Skrivningskod: Glöm den inte!

Om du vill: Lägg till tre bokstäver.

KTH Matematik
Olof Heden

Σ p	G/U	bonus

Efternamn	förnamn	pnr	årskurs

Lósning till kontrollskrivning 4A, 4 oktober 2011, 10.45–11.45, i SF1610 Diskret matematik för CINTE.

Inga hjälpmedel tillåtna.
Minst 8 poäng ger godkänt.
Godkänd ks 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)	I varje RSA-krypto med parametrarna n, e, m och d kan n vara lika med 56.		x
b)	I ett RSA-krypto med parametrarna n, e, m och d kan m vara ett primtal.		x
c)	En kontrollmatris till en 1-felsrättande kod kan ha 4 rader och 13 kolonner.	x	
d)	Koden $C = \{00000, 11111\}$ är 2-felsrättande.	x	
e)	Antalet ord i en 1-felsrättande kod är alltid lika med 2^n för något heltal n.		x
f)	Om för elementen x och y i en Boolesk algebra gäller att $x + y = xy$ så måste $x = y$.	x	

poäng uppg.1

Namn	poäng uppg.2

2a) (1p) Ett RSA-krypto har $n = 21$. Ange samtliga möjliga värden på den krypterande parametern e som vi kan välja i intervallet $1 < e < 10$.

SVAR: 5 eller 7.

b) (1p) Låt den Booleska funktionen $f(x, y, z)$ i de tre variablerna x, y och z definieras genom

$$f(x, y, z) = (x + y)\bar{z} + \bar{x}(y + \bar{z})\overline{(\bar{y} + z)} + y(\bar{x} + z(\bar{y} + \bar{x})) \; .$$

SVAR: 0.

c) (1p) Betrakta en felkorrigerande kod C med kontrollmatrisen

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix} \; .$$

Rätta ordet 1100101.

SVAR: 0100101.

Namn	poäng uppg.3

3) (3p) Ett RSA-krypto har parametrarna $n = 91$ och $e = 31$. Dekryptera meddelandet $b = 2$, dvs bestäm $D(2)$.

Lösning: Då $n = 7 \cdot 13$ så är $m = (7-1) \cdot (13-1) = 72$ och vi söker då en dekrypteringsnyckel d sådan att $e \cdot d \equiv 1 \pmod{72}$ med hjälp av Euklides algoritm:

$$\begin{aligned} 72 &= 2 \cdot 31 + 10 \\ 31 &= 3 \cdot 10 + 1 \end{aligned}$$

varur följer att

$$1 = 31 - 3 \cdot 10 = 31 - 3(72 - 2 \cdot 31) = 7 \cdot 31 - 3 \cdot 72 \, .$$

Således är $31 \cdot 7 \equiv 1 \pmod{72}$ och vi finner att $d = 7$ varur

SVAR: $D(2) = 2^7 \pmod{91} = 37$.

Namn	poäng uppg.4

4) (3p) En 1-felsrättande kod C har kontrollmatrisen (parity check-matrisen)

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

Bestäm antalet ord som C inte kan rätta.

Lösning: Antalet ord i koden är 2^{n-r} där n betecknar antalet kolonner (ordlängden) och r antalet rader (egentligen rangen hos matrisen), så $|C| = 2^{10-4} = 64$. Antalet ord som ligger på ,avståndet ett från ett kodord är lika med antalet möjliga positioner som går att ändra, dvs 10. Vi kan anta att ett kodord själv inte räknas med bland de ord som inte går att rätta. Eftersom det finns totalt $2^{10} = 1024$ ord av längd 10, och inget ord ligger på avstånd ett från två kodord, så får vi

SVAR: $1024 - 64 \cdot 11 = 320$.

Namn	poäng uppg.5

5) (3p) Bestäm antalet Booleska funktioner $f(x, y, z, w, u)$ som har egenskapen att

$$f(x, y, z, w, u) = f(x, \bar{y}, \bar{z}, \bar{w}, u)$$

för alla x, y, z, w och u i $\mathcal{B} = \{0, 1\}$

Lösning: Till varje element i definitionsmängden finns alltid två möjliga funktionsvärden, nämligen 1 och 0. Eftersom vi kräver att funktionsvärdet i "punkten" (x, y, z, w, u) är lika med funktionsvärdet i punkten $(x, \bar{y}, \bar{z}, \bar{w}, u)$ så har vi för varje givet funktionsvärde $f(x, y, z, w, u)$ automatiskt också funktionsvärdet $f(x, \bar{y}, \bar{z}, \bar{w}, u)$. Likaledes har vi för varje givet funktionsvärde $f(x, \bar{y}, \bar{z}, \bar{w}, u)$ automatiskt också funktionsvärdet $f(x, \bar{\bar{y}}, \bar{\bar{z}}, \bar{\bar{w}}, u)$ som ju är lika med $f(x, y, z, w, u)$ eftersom generellt gäller att $\bar{\bar{a}} = a$ för alla element a i en Boolesk algebra. Elementen i definitionsmängden paras alltså ihop genom relationen

$$(x, y, z, w, u) \qquad \longleftrightarrow \qquad (x, \bar{y}, \bar{z}, \bar{w}, u) \ ,$$

och funktionsvärdet är detsamma för de bägge elementen i ett par.

Eftersom det finns totalt $2^5 = 32$ "punkter" i definitionsmängden så finns det 16 par av punkter, och det finns två möjliga funktionsvärden för elementen i paret, så multiplikationsprincipen ger

SVAR: 2^{16} olika Booleska funktioner.