

Klausur Datensicherheit

Semester:	AI7, WI5	SS 06,	17.7.2006
Bearbeitungszeit:	90 Minuten	Hilfsmittel:	Keine

Punkteangaben ohne Gewähr!

Aufgabe 1 (6 Punkte)

- a) Wozu dient der Friedman-Test?

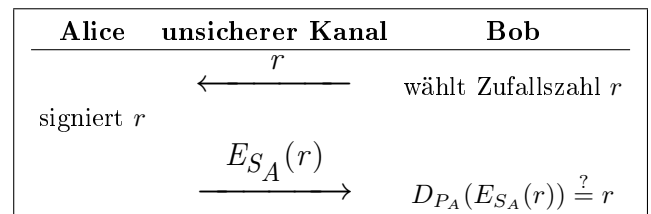
- b) Gegeben sei ein Chiffretext über dem Alphabet $(A, B, C, \dots Z)$. Welche Größen müssen Sie ermitteln als Eingabewerte für den Friedman-Test?

Aufgabe 2 (6 Punkte)

Was müssen Sie als Anwender beim Einrichten von SSH tun, damit Ihre SSH-Verbindungen sicher sind (d.h. dass mit einem Public Key Verfahren authentifiziert und Verschlüsselt wird)?

Aufgabe 3 (6 Punkte)

Authentifikation mit digitalen Signaturen kann z.B. wie folgt durchgeführt werden:



- a) Welchen Vorteil bietet dieses Protokoll gegenüber dem Challenge-and-Response-Protokoll?

- b) Welche Vorteile bietet dieses Protokoll gegenüber der Authentifikation mittels Passwort und Speicherung des Hashwerts des Passworts?

Aufgabe 4 (6 Punkte)

- a) Warum ist der RSA-Algorithmus zum Verschlüsseln von Emails in der Praxis ungeeignet?

- b) Wie wird das Problem (z.B. in GPG) gelöst?

Aufgabe 5 (12 Punkte)

- a) Beweisen Sie, daß 251 eine Primzahl ist.

- b) Berechnen Sie mit Hilfe des Fermat'schen Satzes die multiplikative Inverse zu 16 in \mathbb{Z}_{17} .

- c) Berechnen Sie mit dem erweiterten Euklidischen Algorithmus $10^{-1} \bmod 113$.

- d) Gibt es eine multiplikative Inverse zu 273 in \mathbb{Z}_{858} ? (Begründung!)