Theoretische Fragen

1. Euklidischer Algorithmus* und Satz von Lame* (1.1, 1.2, 1.5, 1.6).
2. Chinesischer Restklassensatz* (2.6-2.7).
3. Die Struktur der multiplikativen Gruppe des Ringes $\mathbb{Z}_m$ (4.1-4.9)*.
4. Pohig-Hellman-Algorithmus für diskrete Logarithmierung (5.1-5.5).
5. Deffie-Hellman Schlüsselaustausch (5.6).
6. ElGamal-Kryptosystem (5.7).
7. Das Geburtstagsparadox* und der Pollard-ρ-Algorithmus für diskrete Logarithmierung (6.1-6.4).
8. Babystep-Giantstep-Algorithmus von Shanks für diskrete Logarithmierung (6.5-6.6).
9. Die Index-Calculus-Methode für diskrete Logarithmierung (6.7-6.8).
10. Quadratischer Reziprozitätssatz (7.1-7.6 mit Beweis*, 7.7 ohne Beweis.)
11. Carmichael Zahlen* (9.1-9.3)
12. Die allgemeine Struktur des probablistischen Primzahlentests (9.5).
13. Verstärkung des Fermatischen Satzes* (9.6).
14. Miller-Rabin Test (9.7).
15. Satz von Monier – Rabin (9.9 ohne Beweis).
16. Thchebyschow-Funktion (11.1-11.3 mit Beweis*, 11.4 ohne Beweis).
17. Kinder binomialer Satz (12.3 mit Beweis*); Lemma 12.4 (ohne Beweis).
18. Satz von AKS (ohne Beweis) mit gutem Verständnis (12.5-12.8).
19. Mersenne-Zahlen und Lukas – Lehmer Satz (14.1-14.6).
20. RSA-Kryptosystem (15.1-15.3).
21. Sätze von Vahlen und Legendre über Kettenbrüche (16.1). Wieners-Attacke auf das RSA-Kryptosystem. (16.2-16.4)
22. Definition der elliptischen Kurve. Definition der Addition auf einer elliptischen Kurve. Genaue Formel für $P_1 + P_2$ (Vorlesung 17).
23. Satz von Gauß über die Anzahl der projektiven Lösungen der Gleichung $x^3 + y^3 + z^3 = 0$ in $\mathbb{F}_p$ (mit Beweis* im Fall 1). Folgerung. Definition der elliptischen Kurve über $\mathbb{F}_p$. Satz von Hasse (Vorlesung 18.)
24. Diskriminant. Lemma. Satz von Nagell – Lutz (mit teilweisem Beweis*). Folgerung (Vorlesung 19).
25. Elliptische Kurven Algorithmus von Lenstra (20.1-20.5).
26. Definition des primitiven Elements des Grades n in einem Ring (21.1). Definition der diskreten direkten und inversen Fourierschen Transformation (21.2, 21.4). Sätze 21.3 und 21.7 (mit Beweis*).
27. Schnelle Berechnung der diskreten Fourierschen Transformation eines Vektors (22.1, 22.2).
28. Schnelle Berechnung des Produktes zweier Polynomen: ein Algorithmus (22.3).
29. Definition einer (nicht)deterministischen Turingmaschine. Die Sprache, die die (nicht)deterministische Turingmaschine akzeptiert. Definition der rekursiv aufzählbaren und rekursiv entscheidbaren Sprachen (Vorlesung 23).
30. Definition der Klassen **P** und **NP** (24.1). Definition von **NP**-vollständigen Problemen (24.2).