Fachrichtung: Informatik Stufe: Diplom
Dozent: Engelke 02.07.2004

Kryptographische Verfahren

Dauer: 20 Minuten

Vorbereitungsphase

Welche Literatur/Skripte waren hilfreich?
Skript

Gibt es allgemeine Tipps, die bei der Vorbereitung helfen könnten?
- Skript und Übungen anschauen
- bei Verständnisproblemen andere Quellen suchen, wenn man es besonders gut machen will

Verlauf der Prüfung

Wie verlief die Prüfung?
- "Welches Themengebiet aus der Vorlesung hat Ihnen denn am besten gefallen?"
Dazu kamen dann zuerst die Fragen, danach zu den anderen Themengebieten. Es wurde relativ viel gefragt, Sie wollte keine ewig langen Antworten haben.

Wie reagierte der Prüfer, wenn Fragen nicht sofort beantwortet wurden?
Sie hakte nach, aber freundlich

Dein Kommentar zur Benotung:
1,0 was will man mehr

Welche Fragen wurden konkret gestellt?
- Auf welchen mathematischen Problemen basieren die "Public Key"(PK) - Algorithmen?
- Zeichnen Sie auf einen Zettel wie eine Signatur funktioniert (also etwas in der Art wie sig=m||PKB(k(m)), das wurde dann noch weiter ausgebaut)
- Allgemeine Fragen zu klassischen Chiffrierverfahren
- Werden die Modi CBC, EBC,...bei PK-Verfahren oder Symmetrischen Chiffrierungen angewendet?
- Was ist Padding undwofür ist es gut?
- Erklären Sie das Diffi-Hellmann Protokoll
- Nennen Sie Beispiele für symmetrische Chiffrierverfahren und deren Eigenschaften
- Zeigen Sie kurz, wie die RSA (De-)Chiffrierung funktioniert (Formeln für Schlüsselerzeugung etc,