Tentamen i Krypteringsmetoder och Säkring av Datasystem

7.5 hp

17 mars, 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. Vad hette Queen Elizabeths fruktade underrättelseminister under 1500-talets England. (Efternamnet räcker.) (2p)

2. Nämn tre digitala signaturer. (3p)

3. Vad är täljaren vid heltalsdivision om resten är 97, kvoten är 98 och nämnaren är 99? (3p)

4. Vad kallas den sortens kryptering där man byter plats på tecknen med varandra enligt en systematisk procedur, snarare än att byta tecknen systematiskt mot andra tecken? (3p)

5. Vad innebär egenskapen *(first) pre-image resistance* hos en hashfunktion? (3p)

6. Låt $n = 134\,391\,636$.
   (a) Primtalsfaktorisera n. (3p)
   (b) Beräkna $11\,717^{126\,985\,970} \bmod n$. (3p)

7. Förklara *kort* hur man-in-the-middle-attacken mot Diffie-Hellmans protokoll för nyckelutväxling går till. (3p)

8. Vad kallas den symmetriska krypteringsmetod som användes av i princip alla hemliga agenter under kalla kriget och som innebär att klartexten, tal för tal, adderas till motsvarande tal ur en slumpmässig krypteringsnyckel? (3p)

9. Beräkna polynominversen av $f_5 = x^2 + 4x + 1 \mod(5, x^3 - 1)$. (4p)

LYCKA TILL!