Számítógépes hálózatok
gyakorló feladatok 12.

Lukovszki Tamás

1. feladat: Tekintsük x_1 és x_2 résztvevő adatrátájának vektor-ábrázolását.

1. Tegyük fel, hogy x_1 AIMD (additive increase multiplicative decrease) stratégiát használ az adatrátájának a szabályozásához, x_2 pedig AIAD (additive increase additive decrease) stratégiát. Ábrázolja az adatráták változását (hasonlóan, mint ahogy az előadás fóliákon látható). Tegye fel, hogy a résztvevők mindig azonos időben döntik el, hogy az adatrátát csökkentik vagy növelik.
2. Kaphatunk-e fair erdeményt, ha a különböző résztvevők különböző stratégiákat használnak az adatráta szabályozására? Miért (nem)?

2. feladat: (RSA) Legyen p=13, q=7 két prímszám, $n = pq$ és e=7. A nyilvános kulcs (n, e).

1. Határozza meg a (n, d) privát kulcsban d értékét.
2. Legyen m=5 az üzenet. Számolja ki a $c = m^e \bmod n$ titkosított üzenetet.
3. Kódolja vissza a titkosított üzenetet, azaz számolja ki $c^d \bmod n$ értékét.

3. feladat: Adja meg egy hálózat alábbi fenyegetéseihez a fenyegetés tipusát és a megsértett biztonsági célokat az előadásnak megfelelően.

1. Egy trojai email, ami ETR felhasználói nevet és jelszót kémlel ki.
2. Egy hálózati router, ami csomagtartalmat analizál és kategorizál.
3. Denial-of-service támadás egy Web-szerver ellen.
4. Egy WLAN felhasználó, aki engedély nélkül a szomszéd WLAN-ját használja.
5. Egy adminisztrátor, aki a hálózati log-file-okat manipulál.