Tentamen i Krypteringsmetoder och Säkring av Datasystem

DI4014 7.5 hp

mars, 2024

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 följande säkerhetsprincip för krypteringsändamål: givet en ordning N, generator g och uppsnappade tal A och B, ange a sådant att $g^a \pmod N = A$ eller b sådant att $g^b \pmod N = B$? (Den trebokstaviga förkortningen räcker.) (2p)

2. En krypteringsmetod kallas *reciprok* om exakt samma procedur kan användas för både kryptering och dekryptering. Nämn en reciprok metod. (3p)

3. Beräkna det minsta positiva tal x sådant att $\begin{cases} x \equiv 12 \pmod{23} \\ x \equiv 34 \pmod{45} \\ x \equiv 56 \pmod{67} \end{cases}$ (4p)

4. Vad hette den skotska drottning, i för- och efternamn, som konspirerade mot att störta drottning Elizabeth I i 1500-talets England? (2p)

5. Vad hette den svenske matematikprofessor, i för- och efternamn, som knäckte det tyska G-skrivarkryptot under andra världskriget? (3p)

6. Låt $n = 123\,456$ och
   (a) primtalsfaktorisera n, (3p)
   (b) beräkna $\gcd(1\,234\,567, n)$, (3p)
   (c) beräkna $1\,234\,567^{1\,191\,555} \bmod n$. (3p)

7. Vad kallas en betrodd tredje aktör vid en krypterad kommunikation mellan två parter? (Den trebokstaviga förkortningen räcker.) (2p)

8. Vid kommunikation mellan olika parter kan man behöva en procedur där man verifierar att man verkligen är den man utger sig för att vara. Vad kallas en sådan procedur? (2p)

9. Låt $f = a_0 + a_1x + \ldots + a_{N-1}x^{N-1}$ och $g = b_0 + b_1x + \ldots + b_{N-1}x^{N-1}$. Då är faltningsprodukten $h = f * g \bmod (d, x^N - 1)$ definierad som $h = c_0 + c_1x + \ldots + c_{N-1}x^{N-1}$ där
$$c_k = \sum_{i+j \equiv k \,(\mathrm{mod}\, N)} a_i b_j \mod d \quad \text{för } k = 0, 1, \ldots, N-1.$$
   Beräkna $(-1 + 3x + x^2) * (1 + 2x) \bmod (5, x^3 - 1)$. (3p)

LYCKA TILL!