DD2448
Andreas Tarandi
890416-0317

Homework I

May 31, 2012
Ingen studiegrupp

1 Skiffer

1.1 Program

De programmen som jag har skrivit för denna uppgift är följande (i bokstavsordning). Samtliga ruby-program är skrivna för ruby 1.9.2.

- **coincidence.rb**
  Beräknar index of coincidence i given fil med varierande nyckellängd och kan även per rad testa alla kombinationer av nycklar per tecken i nyckeln och därmed beräkna hur nära texten i raden ligger engelska. Genom detta kan den även föreslå en nyckel.
  Använder filen "english.rb" som innehåller sannolikhetsfördelningen av tecken i vanlig engelska.
  Kräver gemet "colorize"
- **decrypt.rb**
  Avkrypterar given fil med given nyckel (av längd n)
- **freq.cpp**
  Utför frekvensanalys på given fil och beräknar statistik och ritar histogram
- **hex_to_ascii.rb**
  Tar par av nummer från indata och tolkar som ascii och testar därefter att skifta texten med alla nummer i en given mängd.
- **kasiki.cpp**
  Räknar avstånd mellan återkommande textsegment av längd tre och sparar avstånd och antal förkomster av avståndet.

1.2 Skiffer A

1.2.1 Metod

Det första steget var att utföra frekvensanalys på skiffertexten. För detta använde jag programmet freq.cpp för att ta fram både siffror och histogram på frekvensen av tecken, bigram och trigram.

Vid en första anblick av resultatet av frekvensanalysen ser man att W är klart vanligast. Dessutom ser man på fördelningen över tecknena att det tycks vara ett monoalfabetiskt substitutionsskiffer.

E är visserligen den vanligaste bokstaven i engelska språket, men vid en analys av hur W är utplacerat i texten ser man snabbt att W är mellanrum.

Jag ersatte därmed samtliga W i texten med mellanrum och körde frekvensanalysen ytterligare en gång. Härefter studerade jag frekvensen av tecken, bigram och trigram och pusslade mig fram till klartexten genom att hitta skiffer-klartext-kopplingen bokstav för bokstav, givetvis med start i de vanligaste tecknena och slut i de ovanligaste.

1.2.2 Klartext

helga spake never shall i weep therefor quoth she ye have evilly beguiled me and gunnlaug has surely come out and therewith she wept much

but a little after gunnlaugs coming was bruited about and helga became so hard with raven that he could not keep her at home at mossfell so that back they had to go to burg and raven got small share of her company

now men get ready for the winterwedding thorkel of skaney bade illugi the black and his sons but when master illugi got ready gunnlaug sat in the hall and stirred not to go illugi went up to him and said why dost thou not get ready kinsman

gunnlaug answered i have no mind to go

says illugi nay but certes thou shalt go kinsman says he and cast thou not grief over thee by yearning for one woman make as if thou knewest nought of it for women thou wilt never lack

now gunnlaug did as his father bade him so they came to the wedding and illugi and his sons were set down in the high seat but thorstein egilson and raven his soninlaw and the bridegrooms following were set in the other high seat over against illugi

the women sat on the dais and helga the fair sat next to the bride oft she turned her eyes on gunnlaug thereby proving the saw eyes will betray if maid love man

1.3 Skiffer B

1.3.1 Metod

Började åter igen med frekvensanalys (freq.cpp), men kunde utifrån den se att distributionen över alfabetet var för jämn, vilket tydde på ett polyalfabetiskt skiffer, med stor sannolikhet Vigenères skiffer.

Jag körde därmed kasiki.cpp och hittade att avstånden 18, 36 och 54 alla förkom relativt ofta. Deras gemensamma nämnare är 18, och alltså gissade jag på att detta var nyckellängden m.

För att verifiera detta körde jag först coincidence.rb med nyckellängder 1 till 18 utan att testa nyckelkombinationer (calc_prob_distribution = false i koden). Med detta kunde jag verifiera att siffrorna för nyckellängd 18 låg närmast 0.068 (värdet för engelsk text). Koden beräknar index of coincidence enligt följande formel (från kursboken):

$$I_c(x) = \frac{\sum_{i=0}^{28} f_i(f_i - 1)}{n(n-1)}$$

Där $x = x_1, x_2, ..., x_n$ är en sträng och f_i är frekvensen av tecken i. 28 är längden på alfabetet (engelska alfabetet plus # och _).

När jag nu har verifierat nyckellängden (m = 18) är det dags att försöka hitta nyckeln. För att göra detta använder jag åter coincidence.rb, men denna gång med en fast nyckellängd och koden för att testa nyckelkombinationer på. Den listar för varje tecken i nyckeln (dvs varje "rad") M_g, som närmare sig 0.068 om det är rätt.

$$M_g = \sum_{i=0}^{28} \frac{p_i * f_{(i+g)mod28}}{n'}$$

Där n' är antalet tecken som påverkas av nyckelpositionen och p_i är den ideala distributionen för tecken i. g är den nuvarande skiftningen som prövas.

