

Theoretische Fragen

1. Satz von Lamé (1.6).
2. Chinesischer Restklassensatz (2.6-2.7).
3. Pohig-Hellman-Algorithmus (6.1-6.5).
4. Deffie-Hellman Schlüsselaustausch (6.6).
5. ElGamal-Kryptosystem (7.1.).
6. Die Index-Calculus-Methode für diskrete Logarithmierung (7.2-7.3).
7. Babystep-Giantstep-Algorithmus von Shanks (8.1-8.2).
8. Pollard- ρ -Algorithmus (8.3-8.4).
9. Die Struktur der multiplicativen Gruppe des Ringes \mathbb{Z}_m (9.1-9.9).
10. Quadratischer Reziprozitätssatz (10.1-10.6 mit Beweis, 10.7 ohne Beweis.)
11. Carmichael Zahlen (11.1-11.3)
12. Die allgemeine Struktur des probablistischen Primzahlentests (11.5).
13. Verstärkung des Fermatischen Satzes (11.6).
14. Miller-Rabin Test (11.7).
15. Satz von Monier-Rabin (11.9, ohne Beweis).
16. Thechebyschow-Funktion (12.1-12.5).
17. Kinder binomialer Satz (13.3), Lemma 13.4.
18. Satz von AKS (ohne Beweis) mit gutem Verständniss (13.5-13.8).
19. Mersenne-Zahlen und Lukas-Lehmer Satz (14.1-14.6).
20. RSA-Kryptosystem (15.1-15.3).