KTH CSC, Linda Kann

DD1320/1325 DIAGNOSTISKT PROV I TILLÄMPAD DATALOGI

Fredag 7 oktober 2016

Det här är exempel på C-uppgifter. I betygskriterierna för betyg C ingår att "kunna jämföra algoritmer och datastrukturer och bedöma dessas lämplighet för ett givet problem". C-delen kan höja tentabetyget till D eller C, se mer info under Tenta på kurswebbsidan.

1. *Koda kort*

Betyg C. Följande tre uppsättningar av koder är tänkta att använda för komprimering. Vilka fungerar för komprimering? Vilken är effektivast? Motivera ditt svar!

(20 min)

	kod1
E	11
A	10
N	011
R	010
T	001
S	0001
I	0000

kod2
111
101
100
011
010
001
000

kod3
10
11
110
101
111
0100
0111

2. *Kryptering*

Betyg C. One-time pad är en krypteringsmetod som fungerar så här:
Givet ett meddelande på binär form

- Slumpa fram en nyckel med lika många binära siffror som meddelandet har
- Gör bitvis *xor* mellan meddelandet och nyckeln

Att ta *xor* med samma nyckel på det krypterade meddelandet avkodar. Exempel:

```
meddelande = 100111
slumpad nyckel = 100101
Kryptering: 100111 xor 100101 = 000010
Dekryptering: 000010 xor 100101 = 100111
```

Gör en jämförelse mellan one-time pad och RSA ur tre relevanta aspekter.

(20 min)