

Vizsgafeladatok hálózatok biztonsága tárgyból

Figyelem! A kérdések közül 2 pont értékűt áthúzhat! Csak az **első át nem húzott 20 pont értékű** kérdésre adott válaszait vesszük figyelembe! Ha már rendelkezik ebből a részből korábban elfogadott (legalább 12 pontos) eredménnyel, akkor amennyiben ezt a feladatlapot értékelésre beadja, **ezen a vizsgán ez számít!** Amennyiben ebből a részből a 12 pontot eléri, az eredményét a következő vizsgára tovább viheti, ha a másik rész sikertelen.

1. Mit jelent a *visszajátszás*, mint támadás? Adjon rá egy példát is! (2x0.5 pont)
2. Milyen védekezési módokat ismer a *SYN flood* ellen? Mutassa be, hogyan működnek! (2 pont)
3. Hogyan működnek a vírusok? (1 pont)
4. Milyen utakat, módokat használnak fel rosszindulatú programok a terjedésükre? (5x0.2 pont)
5. A kriptográfiai *aktív támadások*at milyen kategóriába sorolhatjuk (támadási erő szerint)? (1 pont)
6. Mit értünk az alatt, hogy egy feladatra *nem létezik hatékony algoritmus*? (1 pont)
7. Milyen követelménynek kell megfelelnie egy kriptográfiai célokra használható véletlenszám generátornak? (1 pont)
8. Mit tud a DSA-ról? (1 pont)
9. Zajos csatornán történő valós idejű mozgókép és hang átvitelhez milyen blokkrejtjelezési módot használna? (0.3 pont) Miért? (0.7 pont)

10. Üzenethitelesítés (MAC) megvalósítására milyen módszereket ismer (2 db)? Adja meg ezek alapötletét is! (1 pont)
11. Mi a digitális aláírás célja? Alaposan kérem (az esetlegesen használt szakszavak magyarázatával)! (1 pont)
12. Mutassa be a Diffie-Hellman kulcsmegegyezés protokoll működését! (2 pont)
13. Mit tud a biometriai partnerhitelesítési módszerekről?(1 pont)
14. Írjon le 5 fontos fogalmat a nyilvános kulcsú infrastruktúra (PKI) témában! (5x0.2 pont)
15. Érdemes a secure VPN-t és a trusted VPN-t együtt alkalmazni? (0.2 pont) Válaszát indokolja! (0.8 pont)
16. Egy cég munkatársainak ADSL előfizetést vásárol. Ennek felhasználásával szeretné megoldani, hogy a munkatársai otthonról is elérjék a céges szervereket és az IP telefon rendszert. Szükség van-e az ADSL előfizetéseknel fix IP címre? Ha igen, hány darabra, ha nem, akkor hogyan oldja meg? (1 pont)
17. Ismertesse PGP-nél a digitális boríték lényegét! (1 pont)
18. Mit jelent a passzív támadás? (1 pont)
19. Mutassa be RSA-nál a kulcsok létrehozásának menetét! (2 pont)