Tentamen i Krypteringsmetoder och Säkring av Datasystem

7.5 hp

4 juni, 2019

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 kallas den utveckling av monoalfabetiskt substitutionskrypto som innebär att man systematiskt enligt ett visst schema hoppar mellan ett antal olika substitutionskrypton för varje nytt tecken i klartexten? (3p)

2. Vad blir den principala resten vid heltalsdivision av $111^{22} + 33$ med 123? (3p)

3. I Kerberos nätverksautenticieringsprotokoll används tre servrar. Ange benämningen på minst två av dessa. (4p)

4. I en bokhandel finns det tre hyllplan i en 81 cm bred bokhylla lediga. Man vill fylla dessa med ett antal exemplar av den 27 mm tjocka boken *The code book* av Simon Singh och den 84 mm tjocka *The codebreakers* av David Kahn. Kan detta göras så att hyllorna fylls till sista millimetern och det blir 16 fler exemplar av Singhs bok än det blir av Kahns? (4p)

5. Diffie-Hellman-protokollet (DH) är en rutin för nyckelöverenskommelse. Nämn
   (a) en attack mot detta protokoll. (3p)
   (b) ett annat protokoll som bygger på DH men som innehåller skydd mot attacker mot DH. (3p)

6. Beräkna $\phi(1\,670\,633\,952)$ (där ϕ betecknar Eulers totientfunktion). (4p)

7. År 1977 publicerade tre forskare vid MIT en artikel om ett krypteringssystem som var det första att erbjuda publika nycklar som lösning på nyckelparadoxen. Vad heter krypteringssystemet som ännu idag är ett av de mest använda? (2p)

8. Lös kongruensekvationssystemet

$$\begin{cases} x \equiv 123 \pmod{13} \\ 2x \equiv 312 \pmod{32} \\ 3x \equiv 321 \pmod{21} \end{cases} \quad (4p)$$

LYCKA TILL!