**Kriptográfia tételsor 2018/2019 1.félév**

1. A bizalmas kommunikáció modellje és alapfogalmai.
2. Szimmetrikus és aszimmetrikus kriptorendszerek fogalma.
3. Klasszikus szimmetrikus kriptorendszerek.
4. A helyettesítéses titkosítás kriptoanalízise.
5. DES.
6. AES.
7. Hash függvények és egyirányú csapóajtó függvények.
8. Az RSA algoritmusa és paramétereinek a megválasztása.
9. A diszkrét logaritmuson alapuló titkosítás.
10. A diszkrét elliptikus logaritmuson alapuló titkosítás.
11. Vegyes kriptorendszerek, kulcs-csere.
12. Digitális aláírás, az RSA aláírás, a DSA algoritmus.
13. Nyilvános kulcsú infrastruktúra (PKI).
14. A vak aláírás és alkalmazásai.