Svar och lösningsförslag till ks4, 3 maj 2010,
i SF1610(/5B1118) Diskret matematik för CL

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)	Om alla kodord utom $00\ldots0$ i en binär, linjär kod innehåller minst tre 1:or, rättar koden minst ett fel. [Ja, då är ju minimala vikten ≥ 3.]	X	
b)	Om kontrollmatrisen H för en binär, linjär kod är av typ 3×8, finns minst ett fel som koden inte kan rätta. [Ja, antingen en 0-kolonn eller två lika, så minimala vikten < 3.]	X	
c)	$35^{2010} \equiv 3 \pmod{11}$. [Nej, Fermats lilla sats ger $35^{10} \equiv 1 \pmod{11}$, så $35^{2010} \equiv 1 \pmod{11}$.]		X
d)	Om p och q är olika primtal, $n = p \cdot q$, $m = (p-1)(q-1)$ och $s \equiv 1 \pmod{n}$ så är säkert $x^s \equiv x \pmod{m}$. [Nej, $s \equiv 1 \pmod{m}$ ger $x^s \equiv x \pmod{n}$. Motex $p = 3$, $q = 5$, $x = 2$.]		X
e)	Den booleska funktionen $f(x, y, z) = x\bar{y} + y\bar{z}$ är given på disjunktiv normalform. [Nej, i dnf ingår varje variabel i varje term.]		X
f)	$(q \to p) \wedge (p \to \neg\, q) \equiv p$ gäller för alla satslogiska sentenser p och q. ('$\equiv$' betecknar logisk ekvivalens). [Nej. $(q \to p) \wedge (p \to \neg\, q) \equiv \neg\, q$. Sanningsvärdestabell t.ex.]		X

2a) (1p) Man vill skapa en binär kod (inte säkert linjär) av längd 13 som rättar två fel. Vi söker en övre gräns för antalet ord i koden.

Lösning:

Sfärpackningssatsen ger $|\mathcal{C}| \left(\binom{13}{0} + \binom{13}{1} + \binom{13}{2} \right) \leq 2^{13}$, så
Svar: $|\mathcal{C}| \leq \frac{2^{13}}{1+13+78}$ (så $|\mathcal{C}| \leq 89$).

---

b) (1p) A och B har krypteringssystem med offentliga E_A och E_B och hemliga D_A och D_B. B vill skicka A meddelandet $\boldsymbol{x}$, så att ingen obehörig kan läsa det och A kan vara säker på att det kommer från B. Hur kan han göra?

Lösning:

Elektronisk signatur. $D_B(E_A(x))$ (eller $E_A(D_B(x))$) kan bara B skriva (pga D_B) och bara A läsa (med E_B och D_A).
Svar: Han kan skicka $\boldsymbol{D_B(E_A(x))}$ eller $\boldsymbol{E_A(D_B(x))}$.

---

c) (1p) "Om det regnar eller det är natt (eller båda), så är det inte en juninatt" skall översättas till satslogik, med beteckningar
A: "det regnar", B: "det är natt", C: "det är juni".

Lösning:

Man får "Om A eller B (eller båda), så gäller inte både B och C", så
Svar: $\boldsymbol{A \vee B \to \neg(B \wedge C)}$.

---

3) En binär, linjär kod $\mathcal{C}$ av längd $n = 5$ skall definieras av kontrollmatrisen (i boken: checkmatrisen) H med 3 rader.

a) (2p) Ange en möjlig matris H om $\mathcal{C}$ skall rätta ett fel och orden 11010 och 01101 båda skall vara kodord i $\mathcal{C}$.

Lösning:

$\mathcal{C}$ skall rätta ett fel, så alla H:s kolonner skall vara olika och skilda från $(000)^T$. 11010 är ett kodord, så summan av kolonnerna 1, 2 och 4 är $(000)^T$, vi kan t.ex. ta dem som $(100)^T$, $(010)^T$ och $(110)^T$. Pss ger kodordet 01101 att kolonnerna 2, 3 och5 kan vara $(010)^T$, $(001)^T$ och $(011)^T$.
Svar: En möjlig kontrollmatris (det finns fler) är $\mathbf{H} = \begin{pmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} \end{pmatrix}$**.**

---

b) (1p) Om man med H från a) tar emot ordet **10101** och högst ett fel har uppstått, vilket var det sända kodordet?

Lösning:

$H(10101)^T = (110)^T$, som är H:s fjärde kolonn, så det är fel i position 4.
Svar: Det sända ordet var 10111 (oberoende av valet av H).

---

4) (3p) För ett (litet) RSA-system har man valt den offentliga parametern $n = 221 (= 13 \cdot 17)$.

a) (1p) Man tar den offentliga krypteringsexponenten e till det minsta möjliga värde som är ≥ 20. Vad blir e?

Lösning:

$n = 13 \cdot 17$ ger $m = 12 \cdot 16 = 192 = 2^6 \cdot 3$. $\text{sgd}(m, e) = 1$ ger det minsta ≥ 20:
Svar: Den sökta krypteringsexponenten är $e = 23$.

---

b) (2p) Vad blir motsvarande hemliga avkrypteringsexponent d?

Lösning:

d fungerar omm $ed \equiv 1 \pmod{m}$. Euklides algoritm:
$192 = 8 \cdot 23 + 8$, $23 = 2 \cdot 8 + 7$, $8 = 1 \cdot 7 + 1$ och $1 = 8 - 7 = 8 - (23 - 2 \cdot 8) = -23 + 3 \cdot 8 = -23 + 3(192 - 8 \cdot 23) = 3 \cdot 192 - 25 \cdot 23 = (3 - 23)192 + (192 - 25)23 = -20 \cdot 192 + 167 \cdot 23$, så
Svar: Den sökta avkrypteringsexponenten är $d = 167$.

---

5) (3p) Uttryck den booleska funktionen $f(x, y, z, w) =$
$xyzw + \bar{x}yz\bar{w} + \bar{x}\bar{y}\bar{z}w + x\bar{y}\bar{z}w + \bar{x}y\bar{z}\bar{w} + xyz\bar{w} + \bar{x}\bar{y}zw + xy\bar{z}\bar{w} + x\bar{y}zw + xy\bar{z}w$
på **minimal disjunktiv form**, dvs disjunktiv form med så få '$\cdot$' och '+' som möjligt. ('$\cdot$' skall förstås räknas även när de underförstås.)

Lösning:

Uttrycket för f ger karnaughdiagrammet härintill.
Genom att, som i fig., täcka 1:orna med så stora rektanglar som möjligt med sidlängder 1, 2 eller 4, får vi att $f(x, y, z, w)$ är lika med $xy + y\bar{w} + \bar{y}w$.
Alternativt kan xy-rektangeln ersättas med en xw-.
Svar: Uttrycket blir
$\boldsymbol{f(x, y, z, w) = xy + y\bar{w} + \bar{y}w = xw + y\bar{w} + \bar{y}w}$.

xy \ zw	00	01	11	10
00	0	1	1	0
01	1	0	0	1
11	1	1	1	1
10	0	1	1	0