Matematiska Institutionen
KTH

Lappskrivning nr 6, variant A, på kursen Diskret matematik, 5B1118, för Media1, onsdagen den 11 maj 2005 kl 13.15-14.00.

Namn:

Resultat:

Vardera uppgift ger 3 poäng för korrekt lösning, för godkänt krävs 5 poäng (vilket ger att uppgift nummer 6 på tentamensskrivningen räknas som godkänd med tre poäng. Detta gäller ordinarie tentamenstillfället och de två följande omtentamina).

OBS Svaren skall motiveras och lösningarna skrivas på detta pappers fram- och baksida. Inga hjälpmedel är tillåtna.

1. En 1-felsrättande kod C har checkmatrisen (eller kontrollmatrisen)

$$H = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

   Av följande tre ord ligger ett i koden, ett på avståndet ett från ett av kodorden, och ett som så att säga inte går att rätta, dvs på ett avstånd större än ett från alla kodord. Orden är 111111, 111110, 101100.

   a) Vilket ord tillhör koden?

   b) Vilket ord tillhör inte koden men går att rätta. Bestäm också det rättade ordet.

   c) Vilket ord går inte att rätta?

2. Ett RSA krypto har $n = 39$. Välj parametern e själv och dekryptera sedan meddelandet 2. **Obs.** Du skall *dekryptera* meddelandet 2.

3. Betrakta permutationerna $\varphi = (1\ 4\ 6\ 3)(2\ 5)$ och $\psi = (1\ 3\ 6)(4\ 2\ 5)$.

   a) Bestäm ordningen av φ.

   b) Bestäm ordningen av $\varphi\psi$.

   c) Vilka av permutationerna φ, ψ och $\varphi\psi$ är jämna?