Kryptosysteme, Keymanagment (KSK3) für CMS
4. Übungsblatt für den 7. November 2006

13. (*Recherche*) Erkläre in eigenen Worten die Begriffe *CPA* (chosen plaintext attack), *CCA1* (chosen ciphertext attack) und *CCA2* (adaptive chosen ciphertext attack).

14. (*Recherche*) Erkläre in eigenen Worten die Sicherheitsklassen *IND-CPA*, *IND-CCA1* und *IND-CCA2*. Worin unterscheiden sich diese drei Sicherheitsklassen?

15. Für das Cramer-Shoup-Kryptosystem benötigt man (große) Primzahlen p sodass $q = \frac{p-1}{2}$ ebenfalls prim ist. Erzeuge mit *Mathematica* eine Liste aller Primzahlen $p < 10^7$ mit obiger Eigenschaft.

    Hinweis: Die Funktionen `Prime`, `PrimePi`, `PrimeQ` sowie `Select` und `Range` könnten hilfreich sein.

16. (*) Sei p eine Primzahl sodass auch $q = \frac{p-1}{2}$ prim ist. Gesucht ist eine *Mathematica*-Funktion `CramerShoupElement[p]`, die nach jedem Aufruf ein zufälliges Element $g \in \mathbb{Z}_p^*$ mit Ordnung q liefert.

    Hinweis: Die Funktionen `Random` und `Module` könnten hilfreich sein. Mögliche Lösungswege:

    - eine Element der Ordnung $p-1$ (d.h. eine Primitivwurzel von $\mathbb{Z}_p^*$) finden (mit der Funktion `PrimitiveRoot`), und...

    oder

    - ein Element der Ordnung q finden (mit einer eigenen Funktion), und...

    oder

    - .....

    Beachte den folgenden

    > **Satz:** Gegeben sei eine endliche Gruppe $(G, \circ, ^{-1}, e)$, ein Element $x \in G$ der Ordnung n und eine natürliche Zahl k. Dann hat das Element x^k die Ordnung $\frac{n}{\mathrm{ggT}(n,k)}$.