Tentamen i Krypteringsmetoder och Säkring av Datasystem

7.5 hp

15 mars, 2018

Maxpoäng: 30p. **Betygsgränser**: 12p: betyg 3, 18p: betyg 4, 24p: betyg 5.
Hjälpmedel: Miniräknare samt formelsamling som medföljer tentamenstexten.

Kursansvarig: Eric Järpe, telefon 0729-77 36 26, 035-16 76 53.

Till uppgifterna skall *fullständiga lösningar* lämnas. Lösningarna ska vara *utförligt* redovisade! Varje lösning ska börja överst på nytt papper. Endast en lösning per blad. Lösningar kommer finnas på internet: `http://dixon.hh.se/erja/teach` → `Krypteringsmetoder och säkring av datasystem.`

1. Vilken kultur var den första i världen att använda substitutionskryptering (och även frekvensanalys)? (2p)

2. Nämn en Public Key Infrastructure standard. (2p)

3. Låt $N = 9\,398\,610$.
   (a) Primtalsfaktorisera N. (3p)
   (b) Beräkna $7^{6676999} \bmod N$ (3p)

4. Vad kallas den regel som säger att ett krypteringssystems säkerhet inte ska vara beroende av kännedom om vilket system som använts och kryptotexten, utan bara hemlighållandet av den lilla del som brukar kallas krypteringsnyckeln. (2p)

5. För etablering av gemensam nyckelhemlighet kan Diffie-Hellman-protokollet användas.
   (a) Ange en attack[1] mot detta protokoll. (2p)
   (b) Ange ett protokoll som är en utveckling av Diffie-Hellman-protokollet och som är säkert mot attacken i (a). Alternativt beskriv i korthet hur man kan skydda sig mot attacken i (a). (2p)

6. Gunnar ska baka bullar och kakor till ett stort kafferep. På en bullplåt får han plats med 63 bullar och på en kakplåt får 133 kakor plats. Hur många bullplåtar måste Gunnar grädda om alla plåtar ska vara fulla, det ska bli minst 83 000 kakor och det ska bli exakt 87 654 bakverk totalt? (3p)

7. Vad blir risken för kollision om 5 lösenord hashas med en 8 binära bitars hashfunktion? (4p)

[1] Det ska vara en attack som är välkänd för att utnyttja en svaghet i protokollet. T.ex. "brute force"-gissning av nyckeln är alltså inte ett giltigt svar i detta sammanhang.

8. Nämn en säkerhetsprinciper som gör ett krypteringssystem svårt att knäcka och förklara vad den går ut på. (3p)

9. Antag att ett meddelande ska överföras, att alla tecken i meddelandet överförs oberorende av varandra och att varje tecken överförs korrekt med sannolikhet 999‰. Beräkna hur många tecken meddelandet kan innehålla om 99% av dem ska överföras korrekt med approximativt 99% sannolikhet. (4p)

LYCKA TILL!