Tentamen i Krypteringsmetoder och Säkring av Datasystem

DI4014 7.5 hp

augusti, 2024

Maxpoäng: 30p. **Betygsgränser**: 12p: betyg 3, 18p: betyg 4, 24p: betyg 5.
Hjälpmedel: Miniräknare TI-30Xa samt formelsamling.
Kursansvarig: Eric Järpe, telefon 0729-77 36 26.

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. (a) Avgör vilket/vilka tal p av talen 2 357, 2 359, 2 361, 2 363 och 2 365 som är primtal. (3p)

   För primtalet/primtalen p i (a)

   (b) beräkna $\gcd(12\,421, p-1)$. (3p)

   (c) beräkna $12\,421^{42124} \bmod p-1$. (4p)

   (d) gör en uppskattning av *antalet* generatorer $> \frac{p}{3}$ för fältet $\mathbb{F}_p$. (3p)

2. Vilken krypteringsteknik kunde tillämpas med hjälp av Albertis krypteringsskiva? (2p)

3. Beräkna $(4x^3 + 5x + 1)^{-1} \bmod (7, x^4 - 1)$. (3p)

4. Nämn någon krypteringsmetod, annan än Rijndael, av finalisterna i NISTs tävling för symmetriska blockkrypton 1997–2000. (3p)

5. Vad brukar man kalla det exempel på påstådd steganografi genom att med ett fixt antal bokstävers avstånd gömma ord och som studerades av den israeliske matematikern Eliyahu Rips? (2p)

6. Vad är den trebokstaviga förkortningen som står för att med en kvantdator distribuera krypteringsnycklar som på grund av elementalpartiklarnas invecklingsegenskap inte kan observeras av obehöriga utan att detta avslöjas? (2p)

7. Låt $n = 77$ och a minsta möjliga värde enligt specifikationerna av RSA-signatur (se nästa sida).

   (a) Signera hashsumman $h(m) = 26$. (4p)

   (b) Verifiera signaturen från (a). (1p)

LYCKA TILL!

RSA-signatur

Låt m vara det dokument som ska signeras. Då är proceduren vid RSA-signatur:

1. Beräkna hashsumman $h(m)$.
2. Låt p, q vara primtal så att $pq = n > m$.
3. Välj a som är relativt prima med $\phi(n)$.
4. Beräkna $b = \text{lcm}(p-1, q-1)$ och $d = a^{-1} \bmod b$.
5. Signera: $s = h(m)^a \bmod n$.
6. Verifiera: $s^d \bmod n = m$.