Tentamen i Krypteringsmetoder och Säkring av Datasystem

DI4014 7.5 hp

augusti, 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. Vad kallas den säkerhetsprincip som innebär att man för given ordning n och givet element $a \in \mathbb{Z}_n$ ska ange $x \in \mathbb{Z}^+$ så att $x^2 \equiv a \pmod{n}$? Den trebokstaviga förkortningen räcker som svar. (2p)

2. Beräkna $2\,345\,679^{6\,969\,602} \bmod 3\,236\,992$. (4p)

3. Nämn en krypteringsmaskin. (2p)

4. Nämn en metod för steganografi. (2p)

5. Gunhild arrangerar sin uteservering. Där ska finnas små runda bord med plats för 3 personer, avlånga bord med plats för 8 personer och stora runda bord med plats för 11 personer. Hur många bord måste Gunhild *minst* ha totalt för att det ska få plats exakt 777 personer vid utserveringen och de ska finnas dubbelt så många små runda bord som stora runda? (3p)

6. Vad kallas den samling regler för kryptering med publika nycklar som även kan innehålla rutiner för säkerhet och digitala ID-kort? Den trebokstaviga förkortningen räcker. (2p)

7. Vad hette den närmast förtrogne till Queen Mary I av Skottland som ledde kuppförsöket mot Queen Elizabeth I av England? För- och efternamn, tack. (3p)

8. Ange tabellen för generatorn 3 i fältet $\mathbb{Z}_7$. (3p)

9. Vad kallas den sortens krypteringssystem som Lucifer och DES var exempel på efter sin upphovsmakare? (3p)

10. I ett fält angivet av en elliptisk kurva $y^2 = x^3 + ax + b \pmod{p}$ där p är ett primtal > 3 beräknas summan $P + Q$ av två givna punkter P och Q enligt följande:
Om $P = (x_1, y_1)$ och $Q = (x_2, y_2)$ så är $P + Q = (x_3, y_3)$ där
$$\begin{matrix} x_3 = m^2 - x_1 - x_2 \bmod p \\ y_3 = m(x_1 - x_3) - y_1 \bmod p \end{matrix} \quad \text{och} \quad m = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1} \bmod p & \text{om } P \neq Q \\ (3x_1^2 + a)(2y_1)^{-1} \bmod p & \text{om } P = Q \end{cases}$$
Betrakta nu den elliptiska kurvan $y^2 = x^3 + 5x - 2 \pmod{7}$.
   (a) Verifiera att punkterna $(1, 2)$ och $(2, 4)$ ligger på kurvan. (2p)
   (b) Beräkna punkten $(1, 2) + (2, 4)$ i fältet. (4p)

LYCKA TILL!