Kryptologie

Übung, LVA 405.321
C. Fuchs

13. Übungsblatt, SS 2022

15.06.2022

1. Faktorisiere 630548215070129547156718332495889632234434145411971275888376987603260225252787925196579351516987953684263473430861469319483991139381849698802970231911981983987683415722475488683509349075522834501479944197178114 843095289150401179520980618868881 mit der Methode von Fermat. (Diese Zahl wurde von einem österreichischen Terrorist in den 90er Jahren für ein mit RSA chiffriertes Bekennerschreiben an das Nachrichtenmagazin Profil verwendet.)

2. Faktorisiere $n = 89073489106939240931551386805730106 1$ mit der Pollardschen $p-1$-Methode.

3. Faktorisiere 753419 mit der folgenden Variante der Pollardschen $p-1$-Methode. Wähle Schranken A und B und verwende als Exponent

$$k = \prod_{\substack{p \in \mathbb{P}, p \leq A \\ p^e \leq B}} p^e.$$

   (Hinweis: Man wähle $A = 5$ und $B = 90$.)

4. Erkläre warum man die Zahl $132193 = 163 \cdot 811$ nur mit viel Glück mit der Pollardschen $p-1$-Methode faktorisieren kann (Variante nur mit B). Wie kann man B und A in der Variante der Pollardschen $p-1$-Methode wählen, um trotzdem eine Faktorisierung zu erhalten.