2006. tavasz név:

I. ZH *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! Ahhoz, hogy a ZH a vizsgába beszámítson, legalább a pontok 60%-át, azaz 12 pontot kell megszerezni. A zárthelyi megírása, sőt beadása sem kötelező. Ez csak egy lehetőség, de ugyanakkor csak egy lehetőség, pótZH nem lesz. A be nem adott vagy gyenge eredményű ZH nem jelent hátrányt a vizsgán, sőt a beszámíthatóság határát elérő ZH esetén is a hallgató dönti el, hogy kéri-e a ZH eredmény beszámítását vagy sem.

1. Tegyük fel, hogy rlogin-nal be lehet lépni a G gépről az S szerverre. Ha egy T támadó az S-re a G gép IP címével próbál bejutni, blind spoofing esetén milyen lépéseket foglal magába egy sikeres támadás? (3 dolgot említsen) (3 pont)

2. Miért veszélyes a SYN cookie használata? (1 pont)

3. Mi az a rejtekajtó (trap door vagy back door)? (1 pont)

4. Az ún. algoritmikus támadást egy kriptográfiai rendszer mely részén hajtja végre a támadó? (1 pont)

5. Miért szükséges a DES-t lecserélni? (1 pont)

6. Rómeó (R) szeretne megkérni Júlia (J) kezét. A lánykérést úgy szeretné végrehajtani, hogy csak Júlia tudjon a dologról, ő viszont biztos lehessen abban, hogy ki a kérője. Nyilvános kulcsú kriptográfia esetén (1) hogyan kódolja el Rómeó az x=”Please marry me!” nyílt üzenetet? (2) hogyan fejti meg Júlia a reményei szerint Rómeótól származó y üzenetet? (2x 1 pont)

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

8. Miben nyújt többet a digitális aláírás az üzenethitelesítésnél? (1 pont)

2006. tavasz név:

9. Mutasson be egy eredményes támadást a Diffie-Hellman kulcscsere (helyesebben kulcsmegegyezés) protokoll ellen! Lehetőleg tömören, képlet szerű jelöléseket használva írja le a támadást! (3 pont)

10. Biztonságos átvitelre milyen megoldásokat ismer abból a szempontból, hogy hol történik a titkosítás? Kettőt említsen, és mindegyikre adjon konkrét, használható megoldást is! (2x 1pont)

11. PGP-nél mit jelent a digitális boríték és miért van rá szükség? (2x 1 pont)

12. Mikor nevezünk egy elektronikus aláírást minősített elektronikus aláírásnak? Az ilyen aláírással ellátott okirat bizonyító ereje milyen, a polgári életben ismert okirat fajta bizonyító erejének felel meg? (2x 1 pont)

13. Számítsa ki $\mathbf{7^{100}}$ **(mod 13)** értékét! (Súgás: a nyers erő módszere helyett érdemes legalább az ismételt hatványozás és szorzás módszerét használni, illetve aki ismeri a kis Fermat tételt, annak még egyszerűbb!) (2 pont)