Tentamen i Krypteringsmetoder och Säkring av Datasystem

7.5 hp

15 augusti, 2018

Maxpoäng: 30p. **Betygsgränser**: 12p: betyg 3, 18p: betyg 4, 24p: betyg 5.
Hjälpmedel: Miniräknare 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. Vad hette det gods som engelsmännen med Alan Turing i spetsen använde som högkvarter för sin underrättelseverksamhet under andra världskriget, framför allt för kryptoanalysen av Enigman? (2p)

2. För att knäcka en kod som krypterats med hjälp av en krypteringsnyckel kan man med kännedom om krypteringssystemet systematiskt gissa på alla möjliga nycklar och pröva dessa. Vad kallas den tekniken? (3p)

3. Beräkna lcm(13 572, 17 226). (3p)

4. Vad kallas de ord och meningar som (bl a) matematikern Eliyahu Rips lyckades hitta i en välkänd text genom att i stora textmassor välja ut de bokstäver han fick genom att systematiskt hoppa över ett antal bokstäver i texten och bilda en ny text av de bokstäverna han valt? (3p)

5. Vad innebär egenaskapen *second pre-image resistance* hos en hashfunktion? (3p)

6. Beräkna den diskreta multiplikativa inversen av 2 781 mod 973. (3p)

7. Vid kryptering med El Gamal och vid nyckelgenerering med Diffie-Hellman utgörs en vital del av ett visst matematiskt problem. Detta problem skulle kunna lösas blixtsnabbt med Shors algoritm i en kvantdator med hög kapacitet.
   (a) Vad kallas detta problem? (2p)
   (b) Hur lyder problemet? (3p)

8. Lös kongruensekvationen $x^5 + x^2 \equiv x^7 - x \pmod 5$. (2p)

9. Låt $[x]$ betyda *heltalsdelen av* x, dvs $[x] = \max\{k \in \mathbb{Z} : k \leq x\}$.
   (a) Bevisa att för alla $x \in \mathbb{R}$ och $y \in \mathbb{Z}$ är $[x - y] = [x] - [y]$. (3p)

   Låt dessutom $(x \bmod 1) = x - [x]$ för alla $x \in \mathbb{R}$.
   (b) Bevisa att för alla $x \in \mathbb{R}$ och $a, b \in \mathbb{Z}$ är $((ax \bmod 1)b \bmod 1) = ((bx \bmod 1)a \bmod 1)$. (3p)

LYCKA TILL!