14. Számelméleti algoritmusok

Műveletek lépésszáma:

Összeadás:

Szorzás:

Hatványozás:

Hatványozás modulo m:

Euklideszi algoritmus :

Prímtesztelés:

Fermat-teszt:

Nyilvános kulcsú titkosírás:

Digitális aláírás:

RSA titkosírási módszer:

Üzenetekből számok képzése?

p és q prímek generálása?

n,m kiszámítása

e és d választása

titkos és nyílt adatok

kódolás és dekódoló fgv-ek

dekódolás működik