Kryptosysteme, Keymanagment (KSK3) für CMS
12. Übungsblatt für den 16. Jänner 2007

45. (*Recherche*) Finde möglichst viele Anwendungen von elliptischen Kurven in der Kryptographie.

46. (*Recherche*) Welche Parameter für elliptische Kurven empfiehlt das NIST für die Nutzung durch die Regierung (government use)?

47. Klassifiziere – in Form einer Tabelle – alle Kryptosysteme, die wir in der Vorlesung kennengelernt haben, nach verschiedenen sinnvollen Kriterien (wie symmetrisch/nicht symmetrisch, Sicherheit, Effizienz, ...).

48. Stelle die Beziehungen/Zusammenhänge zwischen den Begriffen *Kryptosystem, Entschüsselungsfunktion, Verschlüsselungsfunktion, Schlüsselaustausch, Kompressionsfunktion, Hashfunktion, MAC* und *Digitale Signatur* möglichst anschaulich dar.