

**Seminar “Kryptographische
Protokolle”—Tipps zum Halten eines
Vortrags**

Barbara König

Warum halte ich einen Vortrag?

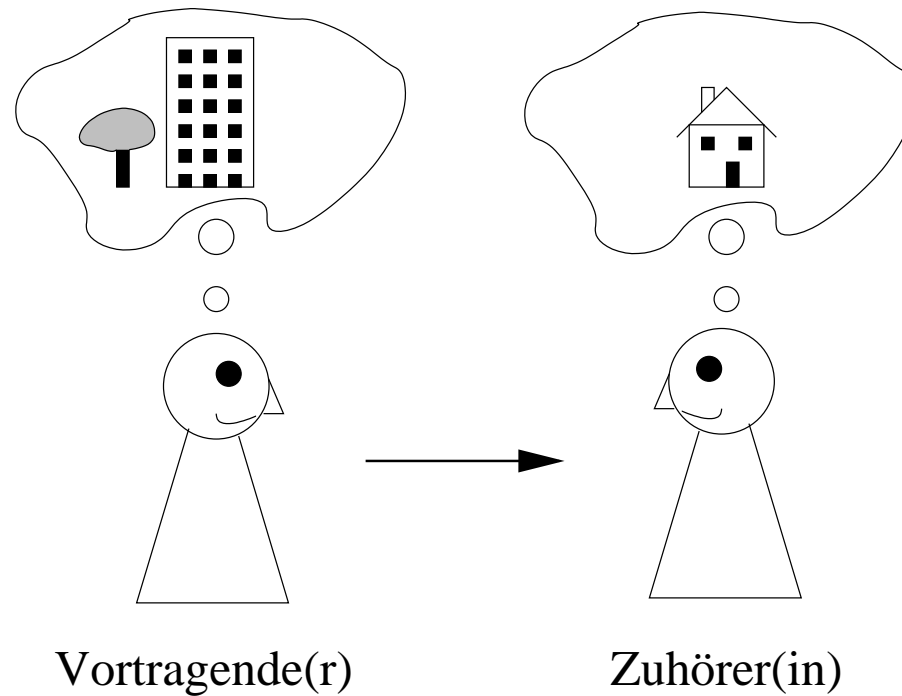
Antwort 1: Um die Zuhörer zu beeindrucken

Taktik:

- Viele Fremdwörter
- Schnelles Tempo
- Wenig hilfreiche Erklärungen
- Wenige Beispiele
- Voraussetzen von erheblichen Vorkenntnissen

Warum halte ich einen Vortrag?

Antwort 2: Um den Zuhörern eine Idee zu vermitteln



Zielsetzung

Auch wenn das Beeindrucken von Zuhörern manchmal wichtig sein kann: wir wollen hier **Ideen vermitteln!**

Daher:

- **Stoff** so aufbereiten (und evtl. einschränken), daß er gut vermittelbar ist
- Vortrag gut **strukturieren**
- **Zentrale Ideen** hervorheben
- Das Publikum **nicht überschätzen**
- **Redundanz**
- Geeignete **graphische Darstellungen** finden
- Gute **Beispiele** suchen

Umgang mit dem Publikum

- Zuhörer ansehen, **Blickkontakt** aufnehmen
- **Aktivierung** der Zuhörer durch Fragen, kleine Aufgaben, etc.

Und ein **Appell** ans Publikum:

Stellt Fragen, wenn Ihr etwas nicht verstanden habt und wenn Euch etwas interessiert!

Medien

Zur Verfügung stehen:

Overhead-Projektor Tafel (Beamer)

- **Folien:**

- dürfen gerne handbeschrieben sein
- mit großer Schrift, Bildern, Farbe, etc.
- nicht zu viel auf eine Folie quetschen
- nicht zu viele Folien vorbereiten

- **Medienwechsel:** auch die Tafel nutzen, z.B., um schwierige Sachverhalte zu erklären

Vorsicht: Aufmerksamkeit der Zuhörer richtet sich gerne auf die Projektionsfläche, vorbei am Sprecher.

Daher ...

