Matematiska Institutionen,
KTH

Några repetitionsproblem på del 4 av kursen Diskret matematik, SF1610, CINTE1, vt14. Dessa problem diskutera den 6/5, de sista 20 minuterna av föreläsningen.

OBS Uppgifterna på KSen är typ E-uppgifter utom uppgift 5 som ibland kan vara en typ D- eller C-uppgift.

1. (E) Ett RSA-krypto har $n = 77$ och $e = 11$. Dekryptera meddelandet $b = 2$.

2. (C) Bestäm kontrollmatrisen $\mathbf{H}$ till en 1-felsrättande kod C sådan att ordet 1111000000 tillhör C men också sådan att ordet 1111111111 inte går att rätta. Bestäm också sannolikheten att ett godtyckligt ord av längd 10 går att rätta med hjälp av kontrollmatrisen $\mathbf{H}$.

3. (D) Undersök om det finns Booleska funktioner g och h i de tre variablerna x, y och z sådana att

$$zx + z\bar{y} + x\bar{y} + g = \bar{y}, \qquad (zx + z\bar{y} + x\bar{y})h = \bar{y}.$$