Kryptographische Algorithmen

Blatt 7 09.06.2004, Abgabe 16.06.2004

Aufgabe 1. Gebe einen Betrüger $\tilde{\mathcal{P}}$ für das Poupard-Stern Protokoll an, der mit Ws $1/B$ durch Erraten der Frage e Erfolg hat.

Aufgabe 2. Gebe einen Simulator zum Poupard-Stern Protokoll an. Skizziere den Beweis von Thm. 6 [Poupard-Stern]. Zeige, dass der Simulator gute Tripel $((x'_1, \ldots, x'_K), e'_i, y'_i)$ mit Ws $1/B$ erzeugt.

Aufgabe 3. Zeige dass die vom Simulator erzeugte Verteilung stat. ununterscheidbar ist von der Übertragung im realen Protokoll $(\mathcal{P}, \tilde{\mathcal{V}})$, sofern $(n - \varphi(n))\ell B/A$ vernachlässigbar klein.