Tentamen i Krypteringsmetoder och Säkring av Datasystem

7.5 hp

juni, 2023

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. Beräkna diskreta inversen till 16 mod 61. (3p)

2. Vad hette det krypteringssystem som var *föregångare* till AES (Advanced Encryption Standard)? (2p)

3. Vad kallas den säkerhetsprincip som innebär att man för givna heltal a, b, N ska ange det heltal x som gör att $a^x \equiv b \bmod N$. Den trebokstaviga förkortningen räcker som svar. (2p)

4. Bestäm en 2-siffrig generator av gruppen $\mathbb{F}_{23}$. (3p)

5. Nämn en krypteringsmaskin. (2p)

6. Nämn två pseudoslumptalsgeneratorer (PRNG). Förkortningar räcker. (4p)

7. Lös kongruensekvationssystemet $\begin{cases} x \equiv 4 \pmod 7 \\ x \equiv 5 \pmod 8 \\ x \equiv 6 \pmod 9 \end{cases}$ (4p)

8. Vad hette det polyalfabetiska substitutionskrypto som på 1500-talet blev den främsta efterföljaren till monoalfabetiskt substitutionskrypto? (3p)

9. Ange två kvantdatorsäkra krypteringsmetoder. (3p)

10. Beräkna $\gcd(3x^5 + 2x^3 + 3x^2 + 4x + 4,\ 4x^5 + x^4 + 2x^3 + 4x + 3) \bmod 5$. (4p)

LYCKA TILL!