Tentamen i Krypteringsmetoder och Säkring av Datasystem

7.5 hp

25 maj, 2011 kl. 14.00 – 18.00

Maxpoäng: 30p. **Betygsgränser**: 12p: betyg G, 21p: betyg VG.
Hjälpmedel: Miniräknare samt formelsamling som medföljer tentamenstexten.
Kursansvarig: Eric Järpe, telefon 0702-822 844, 035-16 76 53.

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 är *Kerberos* (när det gäller datasäkerhet)? (3p)

2. Vad skiljer ett substitutionskrypto från ett Vignèrekrypto? (3p)

3. Beräkna den diskreta inversen till 15 modulo 37. (3p)

4. Vad kallas den teknik som handlar om att *gömma* meddelanden, inte kryptera dem? (3p)

5. På 1970-talet började USA använda en krypteringsalgoritm som hette DES och som sedan höll flera decenneier. Vad står förkortningen DES för? (3p)

6. Primtalsfaktorisera talen
   (a) 49 (1p)
   (b) 312 (1p)
   (c) 12 091 (2p)

7. Nämn en nackdel med symmetriska nycklar och en nackdel med asymmetriska nycklar. (4p)

8. Under andra världskriget använde Tyskland en kodningsmaskin som var mycket framgångsrik och först efter ett monumentalt arbete knäcktes av de allierade. Vad kallades
   (a) den kodningsmaskin som tyskarna använde? (2p)
   (b) de kod*knäckning*smaskiner som de allierade konstruerade för att knäcka tyskarnas kod? (2p)

9. För vilka heltal a är $12a^2 \equiv 3 \pmod 7$? (3p)

LYCKA TILL!