Tentamen i Krypteringsmetoder och Säkring av Datasystem

7.5 hp

17 mars, 2021

Maxpoäng: 30p. **Betygsgränser**: 12p: betyg 3, 18p: betyg 4, 24p: betyg 5.
Hjälpmedel: Miniräknare TI-30Xa 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. Vilken sorts kryptering användes av Queen Mary Stuart of Scotland i sin konspiration mot Queen Elizabeth I of England? (3p)

2. Låt $n = 1\,063\,506$.
   (a) Primtalsfaktorisera n. (3p)
   (b) Beräkna $\gcd(1\,357,\, n)$. (3p)
   (c) Beräkna $1\,357^{2\,346\,119} \bmod n$. (4p)

3. Ange kortfattat med en mening vad *empirisk styrka* innebär hos ett krypteringssystem. (3p)

4. Beräkna $x^8 + 4x^6 + 3x^5 + 4x^3 + 3x + 1 \bmod(5,\, x^5 - 1)$. (3p)

5. Vad kallas de misstänkta meddelanden som bildades från en stor textmassa genom att systematiskt välja varannan bokstav, var tredje bokstav, osv ur textmassan, föreslaget år 1994 av den israeliske matematikern Eliahu Rips? (3p)

6. Man ska överföra ett meddelande bestående av 10 176 tecken. Varje tecken överförs felaktigt med 5% sannolikhet och tecknen överförs oberoende av varandra. Hur stor andel av det totala meddelandet överförs då korrekt med 99% sannolikhet? (4p)

7. Varje krypteringssystem bygger på en säkerhetsprincip som ska vara lätt att göra åt ena hållet (vid krypteringen) och åt andra hållet (vid dekrypteringen) under förutstättningen att man har den hemliga krypteringsnyckeln, men är svårt att göra åt andra hållet om man inte har nyckeln. Nämn 4 sådana säkerhetsprinciper. (4p)

LYCKA TILL!