Tentamen i Krypteringsmetoder och Säkring av Datasystem

7.5 hp

12 augusti, 2020

Maxpoäng: 30p. **Betygsgränser**: 12p: betyg 3, 18p: betyg 4, 24p: betyg 5.
Hjälpmedel: Miniräknare samt formelsamling.
Kursansvarig: Eric Järpe, telefon 0729-77 36 26, 035-16 76 53.

Alla svar skall ges med 4 decimalers noggrannhet där ej annat anges. 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. Nämn en nackdel för kryptering med symmetriska nycklar och en nackdel för kryptering med publika nycklar. (3p)

2. Vem var den dubbelspion som arbetade för drottning Mary Stuart av Skottland genom att agera budbärare av den krypterade kommunikationen mellan Mary och hennes allierade ledda av Anthony Babington, men egentligen var ytterst lojal mot fienden drottning Elizabeth I av England och därför rapporterade alla krypterade meddelanden till hennes hänsynslöse säkerhetschef Sir Francis Walsingham? (3p)

3. Beräkna det minsta tal $x > 147\,174\,714$ sådant att $47^x \equiv 1 \bmod 1144$. (3p)

4. Nämn tre kvalitetsegenskaper för hashfunktioner. (3p)

5. Vilka personer föreslog 1976 *konceptet* kryptering med publika nycklar? (3p)

6. Beräkna
   (a) polynomkvoten då $x^7+3x^5+x^4+4x^3+x^2+4x+2$ divideras med $x^6+x^5+4x^4+3x^3+5x^2+2x$. (3p)
   (b) $\gcd(x^7+3x^5+x^4+4x^3+x^2+4x+2,\ x^6+x^5+4x^4+3x^3+5x^2+2x)$. (4p)

7. Från vilket berömt forskningsinstitut kom de tre grundarna av krypteringssystemet RSA? (3p)

8. Flora ska arrangera en bukett med enbart prästkragar (som har 29 kronblad per blomma), skogsfibbla (med 17 kronblad per blomma) och blåsippor (som har 7 kronblad per blomma). Av övernaturliga skäl måste det
   - totala antalet kronblad i hela buketten vara exakt 7 777,
   - sammanlagda antalet prästkragar och skogsfibblor ska vara dubbelt så stort som antalet blåsippor,
   - finnas minst 100 blommor av varje sort.

   Hur många blommor av varje sort måste Floras bukett innehålla? (5p)

LYCKA TILL!