Tentamen i Krypteringsmetoder och Säkring av Datasystem

7.5 hp

mars, 2022

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 var förlaga till AES (Advanced Encryption Standard)? (2p)

2. Vad kallas den säkerhetsprincip som innebär att man för givna heltal g, a, b, N ska ange det heltal K som gör att $g^{xy} \equiv K \mod N$ där x uppfyller villkoret $g^x \equiv a \mod N$ och y uppfyller villkoret $g^y \equiv b \mod N$. Den trebokstaviga förkortningen räcker som svar. (2p)

3. Avgör om 4 är en generator för fältet $\mathbb{F}_{11}$. (3p)

4. Nämn namnet på eller beskriv en känd kryptoanalysmaskin. (3p)

5. Vad var kodbeteckningen för en av andra världskrigets största tyska offensiver som Sverige varnade för då Arne Beurling knäckt G-skrivarkryptot? (3p)

6. Lös kongruensekvationssystemet $\begin{cases} x \equiv 10 \pmod{11} \\ x \equiv 12 \pmod{13} \\ x \equiv 14 \pmod{15} \end{cases}$ (4p)

7. Vad den krypteringsteknik som innebär att man flyttar om tecknen i klartextmeddelandet snarare än byter ut dem mot andra bokstäver? (3p)

8. Ange en krypteringsmetod som inkluderar en lösning på nyckeldistributionsproblemet och som anses vara säker mot framtidens kvantdatorer. (2p)

9. Antag att ett meddelande överförs via en brusig förbindelse där varje tecken överförs felaktigt med sannolikhet 0.9%. Hur många tecken kan meddelandet bestå av om det ska vara 99% approximativ sannolikhet att minst 99% av tecknen överförs korrekt? (4p)

10. Beräkna $\gcd(2x^7 + 2x^4 + x + 1,\ x^6 + 2x^2 + 2x + 2) \mod 3$. (4p)

LYCKA TILL!