Tentamen i Krypteringsmetoder och Säkring av Datasystem

7.5 hp

30 maj, 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. Nämn ett nätverksautenticieringsprotokoll. (2p)

2. Beräkna 3456^{-1} mod 4567, dvs den diskreta multiplikativa inversen till 3456 då man räknar mod 4567. (3p)

3. För att verifiera en digital signatur i ett certifikat kan en verifieringsnyckel i ett annat certifikat användas. Detta andra certifikats digitala signatur kan verifieras med en nyckel i ett tredje certifikat, osv. Vad kallas denna typ av sekvens av certifikat? (2p)

4. Under andra världskriget använde engelsmännen s.k. *cillies* i sina försök att knäcka tyskarnas Enigmakod. Vad var *cillies* för något? (3p)

5. Beräkna $123^{45^{67}}$ mod 89. (3p)

6. Vad kallas den faktoriseringsalgoritm som implementerad i en kvantdator med hög kapacitet skulle innebära ett avgörande hot mot all RSA-kryptering? (3p)

7. Vid konstruktion av hashfunktioner är minimal kollisionsrisk en önskvärd egenskap. Vad kallas det resultat som säger att det antal personer, n, man måste räkna med för att $P(\text{minst 2 av de } n \text{ personerna fyller år samma dag}) > \frac{1}{2}$ blir överraskande litet? (3p)

8. Nämn ett krypteringssystem med publika nycklar som idag skulle vara säkert mot kryptoanalys med hjälp av en kvantdator med hög kapacitet. (3p)

9. Bestäm alla heltal n sådana att $12n^3 + 1 \equiv 4n^2 + 3n \pmod{28}$. (4p)

10. Ett hemligt meddelande överförs med Vernamchiffer och överkryptering. Du snappar upp att Alice först skickar

    0 4 3 8 6 1 8 5 1 9 7 9 6 5 6 3 0 0 4 6 8 1 9 6 5 3 9 5

    att Bob sedan svarar

    8 0 2 4 6 5 2 5 2 9 5 8 9 0 3 2 9 2 7 0 7 3 9 0 2 8 6 6

    och att Alice slutligen skickar

    8 3 1 4 0 8 4 4 1 1 9 3 5 3 8 7 9 7 4 8 9 8 0 3 8 4 8 2

    Knäck koden! (4p)

LYCKA TILL!