Kryptologie, Sommersemester 2003
Aufgaben zur Prüfungsvorbereitung

Klausur und mündliche Prüfungen finden am 16.7.2003 ab 9:00 Uhr statt. Die Termine für die mündlichen Prüfungen werden am 9.7. festgesetzt. Ich bitte alle Interessenten, sich dann in der Vorlesung in entsprechende Listen einzutragen.

Mit den folgenden, teilweise auch schwierigeren Fragen soll das Stoffgebiet der Vorlesung in etwa abgedeckt werden. In der Klausur sind alle Hilfsmittel zugelassen, aber die Lösungen sind ausschließlich „auf dem Papier" zu erarbeiten. Diese Probeklausur wird am 8.7. in der Übung besprochen. Überlegen Sie sich also vorher Ihre Fragen.

1. Welches ist die Gruppenordnung von $\mathbb{Z}_{209}^*$?
2. Zeigen Sie mit dem Fermat- und mit dem Miller-Rabin-Test, daß 21 keine Primzahl ist.
3. Wieso ist 561 eine Carmichael Zahl?
4. Wieso besitzt 18 ein Inverses in $\mathbb{Z}_{209}^*$? Berechnen Sie dieses!
5. Für den RSA-Modul n=133 sei e=5 der Verschlüsselungsexponent. Berechnen Sie den Entschlüsselungsexponenten.
6. Sei $n=pq$ das Produkt zweier Primzahlen. Wieso muß jemand, der die Ordnung eines beliebigen Elements von $\mathbb{Z}_n^*$ berechnen kann, p und q kennen?
7. Sei $n=pq$ das Produkt zweier Primzahlen. Wieso muß jemand, der in $\mathbb{Z}_n^*$ Quadratwurzeln berechnen kann, p und q kennen?
8. Finden Sie alle irreduziblen Polynome vom Grad 3 in $\mathbb{Z}_2[X]$. Wieso ist a priori klar, daß jedes dieser Polynome primitiv ist?
9. Zeigen Sie, daß das Polynom $f = X^4 + X + 1 \in \mathbb{Z}_2[X]$ primitiv ist. Wieviele Elemente besitzt der endliche Körper $\mathbb{Z}_2[X] \big/ (f)$? Berechnen Sie in diesem Körper das Produkt $\left(X^2 + X + 1\right)\left(X^3 + 1\right) = 111 \cdot 1001$. Benutzen Sie den erweiterten Euklidischen Algorithmus, um das multiplikativ Inverse von $\left(X^2 + X + 1\right) = 111$ in diesem Körper zu berechnen. (Stellen Sie in diesen Rechnungen die Polynome am besten durch Bitstrings dar.)
10. Finden Sie die 4 Quadratwurzeln von 4 in $\mathbb{Z}_{209}^*$!
11. Berechnen Sie die Ordnung von 11 in $\mathbb{Z}_{209}^*$!
12. Gibt es eine Lösung der Gleichung $x^2 = 41$ in $\mathbb{Z}_{1009}$?
13. Bestimmen Sie alle Punkte der elliptischen Kurve $y^2 = x^3 + 2x + 3$ über dem Körper $\mathbb{Z}_7$. Gibt es einen Punkt maximaler Ordnung in dieser Gruppe?
14. Was bedeutet es, wenn man sagt: Eine Gruppe besitzt ein schwieriges diskretes Logarithmus-Problem?
15. Beschreiben Sie den Diffie-Hellman Schlüsselaustausch in einer Gruppe mit schwierigem Logarithmus-Problem.
16. Beschreiben Sie den Cipher-Block-Chaining Modus des DES.