KTH Matematik
Examinator: Petter Brändén
Kursansvarig: Olof Sisask

Σ p	G/U	bonus

Efternamn	förnamn	pnr	programkod

Kontrollskrivning 4A till Diskret Matematik SF1610, för CINTE, vt2018

Inga hjälpmedel tillåtna.
Minst 8 poäng ger godkänt.
Godkänd KS nr n medför godkänd uppgift n vid tentor till (men inte med) nästa ordinarie tenta (högst ett år), $n = 1, \ldots, 5$.
13–15 poäng ger ett ytterligare bonuspoäng till tentamen.
Uppgifterna 3)–5) kräver väl motiverade lösningar för full poäng.
Uppgifterna står inte säkert i svårighetsordning.
Spara alltid återlämnade skrivningar till slutet av kursen!

Skriv dina lösningar och svar på samma blad som uppgifterna; använd baksidan om det behövs.

1) (För varje delfråga ger rätt svar $\frac{1}{2}$p, inget svar 0p, fel svar $-\frac{1}{2}$p.
Totalpoängen på uppgiften rundas av uppåt till närmaste icke–negativa heltal.)
Kryssa för om påståendena **a)**–**f)** är sanna eller falska (eller avstå)!

		sant	**falskt**
a)	En linjär kod med dimension 4 har 4! kodord.		X
b)	I ett RSA-krypto, om de offentliga parametrarna är $n = 33$ och $e = 7$, då är dekrypteringsnyckeln $d = 3$.	X	
c)	Om x och y är kodord i en linjär kod, då är $x - y$ också ett kodord.	X	
d)	Det finns exakt $\binom{4}{2}$ Booleska funktioner $f(x, y, z, w)$ som ger värdet 1 på precis hälften av sina inputs.		X
e)	Om $f(x, y)$ och $g(x, y)$ är Booleska funktioner, då är $f(x, y) = f(x, y) + f(x, y)g(x, y)$.	X	
f)	Koden med kontrollmatrisen $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$ kan upptäcka (men ej nödvändigtvis rätta) 1-bitsfel på kodord från den motsvarande koden.	X	

poäng uppg.1

Namn	poäng uppg.2

2a) (1p) Du håller på att konstruera ett RSA-krypto med primtalen $p = 3$, $q = 5$ och krypteringsnyckel $e = 3$. Vad är den offentliga modulon n och den privata dekrypteringsnyckeln d?
(Det räcker att ange rätt svar.)

Svar: $n = 15$ och $d = 3$

b) (1p) Låt $\mathbf{H}$ vara kontrollmatrisen

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}.$$

för en linjär kod. Rätta meddelandet $y = \texttt{1010}$ enligt närmaste-granne-principen för denna kod.
(Det räcker att ange rätt svar.)

Svar: `1011`

c) (1p) Låt f vara den Booleska funktionen

$$f(x, y, z) = \overline{x + y \cdot \overline{z}} + \overline{x} \cdot \overline{z} \cdot (y + 1).$$

Beräkna $f(0, 1, 0)$.
(Det räcker att ange rätt svar.)

Svar: `1`

Namn	poäng uppg.3

3) (3p) Betrakta följande kontrollmatris $\mathbf{H}$ som bestämmer en linjär kod $\mathcal{C}$.

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

(a) Om du inte kan göra (b), hitta *ett* kodord i koden.
(b) Hitta och skriv ned *alla* kodord i koden, t.ex. genom att lösa systemet av linjära ekvationer.

OBS. En komplett lösning med fullständiga motiveringar skall ges.

Lösning: enligt definitionen för hur en kod bestäms av en kontrollmatris så består kodorden av lösningarna x till $\mathbf{H}x = 0$. För att lösa detta ekvationssystem så gaussar vi matrisen och får efter några steg fram att systemet har samma lösningar som

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Som ses från trappstegsformen på matrisen så har vi två fria variabler: x_4 och x_5, som kan specificeras valfritt som 0 eller 1, och sedan är de andra variablerna bestämda enligt

$$\begin{aligned} x_1 &= x_4 \\ x_2 &= x_5 \\ x_3 &= x_4 + x_5. \end{aligned}$$

Orden är alltså

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}.$$

Namn	poäng uppg.4

4) (3p) Uttryck den Booleska funktionen

$$f(x,y,z) = \overline{x + y \cdot \overline{z}} + \overline{x} \cdot \overline{z} \cdot (y+1)$$

på *disjunktiv normalform* (normalform för summa av produkter).
OBS. En komplett lösning med fullständiga motiveringar skall ges.

Lösning: vi expanderar allt vi kan med hjälp av de Morgans lagar, dubbelnegationslagen och distributiva lagen:

$$\begin{aligned} f(x,y,z) &= \overline{x} \cdot \overline{y \cdot \overline{z}} + \overline{x} \cdot \overline{z} \cdot (y + \overline{y}) \\ &= \overline{x} \cdot (\overline{y} + z) + (\overline{x} \cdot \overline{z} \cdot y + \overline{x} \cdot \overline{z} \cdot \overline{y}) \\ &= (\overline{x} \cdot \overline{y} + \overline{x} \cdot z) + (\overline{x} \cdot \overline{z} \cdot y + \overline{x} \cdot \overline{z} \cdot \overline{y}) \\ &= \big(\overline{x} \cdot \overline{y} \cdot (z + \overline{z}) \ + \ \overline{x} \cdot z \cdot (y + \overline{y})\big) + (\overline{x} \cdot \overline{z} \cdot y \ + \ \overline{x} \cdot \overline{z} \cdot \overline{y}) \\ &= \overline{x} \cdot \overline{y} \cdot z + \overline{x} \cdot \overline{y} \cdot \overline{z} + \overline{x} \cdot y \cdot z + \overline{x} \cdot y \cdot \overline{z}. \end{aligned}$$

Alternativt kan en forma värdetabellen för f och härleda uttrycket från denna.

Namn	poäng uppg.5

5) (3p) Betrakta primtalen $p = 5$, $q = 7$. Konstruera ett RSA-krypto med $n = pq$ sådan att krypteringsnyckeln e, med $e > 1$, också fungerar som dekrypteringsnyckel.
OBS. En komplett lösning med fullständiga motiveringar skall ges.

Lösning: Vi har den offentliga modulon

$$n = 5 \cdot 7 = 35$$

och den privata

$$m = 4 \cdot 6 = 24.$$

Vi vill hitta $e > 1$ med $\gcd(e, m) = 1$ sådan att dekrypteringsnyckeln d är lika med e. I allmänhet är d den multiplikativa inversen till e modulo m, dvs lösningen till $ed \equiv 1 \pmod{m}$, så vi vill hitta e sådan att

$$e^2 \equiv 1 \pmod{24}.$$

$e = 5$ är en uppenbar lösning, men även $e = 7$, 11, 13$(= 24-11)$, 17$(= 24-7)$, 19$(= 24-5)$ och 23$(= 24-1)$ fungerar.

Svar: $e = 5$.