Üben des Vortrags

- **Vortrag** vorher üben, evtl. vor Probepublikum
- **Zeit messen** (Dauer: ca. 45 Minuten)
- Vortrag **nicht auswendiglernen!**
- **Schlußworte** ausdenken (Kurze Zusammenfassung des Vortrags, abschließende Bewertung, “Danke. Gibt es Fragen?”)

Nur keine Panik! Ein bißchen Lampenfieber gehört aber dazu.

Literatur

- Viele der Vorträge basieren auf:
William Stallings: Cryptography and Network Security - Principles and Practice, Third Edition, 2003. Prentice Hall.
(Kann bei uns eingesehen werden.)
- Bei Bedarf: Eigene **Literaturrecherche**
 - Bibliothek
 - Verfolgen von Referenzen (“Recommended Reading”)
 - Internet
- **Literaturverzeichnis** in der Ausarbeitung nicht vergessen!

Ausarbeitung

- ca. 5-10 Seiten
- Zusammenfassung des Themas in eigenen Worten
- Weniger wichtige Details weglassen
- Ausarbeitung \neq Folien
- Muß bis zum Vortragstermin erstellt werden
- Am besten erst nach dem Vortrag austeilen
- Wir empfehlen \LaTeX zur Erstellung der Ausarbeitung
- Als Datei (PostScript, PDF, HTML, kein Word) an `koenigba@informatik.uni-stuttgart.de` schicken

Ablauf des Seminars

- **Vortrag**
 - Reine Vortragszeit: ca. 45 Minuten
 - Mit Zwischenfragen: maximal 1 Stunde
 - **Sprache:** Deutsch oder Englisch
- **Diskussion:** ca. 15 Minuten
- **Feedback** (siehe Feedback-Regeln)

Benotung

Die Note setzt sich aus **drei Teilen** zusammen:

- Erarbeitung und Verständnis des Themas
- Aufbau und Halten des Vortrags
- Ausarbeitung

Zeitplan

	Datum	Thema	Vortragende(r)
		Verschlüsselungsverfahren	
1	12.05.2003	Verschlüsselungsverfahren DES	Thomas Laun
2	19.05.2003	Verschlüsselungsverfahren RSA	Stefan Kiefer
3	26.05.2003	PGP: Pretty Good Privacy	Prokop Jehlicka
		Protokolle	
4	02.06.2003	Authentifizierung und digitale Unterschriften	Siegfried Langauf
5	16.06.2003	Schlüsselverteilung	Yang Zhou
6	23.06.2003	Angriffe I	Haiyi Peng
7	30.06.2003	Angriffe II	Qing Jiang
8	07.07.2003	Eindringlinge und Passwörter	Aymen Trigui
		Korrektheit	
9	14.07.2003	Kryptographische Protokolle und Model Checking	Ge Gao
10	21.07.2003	Zusatzvortrag	

Deadlines

3 Wochen vorher beim Betreuer melden!

	Deadline	Thema	Vortragende(r)
		Verschlüsselungsverfahren	
1	21.04.2003	Verschlüsselungsverfahren DES	Thomas Laun
2	28.04.2003	Verschlüsselungsverfahren RSA	Stefan Kiefer
3	05.05.2003	PGP: Pretty Good Privacy	Prokop Jehlicka
		Protokolle	
4	12.05.2003	Authentifizierung und digitale Unterschriften	Siegfried Langauf
5	19.05.2003	Schlüsselverteilung	Yang Zhou
6	02.06.2003	Angriffe I	Haiyi Peng
7	09.06.2003	Angriffe II	Qing Jiang
8	16.06.2003	Eindringlinge und Passwörter	Aymen Trigui
		Korrektheit	
9	23.06.2003	Kryptographische Protokolle und Model Checking	Ge Gao

Werbung in eigener Sache ...

Vorlesungen (Vertiefungslinie “Theoretische Informatik”)

- **Model Checking** (Javier Esparza)

Zeit: Montag, 15:45–17:15 Raum: V38.04

Übung: Donnerstag, 15:45–17:15 (14-tägig)

Raum: 0.363

- **Programmanalyse** (Barbara König)

Zeit: Montag, 11:30–13:00 Raum: V38.02

Übung: Donnerstag, 14:00-15:30 (14-tägig)

Raum: 0.453