Tentamen i Krypteringsmetoder och Säkring av Datasystem

7.5 hp

maj, 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 kallas den stav som man lindade en läderremsa runt för att snabbt kunna avläsa ett meddelande gömt bland andra bokstäver som var skrivna på nämnda remsa enligt en teknik från 400 f.Kr. och därmed var en av de första formerna av steganografi? (2p)

2. Nämn en fördel och en nackdel för kryptering med publika nycklar. (3p)

3. Avgör om den diskreta inversen av 139 mod 931 existerar och beräkna den i så fall. (3p)

4. *Mlecchita-Vikalpa* var ett slags indiskt substitutionskrypto där hälften av alfabetets tecken var parade med andra hälften av alfabetet (i valfri ordning). Parningen innebar att varje förekomst av ett tecken ur klartexten byttes mot andra halvan i paret[1]. I vilket välkänt över 2000 år gammalt indiskt litterärt verk är denna krypteringsmetod ursprungligen presenterad? (3p)

5. Nämn två av de tre algoritmer som en digital signeringsalgoritm består av. (3p)

6. Beräkna den principala resten av $42\,103^{30\,241} + 120\,043^{43\,201} \bmod 14\,022$. (3p)

7. Antag att man använder LFSR med nyckeln 11010100111. Ange de tre första värdena i sekvensen som därpå följer. (3p)

8. Nämn ett programmeringsspråk för programmering i kvantdatorer. (3p)

9. Vad hette den person som uppfann krypteringssystemet *Lucifer* som ugjorde förlaga till DES. Även tekniken som används vid detta krypteringssystem och många andra är uppkallad efter honom. Efternamnet räcker. (3p)

10. För vilka tal $n \in \mathbb{Z}^+$ ger $n^3 + 23n^2 + 167n + 397$ resten 12 vid heltalsdivision med 13? (3p)

LYCKA TILL!

[1] Detta innebar att det blev samma metod för kryptering som för dekryptering – orehört praktiskt!