2006. tavasz – **1**. vizsga **1**. rész név:

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. Hálózati támadásnak milyen motivációi lehetnek? (legalább 3 félét említsen) (1 pont)

2. Az *IP spoofing* alkalmas-e az internet használó kilétének elrejtésére (anonimitás biztosítására)? (0.2 pont) Válaszát indokolja! (0.8 pont)

3. Mutassa be a Smurf támadást! Mi a támadás célja? (2 pontért alapos választ kérek!)

4. Mit tud a trójai faló (Trojan Horse) típusú programokról? (1 pont)

5. Mit jelent a *gyakorlati titkosság*? (1 pont)

6. Hogyan működik a *triple-DES*? (1 pont)

7. Mit értünk az alatt, hogy egy feladatra *létezik hatékony algoritmus*? (1 pont)

8. Kriptográfiai célokra miért nem alkalmazhatunk tetszőleges véletlenszám generátort? (Például ami egy számítógépes játékban, vagy akár tudományos igényű szimulációban megfelel.) (1 pont)

9. Mi az a kulcs hierarchia? (1 pont)

2006. tavasz – **1**. vizsga **1**. rész név:

10. Milyen tulajdonsággal rendelkezik egy *egyirányú hash függvény*? (1 pont)

11. Miért van szüksége a CFB (Cipher Feed Back) nevű eljárásra? Miért nem használhatjuk helyette a CBC-t? (1 pont)

12. Mi az üzenethitelesítés célja? Alaposan gondolja végig! (1 pont)

13. Milyen (3db) csoportokba sorolhatók a partnerhitelesítés módszerei? (1 pont)

14. Soroljon fel 4 fontos adatot, amit egy tanúsítványnak tartalmaznia kell! (1 pont)

15. Milyen előnye és milyen hátránya van a *secure VPN*-nek a *trusted VPN*-hez viszonyítva? (2x 1 pont)

16. Mit tud a PGP kulcsgondozásáról? (1 pont)

17. Mi az a CRL, és miért van rá szükség? (1 pont)

18. Mi a baj az MD5-tel? (Miért kell lecserélni?) (1 pont)

19. Mutassa be RSA-nál a kulcsok létrehozásának menetét! (2 pont)