# Zárthelyiek 2022 tavasz

1. Teszteljük le Fermat prímtesztet alkalmazva a 563 számot, ha az alap a 7-! Mit tudunk mondani róla?
2. Két körös Miller-Rabin teszt segítségével mutassa meg, hogy a 937 prímszám-e vagy összetett (a bázisok legyenek: 11,15)!
3. Generáljon egy RSA titkosításhoz titkos és nyilvános kulcspárt amennyiben a két választott prímszám a következő: a 257 és az 631, és a titkosító exponens egyike a következő számoknak a feltételeknek megfelelően: 12,33,47, 49.
4. Az RSA titkos kulcsunk: 7 és 13 prímek, valamint a 70 titkos exponens. Fejtsük vissza a 10 titkosított üzenetet a kínai maradék tétel segítségével!