Genom att välja ut de g med högst M_g föreslår programmet sen en nyckel. Jag använder därefter decrypt.rb för att dekryptera skifret med nyckeln. Detta gav relativt bra resultat, men texten var fortfarande hyfsat oläslig. Genom att be programmet att göra radbrytning efter varje nyckellängd kunde jag lätt identifiera i vilka positioner det var fel, och genom att hitta vanliga ord som AND och THE kunde jag räkna ut hur mycket nyckeln borde ändras i den positionen. Genom att systematiskt applicera detta kom jag fram till nyckeln:
DLTAHPXDLTHLPTXADH

1.3.2 Klartext

NOW GUNNLAUG AND RAVEN FELL ATALKING TOGETHER AND EACH TOLD EACH OF HIS TRAVELS RAVEN SAID THAT HE HAD GONE THE SUMMER BEFORE FROM ICELAND TO NORWAY AND HAD COME EAST TO SWEDEN IN THE FOREPART OF WINTER THEY SOON GOT FRIENDLY TOGETHER

BUT ONE DAY WHEN THE THING WAS OVER THEY WERE BOTH BEFORE THE KING GUNNLAUG AND RAVEN

THEN SPAKE GUNNLAUG NOW LORD I WOULD THAT THOU SHOULDST HEAR THE SONG

THAT I MAY DO NOW SAID THE KING

MY SONG TOO WILLSET FORTH NOW SAYS RAVEN

THOU MAYST DO SO SAID THE KING

THEN GUNNLAUG SAID I WILL SET FORTH MINE FIRST IF THOU WILT HAVE IT SO KING

NAY SAID RAVEN IT BEHOVETH ME TO BE FIRST LORD FOR I MYSELF CAME FIRST TO THEE

WHERETO CAME OUR FATHERS FORTH SO THAT MY FATHER WAS THE LITTLE BOAT TOWED BEHIND WHERETO BUT NOWHERE SAYS GUNNLAUG AND IN LIKEWISE SHALL IT BE WITH US

RAVEN ANSWERED LET US BE COURTEOUS ENOUGH NOT TO MAKE THIS A MATTER OF BANDYING OF WORDS LET THE KING RULE HERE

THE KING SAID LET GUNNLAUG SET FORTH HIS SONG FIRST FOR HE WILL NOT BE AT PEACE TILL HE HAS HIS WILL

THEN GUNNLAUG SET FORTH THE SONG WHICH HE HAD MADE TO KING OLAF AND WHEN IT WAS AT AN END THE KING SPAKE RAVEN SAYS HE HOW IS THE SONG DONE

1.4 Skiffer C

1.4.1 Metod

När jag såg skifferalfabetet var det tämligen uppenbart att siffrorna i par av två var hexidecimala tal. Det rimligaste sättet att tolka hexidecimala tal är som ascii. Mitt första försök var därmed m.h.a hex_to_ascii.rb läsa filen två tecken i taget och skriva ut ascii. Detta gav som väntat inte någon klartext. Jag lät därefter koden testa att förskjuta alla tecken med alla tal i mängden 0 till 0x7f modulus 0x7f. Utdatan från detta sparade jag i en fil i vilken jag sedan sökte efter "the". Jag hitade två nycklar som verkade rimliga, 0x4e och 0x6e. Avståndet mellan dessa två är 0x20, vilket är avståndet mellan A och a i ascii-tabellen. 0x6e verkade dock som en mycket rimligare nyckel då utdatan blev nästan klartext med både stora och små bokstäver.

Efter detta hade jag alltså nästan klartext, dock hade texten den egenheten att o och O hade bytts ut med _ och ? (och vise versa). Jag vet inte om detta berodde på att min avkryptering gjorde något litet fel, eller om det faktiskt skulle vara så. Ett sådant fel kan lätt ha uppstått på grund av att roteringen kring ändarna inte fungerade perfekt. Hur som helst fick jag ändå fram klartexten genom att helt enkelt göra det utbyte i efterhand.

1.4.2 Klartext

```
Therefore, resort to Karma–yoga and cut the ignorance–
    born doubt abiding in your heart by the sword of
    Self–knowledge, and get up (to fight), O Arjuna.
    (4.42)

Chapter 5: Path of Renunciation

Arjuna said: O Krishna, You praise transcendental
    knowledge (the Saamkhya or Karma–Samnyasa) and also
    performance of unattached action, Karma–yoga. Tell
    me, definitely, which one is better of the two. (See
     also 5.05) (5.01) ( Karma–Samnyasa means
    renunciation of doership, ownership, and selfish
    motive behind an action, and not the renunciation of
     work, or the worldly objects. Karma–Samnyasa comes
    only after the dawn of Self–knowledge. Therefore,
    words Jnana, Saamkhya, Samnyasa, and Karma–Samnyasa
    are used interchangeably throughout the Gita.
    Renunciation is considered the goal of life, and
```

Karma and Jnana are the necessary means to achieve the goal.)

The Supreme Lord said: Karma–Samnyasa, and Karma–yoga both lead to the Supreme. But, of the two, Karma–yoga is superior to Karma–Samnyasa. (5.02)

A person should be considered a true Samnyasi or renunciant who neither likes nor dislikes. Because, free from the dualities, O Arjuna, one is easily liberated from bondage. (5.03)

The ignorant, not the wise, consider Karma–Samnyasa and Karma–yoga as different from each other. The person who has truly mastered one, gets the benefits of both. (5.04)

Whatever goal a Samnyasi reaches, a Karma–yogi also reaches the same goal. One who sees the path of renunciation and the path of work as the same, really sees. (See also 6.01 and 6.02) (5.05)

But Samnyasa, O Arjuna, is difficult to attain without Karma–yoga. A Karma–yogi sage quickly attains Brahman. (See also 4.31, and 4.38) (5.06)

A Karma–yogi whose mind is pure, whose mind and senses are under control, and who sees one and the same Self in all beings, is not bound (by Karma) though engaged in work. (5.07)

A Samnyasi who knows the truth thinks: I do nothing at all. For in seeing, hearing, touching, smelling, eating, walking, sleeping, breathing; and (5.08)

2 AES

Lösning i kattis. Använde de officiella papprerna för implementationen, kopierade färdig S-BOX och liknande konstanter från wikipedia (där detta är gjort finns kommentarer i koden).

3 SHA256

Lösning i kattis. Använde de officiella papprerna för implementationen, kopierade konstanter från wikipedia (där detta är gjort finns kommentarer i koden).