Tentamen i Krypteringsmetoder och Säkring av Datasystem

DI4014 7.5 hp

augusti, 2024

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.

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 det krypteringssystem som kröntes till AES då NISTs krypteringstävling avgjordes år 2000? (3p)

2. Vad hette det gods i England där flera 1000 av de mest framstående kryptoanalytikerna i Storbritannien arbetade under andra världskriget? (2p)

3. Beräkna $107^{125^{163}}$ mod 153. (4p)
(Observera att med $107^{125^{163}}$ menas $107^{(125^{163})}$, inte $(107^{125})^{163}$.)

4. Vad är en *scytale*? (3p)

5. Nämn två metoder för nyckelgenerering som är utvecklingar av Diffie-Hellman. (4p)

6. Vilket är det minsta positiva heltalet x sådant att

$$\begin{cases} x \equiv 12 \pmod{21} \\ x \equiv 34 \pmod{43} \\ x \equiv 56 \pmod{65}? \end{cases}$$ (4p)

7. Vad hette den man som ledde Queen Mary Stuarts sammansvärjning mot Queen Elizabeth då Mary satt fängslad i Towern? (Efternamnet räcker.) (3p)

8. Vad innebär *empirisk styrka* hos ett krypteringssystem? (3p)

9. I ett IOT-system ska lösenord lagras på ett 1 GB minne. Lösenorden ska vara 11 eller 12 tecken långa. Under antagandet att varje tecken motsvarar 1 B (dvs en Byte) hur många 11 tecken långa lösenord kan sparas så att det blir så nära antalet 12 tecken långa lösenord och så att minnet utnyttjas maximalt? (4p)

LYCKA TILL!