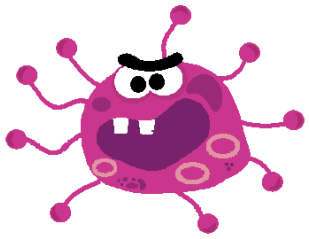
KTH EECS, Sten Andersson, Alexander Baltatzis



DD1320
TENTAMEN I TILLÄMPAD DATALOGI
Onsdag 11 mars kl 14–18

Hjälpmedel: Egenskrivet formelblad, max 4 sidor (eller två dubbelsidiga A4). För betyg E krävs att alla E-uppgifter är godkända (upp till två E-uppgifter kan kompletteras). För betyg D respektive C krävs (utöver E-kraven) D respektive C på C-uppgiften. För betyg B respektive A krävs (utöver C-kraven) betyg B respektive A på A-uppgiften. Lycka till!

E 1. *KMP*

Vi söker efter virala virus som virvlar omkring i världen.

15 min Rita en KMP-automat för ordet *VIRALAVIRVELVIRUS* samt ange next-vektorn.

E 2. *Bubbelsortering*

15 min

a) Följande sex tal ska sorteras i stigande ordning med bubbelsortering. Visa i vilken ordning talen ligger för varje varv i sorteringen.

```
8, 1, 7, 9, 2, 4
```

b) Hur många varv kommer bubbelsorteringen att köra för detta exempel? Motivera kort.

E 3. *Graf*

En vanligt mekanism för uppkomst av nya virus är genom "Cross-species transmission"(CST) där en art överför ett virus till en annan. Givet nedan är några förekommande sådana där en riskfaktor (1-3, lågt till högt) anges.

```
Råtta -> Fladdermus (3)
Råtta -> Människa (2)
Råtta -> Hund (1)
Råtta -> Katt (1)
Fladdermus -> Människa (2)
Fladdermus -> Hund (3)
Hund -> Katt (1)
Hund -> Människa (2)
Katt -> Människa (1)
Katt -> Hund(1)
```

15 min

a) Rita en graf (med hörn och kanter) som beskriver dessa överföringar.

b) Hur många hörn har grafen?

c) Hur många kanter har grafen?

E 4. *Kryptering*

Du behöver skicka ett meddelande till Dr Mildred Who men denne är rädd för att det kan innehålla virus eller bli infekterat på vägen. Du bestämmer dig därför för att använda kryptering och verifiering med RSA.

Det okodade meddelandet ligger i variabeln `message`.

Du har tillgång till funktionen `rsa` som tar en nyckel och en text och returnerar en kodad text. Nu vill du skriva ett program för att skicka `message`.

10 min *Vilket eller vilka* av alternativen nedan kan du använda för att skicka meddelandet så att enbart Dr Who kan dekryptera det och vara säker på att det är du som skickat det.

a)
```
text2 = rsa ( MinPrivataNyckel, message )
text3 = rsa ( DrWhoPrivataNyckel, text2 )
mail ( "DrMildredWho@who.org", text3 )
```

b)
```
text2 = rsa ( MinPublikaNyckel, message )
text3 = rsa ( DrWhoPublikaNyckel, text2 )
mail ( "DrMildredWho@who.org", text3 )
```

c)
```
text2 = rsa ( MinPrivataNyckel, message )
text3 = rsa ( DrWhoPublikaNyckel, text2 )
mail ( "DrMildredWho@who.org", text3 )
```

d)
```
text2 = rsa ( MinPublikaNyckel, message )
text3 = rsa ( DrWhoPrivataNyckel, text2 )
mail ( "DrMildredWho@who.org", text3 )
```

e)
```
text2 = rsa ( DrWhoPublikaNyckel, message )
text3 = rsa ( MinPrivataNyckel, text2 )
mail ( "DrMildredWho@who.org", text3 )
```

E 5. *Heap*

För att rangordna olika hotbilder mot grundläggande samhällsfunktioner (t e x cyberattacker, miljökatastrofer eller pandemier) använder myndigheten för samhällsskydd och beredskap (MSB) sig av en max-heap där varje potentiell samhällsfara har en riskfaktor (0-10, låg till hög). I kronologisk ordning inträffar följande sex händelser som ska läggas in i denna heap.

10 min Rita detta steg för steg (det räcker att du anger riskfaktorn). Du kan välja mellan att rita heapen på trädform eller på vektorform.

```
Generaldirektörens guldfisk dör: 0
Jordbävning: 1
Zombieapokalyps: 2
Pandemi: 6
Mello lägger ner: 7
Soleruption: 3
```

E 6. *Komprimering och felkorrigering*

10 min

Ett s k DNA-virus innehåller genetiska sekvenser med nukleotiderna adenin (A), guanin (G), cytosin (C) och tymin (T) vilket skrives t ex CGCCTATACGGA. I en databas med över 10^{12} genetiska sekvenser lagras de *fyra* tecknen CGAT med ASCII-kod som kräver sju bitar per tecken. För att spara plats vill man istället lagra på kompaktast möjliga vis. Vi förutsätter här att varje nukleotid är *lika vanligt förekommande*.

a) Hur skulle kunna denna kodning kunna se ut? Visa med ett exempel.

b) För att upptäcka bitfel vid läsning av sekvenser vill man feldetektera med en *paritetsbit*. Förklara hur detta skulle kunna gå till, och visa med ett exempel.

Motivera dina svar!

C 7. *Bloomfilter*

Ett antal viruspatienter har satts i karantän. Karantänen för den enskilde varar som mest i 14 dagar och man är beredd på en hög omsättning patienter. Det finns ett maxtak på hur många patienter man kan husera samtidigt. Man vet inte hur länge epidemin varar.

Viruspatienterna behöver tillfälliga personliga lösenord. För att inte lagra lösenorden i klartext så tänker man använda bloomfilter.

Valet står mellan att lagra lösenorden i ett *bloomfilter* eller *hashade och saltade*.

25 min Jämför dessa två alternativ. Var noga med att motivera dina slutsatser med hänvisning till de givna förutsättningarna.

A 8. *Binära träd*

Givet ett binärt sökträd som innehåller heltal.

a) Konstruera en effektiv algoritm som givet (1) en pekare till ett binärt sökträd och (2) en sökt summa, returnerar två nodpekare. Summan av värdena i de två noderna ska bli den sökta summan. Om det inte går att hitta två sådana noder så ska *None, None* returneras.

25 min Algoritmen och datastrukturer ska vara tydligt beskrivna.

b) Ange komplexitet för din algoritm.

c) Visa hur din algoritm fungerar om man söker efter summan 10 i trädet p nedan.

d) Visa hur din algoritm fungerar om man söker efter summan 10 i trädet q nedan.