

## Aufgabe 13:

**Schutz von E-Mails durch Kryptographie**

E-Mails sind wie Postkarten: Jeder kann sie auf den Transportwegen abfangen und lesen oder manipulieren. In gewisser Weise sind E-Mails sogar noch schlimmer als Postkarten. Sie können nämlich automatisch „gelesen“, ausgewertet und manipuliert werden. Zum Glück gibt es jedoch Sicherheitsprotokolle wie *OpenPGP* oder *S/Mime*, mit denen sich Integrität, Vertraulichkeit und Authentizität von E-Mails sicherstellen lassen. Doch warum fragen mich eigentlich alle Nase lang Leute, was das da für ein komischer Anhang an meinen Mails ist, mit dem sie nichts anfangen können? Ich verweise dann immer auf die Homepage von *GnuPG*, ernte aber meist nur noch mehr Unverständnis.

Klären Sie in ihrer Ausarbeitung bitte die folgenden Fragen:

- Welche Sicherheitsprotokolle zum Schutz der E-Mail-Kommunikation gibt es?
- Welchen Funktionsumfang haben diese Protokolle? Was leisten sie, wo liegen die Grenzen? Wodurch unterscheiden sie sich?
- Gibt es Schwachstellen oder Angriffsmöglichkeiten?
- Werden die Protokolle eingesetzt? In welchem Umfang/ Personenkreis? Ist entsprechende Software verfügbar? Was kostet sie?
- Sollte sich herausstellen, daß die Protokolle nur von einem sehr kleinen Personenkreis verwendet werden: Warum?
- Geben Sie insbesondere in Bezug auf die Benutzbarkeit von Software zur E-Mail-Sicherheit Verbesserungsmöglichkeiten an.