Tentamen i Krypteringsmetoder och Säkring av Datasystem

7.5 hp

12 augusti, 2019

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. Vad hette Queen Elizabeths chef för spioneri och underrättelseverksamhet under 1500-talets England? (Efternamnet räcker.) (3p)

2. Beräkna den diskreta inversen 111^{-1} mod 1111. (3p)

3. Vad står förkortningen MDC för när det gäller dataöverföring? (3p)

4. Vad hette det krypteringssystem som låg till grund för DES (Data Encryption Standard)? (4p)

5. Beräkna matrisprodukten $\begin{bmatrix} 3 & 2 \\ -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 4 \\ 1 & 3 \end{bmatrix}$ (3p)

6. Vad kallas ett system som initierar och administrerar certifikat? (3p)

7. Beräkna minsta heltal $n > 12345$ så att $2n^3 - 55n^2 + 454n \equiv 1001 \pmod{37}$. (4p)

8. Vid en arkeologisk utgrävning hittas 8 olika stora lådor. En ovärderlig skatt kan räddas om man öppnar den rätta av dessa lådor, men man vet inte vilken man ska välja och om man väljer fel går skatten förlorad. Tillsammans med lådorna hittas inskriptionen

   Pär Riolph | Ölf Udopammar | Ravi Loke | My Ursack | Krön Cachm

   Denna tros vara ett krypterat meddelande som skulle kunna ge ledning till vilken av lådorna som ska öppnas. Fyndet dateras till en tid och plats då endast steganografi och Vignèrekrypto med Caesarrullning var kända metoder. Kan du hjälpa arkeologerna med deras kryptoanalys? (4p)

9. Antag att man bildar samtliga n tecken långa lösenord med ett alfabet bestående av m tecken. Vad är då risken att man får minst en kollision då man k gånger slumpmässigt väljer ett lösenord? (4p)

LYCKA TILL!