsmerkmal: Teilen in n
- Graustufen und Farben
- Anwendung beim Onlinebanking



Visuelle Kryptographie

Fragen

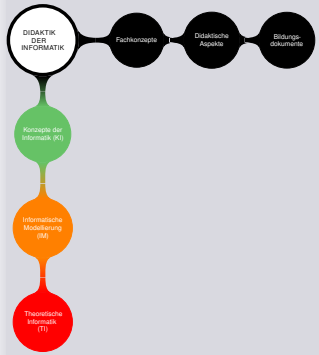
- Zentraler Aspekt?
- Tauglichkeit der Beispiele?
- Weiteres Beispiel mit Graustufen und höherer Auflösung?



Visuelle Kryptographie

Fragen

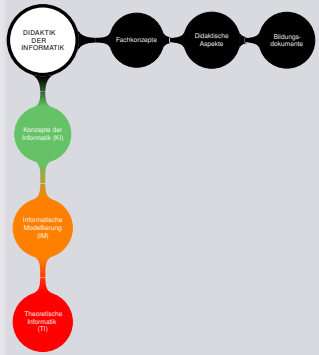
- Zentraler Aspekt?
- Tauglichkeit der Beispiele?
- Weiteres Beispiel mit Graustufen und höherer Auflösung?
- Secret Sharing als Oberbegriff?
- Weitere Beispiele für Secret Sharing? Diffie Hellmann?



Ausblick

Ausstehende Stationen

- Modulare Arithmetik an Zahnrädern
- Bitoperation XOR
- RSA
- DES
- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung
- Hybride Verschlüsselung
- Digitale Signaturen



Literatur für das Seminar I