**Kryptosysteme, Keymanagment (KSK3) für CMS**
**9. Übungsblatt für den 12. Dezember 2006**

32. (*Recherche*) In welchen Punkten unterscheiden sich MACs und Digitale Signaturen? Gib einige konkrete Beispiele für die Verwendung von MACs und Digitalen Signaturen an.

33. (*Recherche*) Stelle Gemeinsamkeiten und Unterschiede von DSA und ElGamal Signaturschema fest.

34. Formatiere die Nachricht(Bitfolge) $m = 010001101011$ nach ISO/IEC 9796 mit Signaturlänge $k = 32$, d.h. berechne die Bitfolge $IR$.

35. Erzeuge ein zu ISO/IEC 9796 mit $k = 32$ kompatibles RSA-Signatur-Schlüsselpaar $(n, d)$, $(n, e)$.