Kódoláselmélet Tételsor

A vizsga alatt elbeszélgetünk a megadott témáról, a megfelelő matematika állításokról és az ahhoz kapcsolódó egyszerű feladatokról ami demonstrálja hogy a hallgató érti az adott definíciókat és állításokat.

1. RSA-kódolás (üzenet küldés, aláírás, fej vagy írás)
2. Miller-Rabin-teszt
3. Carmichael-számok
4. Legendre-szimbólum számítása
5. Solovay-Strassen-teszt
6. Fermat-faktorizáció
7. Négyzetgyök n lánctörtes közelítése
8. Faktorizáció Pollard rho-módszere
9. Diszkrét logaritmus, Sylvester-Pohlig-Hellman-algoritmus
10. Diffie-Hellman-féle kulcsváltás, Massy-Omura és Elgamal rejtjelrendszerek
11. Elliptikus görbék és alkalmazása
12. Kódolás alapfogalmak (információs ráta, hibajavító képesség, stb.)
13. Duális kódok, dimenziótétel
14. Tökéletes kódok, Hamming-kód és dekódolása
15. Kiterjesztett bináris Golay-kód és dekódolása
16. Ciklikus kódok, generátorpolinom
17. BCH-kódok tervezése
18. Reed-Solomon-kódok tervezése