Tentamen i Krypteringsmetoder och Säkring av Datasystem

DI4014 7.5 hp

mars, 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.

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. Nämn ett polyalfabetiskt substitutionskrypto. (2p)

2. Beräkna en 2-siffrig generator för fältet $\mathbb{F}_{23}$. (3p)

3. Nämn 3 kvalitetsegenskaper för hashfunktioner. (3p)

4. Dekryptera det XOR-krypterade meddelandet

   `10010001111010`

   med LFSR-nyckeln

   `0101100010`. (4p)

5. Nämn ett krypto där man kan kryptera och dekryptera med samma nyckel och samma metod. (3p)

6. Vad hette den person som uppfann det krypto som senare fick tjäna som DES. (Efternamnet räcker.) (2p)

7. Lös kongruensekvationssystemet

$$\begin{cases} x \equiv 3 \bmod 31 \\ 2x \equiv 8 \bmod 82 \\ 3x \equiv 6 \bmod 63 \end{cases} \quad \text{(5p)}$$

8. *Förklara* vad Auguste Kerckhoffs är mest känd för beträffande kryptologi? (3p)

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

LYCKA TILL!