Tentamen i Krypteringsmetoder och Säkring av Datasystem

7.5 hp

31 maj, 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. Hur många olika kryptoalfabet kan åstadkommas vid Caesarrullning? (2p)

2. Nämn 2 digitala signaturer. (3p)

3. Avgör om talen 2 581 153 och 5 491 557 är relativt prima. (4p)

4. Varför kan man inte använda vanlig frekvensanalys för att knäcka ett Vignère-krypto? (3p)

5. Vad innebär ensidig autenticiering? (3p)

6. Ett meddelande med 117 tecken ska skickas över en förbindelse med teckenfelsannolikhet 3%. Vad är då approximativt sannolikheten att minst 100 tecken överförs korrekt? (3p)

7. Nämn en antik form av steganografi. (2p)

8. Vad kallas fenomenet när två olika records, x och x', ger samma hashvärde, $h(x) = h(x')$? (2p)

9. Låt $f = x^4 - x^2 + x + 1$ och $g = x^4 - x^3 - x^2 + x$.
   (a) Beräkna polynomkvoten f/g mod 3. (2p)
   (b) Existerar den diskreta polynominversen f^{-1} mod $(3, g)$? Om ja, beräkna denna invers. Om nej, bevisa det. (4p)

10. Vad hette den person som betydde mest för kryptoanalysen av Enigmakryptot? (Efternamnet räcker.) (2p)

LYCKA TILL!