Kryptosysteme, Keymanagment (KSK3) für CMS
8. Übungsblatt für den 5. Dezember 2006

27. (*Zur Konstruktion der kollisionsresistenten Kompressionsfunktion aus der Vorlesung*) Sei p eine n-bit Primzahl, so dass auch $q = \frac{p-1}{2}$ eine Primzahl ist. Wieviele Bits benötigt die Binardarstellung von $q - 1$?

28. (*Recherche*) Finde einige Beispiele für MACs und beschreibe sie jeweils kurz.

29. (*Recherche*) Wie berechnet man den CRC16 bzw. CRC32 Wert einer Bitfolge? Sind CRC16 bzw. CRC32 Hashfunktionen? Sind sie kollisionsresistent?

30. (*Recherche*) Was versteht man unter einer Merkle-Damgård-Hashfunktion?

31. (*Recherche*) Erkläre die Davies-Meyer-Konstruktion und finde Literaturquellen dazu.