Svar och lösningsförslag till extra-ks4, 23 maj 2007,
i 5B1118 Diskret matematik för CL2, CL3 och Media1

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.)

		sant	**falskt**
a)	Ett RSA-krypto kan ha parametrarna $n = 46$ och $e = 2$. Nej, $n = 46 = 2 \cdot 23$ ger $m = 1 \cdot 22 = 22$ och $\text{sgd}(22, 2) \neq 1$.		X
b)	Ett RSA-krypto kan ha $d = 5$ och $e = 5$. Ja, $n = 35 = 5 \cdot 7$ ger $m = 4 \cdot 6 = 24$ och $5 \cdot 5 \equiv 1 \pmod{24}$.	X	
c)	Om kolonnerna i matrisen H, med ettor och nollor, är olika så är H en kontrollmatris till en 1-felsrättande kod. Nej, inte säkert. De måste vara nollskilda.		X
d)	Om C är en 1-felsrättande kod av längd 7 med 8 ord så har C en kontrollmatris H med 3 rader. Nej, 4 rader krävs ($8 = 2^3$, $7 - 3 = 4$).		X
e)	Det finns precis 8 booleska funktioner i de tre variablerna x, y och z. Nej, men 2^8.		X
f)	I en boolesk algebra B gäller alltid att $x + xy = x$ för alla $x, y \in B$. Ja, $x + xy = x(1 + y) = x \cdot 1 = x$.	X	

2a) (1p) Du använder en 1-felsrättande kod med kontrollmatrisen

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

Du tar emot meddelandet 111111. Om ordet går att rätta skall du rätta det. Om det inte går att rätta skall du skriva att ordet inte går att rätta.

Lösning:

$H(111111)^T = (010)^T$, som inte är en kolonn i H, så ordet måste ha mer än ett fel. (Man ser att det kan vara fel i positionerna 1,2, i 3,6 eller i 4,5.)
Svar: Ordet går inte att rätta.

---

b) (1p) Ange en minimal disjunktiv form för nedanstående booleska funktion i de tre variablerna x, y och z: $f(x, y, z) = xyz + xy\bar{z} + x\bar{y}z$.

Lösning:

Med ett karnaughdiagram finner man den (i detta fall entydiga) minimala disjunktiva formen. $f(x, y, z) = xyz + xy\bar{z} + x\bar{y}z = xyz + xyz + xy\bar{z} + x\bar{y}z = xy(z + \bar{z}) + xz(y + \bar{y}) = xy \cdot 1 + xz \cdot 1 = xy + xz$.
Svar: Minimal disjunktiv form är $f(x, y, z) = xy + xz$.

---

c) (1p) Du vill ha ett RSA-krypto med parametern $n = 65$. Ange ett möjligt värde på parametern e.

Lösning:

$n = 65 = 5 \cdot 13$ ger $m = 4 \cdot 12$. Kravet på e är $\text{sgd}(m, e) = 1$, så t.ex. $e = 5$ går bra. **Svar: T.ex. $e = 5$ fungerar.**

---

3) (3p) Skriv följande booleska funktion, i de tre variablerna x, y och z, på en disjunktiv normalform: $f(x,y,z) = (xy + \overline{(x+y)})z$.

Lösning:

Eftersom $\overline{(x+y)} = \bar{x} \cdot \bar{y}$, får man $f(x,y,z) = (xy + \overline{(x+y)})z = (xy + \bar{x}\bar{y})z = xyz + \bar{x}\bar{y}z$, vilket är en disjunktiv normalform (en summa av produkter, där varje produkt innehåller precis en av v och $\bar{v}$ för varje variabel $v = x, y, z$).
Svar: $\boldsymbol{f(x,y,z) = xyz + \bar{x}\bar{y}z}$, en disjunktiv normalform.

---

4) (3p) Ett RSA-krypto har de offentliga nycklarna $n = 39$ och $e = 11$. Bestäm parametern d och ange hur hur meddelande 2 kan dekrypteras, dvs ange hur $D(2)$ beräknas.
(Du behöver alltså inte beräkna $D(2)$ för att få full poäng på denna uppgift men du skall berätta hur man går till väga.)

Lösning:

$n = 39 = 3 \cdot 13$ ger $m = 2 \cdot 12 = 24$. d bestäms av att $e \cdot d \equiv 1 \pmod{m}$.
Man finner d (genom inspektion eller) med Euklides algoritm:

$$\begin{array}{ll} 24 = 2 \cdot 11 + 2 & 1 = 11 - 5 \cdot 2 = 11 - 5(24 - 2 \cdot 11) = \\ 11 = 5 \cdot 2 + 1 & \quad = -5 \cdot 24 + 11 \cdot 11, \end{array}$$

så $d = 11$ och $D(2) = 2^{11}$ i Z_n (dvs $0 \leq D(2) < 39$ och $D(2) \equiv 2^{11} \pmod{n}$).
Svar: $\boldsymbol{d = 11}$ och $\boldsymbol{D(2) = 2^{11}}$ i $\boldsymbol{Z_{39}}$ (så $\boldsymbol{D(2) = 20}$).

---

5) (3p) Bestäm en kontrollmatris till en 1-felsrättande kod C av längd 7 och som innehåller 16 ord och som är sådan att ordet 1011000 tillhör koden C.

Lösning:

Eftersom koden skall innehålla $16 = 2^4$ ord, är dess dimension 4 och kontrollmatrisen H skall ha rang $7 - 4 = 3$, dvs 3 linjärt oberoende rader. 7 stycken olika och nollskilda kolonner, så alla möjliga kolonner skall vara med (en hammingkod). Villkoret att ordet 1011000 tillhör C betyder att kolonnerna 1,3 och 4 skall ha summa noll.
Man kan t.ex. ta dem som $(100)^T, (010)^T, (110)^T$ och fylla på övriga kolonner skilda från varandra. Många olika svar är alltså möjliga.

Svar: T.ex. $\boldsymbol{H} = \begin{bmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} \end{bmatrix}$
