Skrivningskod: Glöm den inte!

Om du vill: Lägg till tre bokstäver.

KTH Matematik
Olof Heden

Σ p	G/U	bonus

Efternamn	förnamn	pnr	årskurs

Kontrollskrivning 4B, 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 57.		
b)	En kontrollmatris till en 1-felsrättande kod kan ha 4 rader och 9 kolonner.		
c)	I ett RSA-krypto med parametrarna n, e, m och d kan m vara ett primtal.		
d)	Koden $C = \{00000, 11111\}$ är 2-felsrättande.		
e)	Om för elementen x och y i en Boolesk algebra gäller att $x + y = xy$ så måste $x = y$.		
f)	Antalet ord i en 1-felsrättande kod är alltid lika med 2^n för något heltal n.		

poäng uppg.1

Namn	poäng uppg.2

2a) (1p) Låt den Booleska funktionen $f(x, y, z)$ i de tre variablerna x, y och z definieras genom

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

Bestäm $f(1, 0, 1)$.

b) (1p) Ett RSA-krypto har $n = 33$. Ange samtliga möjliga värden på den krypterande parametern e som vi kan välja i intervallet $1 < e < 12$.

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 1000110.

Namn	poäng uppg.3

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

Namn	poäng uppg.4

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

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

Bestäm antalet ord som C inte kan rätta.

Namn	poäng uppg.5

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

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

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