KTH Matematik

Kontrollskrivning 5
5B1118 Diskret Matematik
9 maj, 2006

- tid:**10:15-11:15**
- Tillåtna hjälpmedel: Miniräknare. Inga böker/anteckningar får användas.
- **Allt ska motiveras.** Ett svar utan förklaring är värd 0 poäng!
- Minst 3 poäng krävs för godkänt.

(1) (3 p.)
   (a) Ge ett exempel av en bipartit graf $(X \cup Y, E)$, med $|X| \geq |Y| \geq 4$, som inte har en komplett matching (förklara varfr!).
   (b) Hitta en maximal matching av en sådan graf G.

(2) (3 p.) Kryptera ordet SECURE och dekryptera ordet JVTTBUPJHAPVU, med ett Cearser-Chiffer kryptosystem (E_b, D_b), där $b = 7$.

Låt $\mathbb{Z}_{26}$ motsvara den engelska alfabetet, $A = 0, ..., Z = 25$. Låt $E_7 : \mathbb{Z}_{26} \to \mathbb{Z}_{26}, E_7(x) = x + 7 \; mod \, 26$, och $D_7 : \mathbb{Z}_{26} \to \mathbb{Z}_{26}, D_7(y) = y - 7 \; mod \, 26$.

Då är: $E_7(SECURE) = ZLJBYL$ och

$D_7(JVTTBUPJHAPVU) = COMMUNICATION.$

(3) (3 p.) Antag given ett RSA-system med kripteringsnyckel $n = 143$ och $e = 7$.
   (a) Bestäm dekripteringstalet d. $143 = 13 \cdot 11, m = 12 \cdot 10 = 120$. Då är d inversen av 7 mod 120. det finns eftersom $(7, 120) = 1$. Från $1 = 120 - 7 \cdot 17$ ser man att $d = -17 = 103$ mod 120.

(b) Kryptera meddelandet 5. $E(5) = 5^7 \bmod 143$. $5^4 = 53 \bmod 143$, $5^7 = 53 \cdot 25 \cdot 5 = 6625 = 47 \bmod 143$.

(c) Dekryptera resultatet. $D(47) = 47^{103}$, $103 = 64 + 32 + 4 + 2 + 1$.

$$47^{103} = 47^{64}47^{32}47^{4}47^{2}47.$$

$47^2 = 2209 = 64 \bmod 143$, $47^4 = 92.mod143$, $47^8 = 27 \bmod 143$, $47^{16} = 14 \bmod 143$, $47^{32} = 53 \bmod 143$, $47^{64} = 92 \bmod 143$.

$47^{103} = 92 \cdot 53 \cdot 92 \cdot 64 \cdot 47 = 5\ mod\ 143$