# Gyakorló zárthelyiek 2023 tavasz

1. RSA titkosítás
   1. Két körös Miller-Rabin teszt segítségével mutassa meg, hogy a 257 és 631 prímszám-e vagy összetett (a bázisok legyenek: 7,17)!
   2. Generáljon egy RSA titkosításhoz titkos és nyilvános kulcspárt. Használja a 257 és a 631 számokat, ha a Miller-Rabin szerint prímszámok, egyébként válasszon másik számot. A titkosító exponens egyike a következő számoknak a feltételeknek megfelelően: 12,33,47, 49. Végezetül titkosítsa a 20 nyilvános üzenetet!
2. RSA digitális aláírás
   1. Kínai maradéktétel segítségével generáljon aláírást a 20 nyilvános üzenethez, ha a prímek 31 és 41 és az aláíró kulcs 317.
   2. Ellenőrizze le, hogy érvényes a 79 aláírt üzenet. Legyen az ellenőrző kulcs 53, a prímek 31 és 41. A csatornán megkaptuk még az eredeti üzenetet, amely 44.