O.S. Institutionen för matematik
KTH

Problem till övning nr 8 den 4 maj, SF1610 Diskret matematik CINTE, vt2018

1. (E) Ett RSA-krypto har de offentliga nycklarna $n = 55$ och $e = 7$. Kryptera meddelandet $a = 2$ och dekryptera meddelandet $b = 2$.
2. (E) Bestäm antalet RSA-krypton med parametrarna n, e, d som en kan skapa med ett n i intervallet $50 \leqslant n \leqslant 60$.
3. (E) Ett RSA-krypto har $n = 33$. Ange samtliga möjliga värden på den offentliga krypteringsnyckeln e som vi kan välja i intervallet $1 < e < 12$.
4. (C) Du ska välja två primtal p, q för att skapa ett RSA-krypto, med 200 (decimal-) siffror per primtal. Ungefär hur många val av paret $\{p, q\}$ finns det? (Du kan söka på nätet efter 'the prime number theorem' för att hjälpa dig.) Kan en skapa en databas som innehåller alla sådana primtal?
5. (E) En 1-felsrättande kod C med längden $n = 11$ defineras av parity-check matrisen
$$\mathbf{H} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$
   (a) Bestäm antalet ord $|C|$ i koden C.
   (b) Rätta orden `11000000000`, `11111110111`, och `01100000000`.
   (c) Bestäm antalet ord som varken finns i den felkorrigerande koden C och inte heller går att rätta.
6. (E) Fyll i matrisen $\mathbf{H}$ nedan så att den blir kontrollmatrisen (parity-check matris) till en 1-felsrättande kod.
$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & & \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & & & & 1 & \end{pmatrix}$$
7. (D) Hur många kodord finns det i koden som har följande kontrollmatris? Lista dessa kodord.
$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$
8. (E) Undersök, t.ex. genom att skriva funktionerna nedan på en disjunktiv normalform, om nedanstående Booleska polynom representerar samma Booleska funktion:
$$(x\bar{y} + \bar{x})\bar{z}\bar{w} + \bar{y}(\bar{x} + z) \qquad \text{resp.} \qquad \bar{y}(\bar{w} + z) + \bar{x}\bar{z}(\bar{y} + y\bar{w})$$
9. (D) Bestäm antalet Booleska funktioner $f(x, y, z, u, w)$ från B^5 till B sådana att
$$f(x, y, z, u, w) = f(x, y, z, \bar{u}, w), \quad \text{och} \quad f(0, 1, 0, 1, 0) = f(1, 0, 1, 0, 1).$$
10. (C) Karaktärisera samtliga Booleska funktioner g och h från B^n till B sådana att det finns minst en Boolesk funktion f som löser "andragrads-ekvationen" $ff + fg = h$.

Svar

1. Elementet 2 krypteras till $E(2) = 18$, och dekrypteras till $D(2) = 2^{23} = 8$.
2. 56, om vi tillåter ett av primtalen att vara 2; annars 44. (Detta räknar även $e = 1$ som inte skulle väljas i praktiken, men metoden fungerar även för detta e.)
3. 3, 7, 9, 11.
4. $\binom{k}{2}$ där $k = \pi\big(10^{200}\big) - \pi\big(10^{199}\big)$ och $\pi(x)$ = antalet primtal $\leqslant x$ är primtalsräknefunktionen. Enligt 'the prime number theorem'/primtalssatsen är $k \geqslant 10^{197}$. Det uppskattas finnas runt 10^{80} atomer i det observerbera universum, så nej: det går inte att lista alla dessa primtal.
5. (a) 128.
   (b) `11010000000`, `11111110111`, resp går ej att rätta.
   (c) 512.
6. $$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$
7. 2 ord: `000` och `111`. Obs! Det är **rangen** som är viktig.
8. Ja, de beskriver samma funktion.
9. 32768.
10. Varje par av Booleska funktioner g och h från B^n till B ger en lösbar ekvation.

E-mail address: `sisask@kth.se`