Tentamen i Krypteringsmetoder och Säkring av Datasystem

7.5 hp

19 mars, 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 hette den svenske matematikprofessor som knäckte nazisternas krypteringssystem *G-schreiber* under andra världskriget? (3p)

2. Primtalsfaktorisera talet 1 008 478 500. (3p)

3. Vad står förkortningen TTP för i datasäkerhetssammanhang? (3p)

4. Bestäm det minsta positiva heltal x sådant att $x \equiv 123 \pmod{234}$ och $x \equiv 345 \pmod{456}$. (4p)

5. Vad kallas den form av kryptering som innebär att varje förekomst av ett visst tecken, säg a, byts mot ett annat tecken, varje förekomst av ett visst annat tecken, säg b, byts mot ett tredje tecken osv? (3p)

6. Vad innebär Kerckhoffs princip? (3p)

7. Beräkna $54\,919^{15\,683} \bmod 3\,567$. (3p)

8. Vid en förbindelse överförs varje tecken korrekt med sannolikhet 99.8% oberoende av varandra. Hur många tecken kommer fram korrekt med 95% säkerhet om meddelandet som skickas är 101 702 tecken långt? (4p)

9. Signering av meddelanden med hjälp av metoden *El Gamal* går till som följer:

   i. Antag att meddelandet m ska signeras där $m < p$ och p är ett stort primtal.

   ii. Välj ett till stort primtal q så att $p - 1$ är multipel av q.

   iii. Konstruera en generator g av $\mathbb{F}_p$.

   iv. Välj ett tal a (privat nyckel).

   v. Beräkna $b = g^a \pmod{p}$ publik verifieringsnyckel.

   vi. Signering:

   - Välj ett tal $k < p$ sådant att $\gcd(k, p-1) = 1$.
   - Beräkna $r = g^k$.
   - Beräkna s sådant att $ar + ks \equiv m \pmod{q}$.
   - Signaturen är då (r, s).

   vii. Verifiering:

   - Kolla att villkoret $b^r r^s \equiv g^m \pmod{p}$ är uppfyllt.

   Använd denna metod för att signera och verifiera meddelandet $m = 42$, med $p = 59$, q största värde enligt villkoren, $g = 2$, $a = 3$, k minsta värde enligt villkoren och så att $k \neq a$. (4p)

LYCKA TILL!