Matematiska Institutionen
KTH

Lösning till lappskrivning nr 6, variant A, på kursen Diskret matematik, 5B1118, för Media1, onsdagen den 11 maj 2005.

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?

   Lösning. a) $c = 101100$ tillhör koden eftersom $Hc^T = 0$.

   b) $c = 111110$ går att rätta eftersom Hc^T är lika med kolonn nummer tre i H. Det rättade ordet blir då 110110.

   c) $c = 111111$ går inte att rätta eftersom Hc^T inte blir någon av H:s kolonner.

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

   Lösning. $n = 39$ ger att $p = 3$ och $q = 13$ och därmed att $m = (p-1)(q-1) = 24$. Vi väljer t ex $d = 5$ ty då har d en invers e. Dekrypteringen av 2 blir d8a

$$D(2) \equiv_{39} 2^5 = 32.$$

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?

   Lösning. a) Ordningen är fyra eftersom minsta gemensamma multipeln till de bägge cykellängderna 4 och 2 är just 4.

   b) Beräknar först $\varphi\psi = (1)(2)(3)(4\ 5\ 6)$ som ju har ordning tre.

   c) Varje k-cykel kan skrivas som en produkt av $k-1$ stycken transpositioner. Vi får alltså φ är en produkt av t ex 4 transpositioner, ψ av fyra transpositioner och $\varphi\psi$ en produkt av 2 transpositioner. Så svar alla de givna permutationerna är jämna.