Tentamen i Krypteringsmetoder och Säkring av Datasystem

7.5 hp

17 mars, 2014 kl. 9.00 – 13.00

Maxpoäng: 30p. **Betygsgränser**: 12p: betyg 3, 18p: betyg 4, 24p: betyg 5.
Hjälpmedel: Typgodkänd 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. Ett krypto som användes under lång tid var DES.
   (a) Vad står förkortningen DES för? (2p)
   (b) Vilket annat krypto var DES en utveckling av? (2p)

2. Primtalsfaktorisera talen
   (a) 91 (2p)
   (b) 405 (2p)
   (c) 1 389 648 (3p)

3. Hur skiljer sig en signeringsalgoritm från en krypteringsalgoritm? (3p)

4. Faktorisera talet 6 439 om man vet att $\phi(6\,439) = 6\,256$ där ϕ är Eulers ϕ-funktion. (4p)

5. I *Rövarspråket* ersätts varje konsonant med ett "o" och samma konsonant igen, dvs varje konsonant, x, ersätts med mönstret "xox". Är detta exempel på ett substitutionskrypto, ett Vignèrekrypto eller steganografi? (3p)

6. Nämn 2 viktiga säkerhetsaspekter vid val av hashalgoritmer. (3p)

7. Man vill konstruera ett nätverk som skyddas av 10 000 st 4 tecken långa lösenord. Hur många tecken måste finnas i den teckenuppsättning som man väljer tecknen bland för att sannolikheten att en slumpmässigt vald kod inte råkar vara en av de 10 000 giltiga lösenorden ska bli mindre än 1%? (4p)

8. Avgör om den diskreta inversen till 737 mod 373 existerar och beräkna den i så fall. (5p)

LYCKA TILL!