Frederiksborg Gymnasium og HF

Studieretningsprojekt 2011/12

Elevens navn:	**Pernille Josefine Græsholt**	Klasse:	3x 25

	Fag:	Lærer:
Studieretningsfag på A-niveau	MA	GJ Gert Uttenthal Jensen
Fag på mindst B-niveau	DA	HD Hanne Døcker

Område og faglig problemstilling (Udfyldes af eksaminator).

Kryptologi og populærvidenskab

Opgaveformulering (Udfyldes af eksaminator)

Du skal udarbejde en artikel om kryptering med særlig fokus på RSA-kryptering. Målgruppen er den interesserede læser af et seriøst populærvidenskabeligt tidsskrift som "Aktuel Naturvidenskab". Begrund de valg, du har truffet, af retorisk, sproglig og argumentationsteoretisk karakter.

Redegør i artiklen for kryptologiens udvikling og betydning generelt, og beskriv mere specifikt RSA-kryptosystemet.

Redegør for, hvilke matematiske-indholdsmæssige valg du har gjort, og diskuter med udgangspunkt i disse valg, hvor udfordringerne i popularisering af naturvidenskab ligger.

Opgaven i bilag 1 skal inddrages et passende sted i din besvarelse enten i artiklen eller udenfor.

Det forventes, at opgaven har et omfang svarende til 15-20 normalsider.
(Indholdsfortegnelse, noter, litteraturliste, grafer, illustrationer etc. medregnes ikke i sidetallet).

Vejleders underskrift: Gert Uttenthal Jensen Vejleders underskrift: Hanne Døcker

Jeg bekræfter herved med min underskrift, at opgavebesvarelsen er udarbejdet af mig. Jeg har ikke anvendt tidligere bedømt arbejde uden henvisning hertil, og opgavebesvarelsen er udfærdiget uden anvendelse af uretmæssig hjælp og uden brug af hjælpemidler, der ikke har været tilladt under prøven.

Elevens underskrift: Pernille Græsholt

Opgaven udleveres d. 6/12 2011 kl.14.00

Opgaven afleveres d. 20/12 2011 kl. 14.00 i 4 eksemplarer i adm. 2
- Husk dette ark som forside i alle 4 eksemplarer.

Bilag 1:

Opgave: Du skal du kryptere med følgende meget enkle RSA-kryptosystem:

- baseret p primtallene p=7 og q=17 vise skal du vise, at (n,e)=(119,53) kan fungere som offentlig nøgle,
- vis at d=29 kan bruges som den tilhørende hemmelige nøgle
- foretage en kryptering af en simpel meddelelse fx tallet 39 (du m gerne vælge at kryptere et ord hvor fx A=01 B=02 osv)
- foretage en dekryptering af den fremkomne kryptotekst.

19. december | 2011

Kryptologi og populærvidenskab

Elev: Pernille Josefine Græsholt

SRP om populærvidenskabelig formidling af et naturfagligt emne.

Vejledere: Hanne Døcker og Gert Uttenthal Jensen.

Fag: Dansk A og matematik A.

Klasse: 3x.

Abstract

The study investigates the interaction between a popular science article and a natural science subject like cryptology. It focuses on translating mathematical concepts into a language that is easily understood. It defines that an article must be interesting and fascinate the reader. To achieve this requirement, the article uses language full of imagery, and other rhetorical devices such as logos and pathos. The article introduces exciting examples of how history and society has been affected by cryptology. The article describes the concepts of private and public keys and explains step by step the communication process behind them. Furthermore, it states that every symmetric cryptosystem lack the security obtained by today's asymmetric cryptosystem RSA. The security of RSA lies in the difficulty of using prime number factorization on large numbers. The article concludes that in order to protect our privacy cryptography is necessary. The study discovers that some people find mathematics boring. In effect of that assumption, the study concludes that technical expressions must be excluded from the article.

Indholdsfortegnelse

NB: Artikel er lavet i redigeringsprogrammet *InDesign* og har derfor andre sidetal.

Indledning

"Den hemmelige kommunikations kunst, også kaldet kryptografi, bliver informationsalderens låse og nøgler."[1]

Med de ord lægger Simon Singh grundlaget for min artikel med et spændende emne, der indirekte griber ind i de fleste menneskers hverdag. I dette sekund kæmpes en hæsblæsende kamp for retten til kryptering. Det er krypteringens udvikling, navnlig udviklingen af RSA-kryptosystemet, som har ført til denne kamp.[2]

Jeg vil undersøge teknikken bag RSA og udføre en RSA-kryptering for at demonstrere, hvordan kryptering fungerer. Herunder vil jeg komme ind på de regnetekniske operationer i kryptering.

For at forstå RSA er det nødvendigt at have noget baggrundsviden om kryptologi. I min artikel vil jeg først redegøre for, hvordan kendskab til og udvikling af kryptologi har påvirket historiens gang. Dette vil jeg gøre ved at kigge på kryptologiens begyndelse, for derefter at kaste et hurtigt blik på den berømte krypteringsmaskine ENIGMA og sammenligne med RSA. Jeg slutter af med at se på, hvor vi er i dag med fokus på kampen om kryptering.

Jeg har valgt at belyse emnet kryptografi ud fra en populærvidenskabelige synsvinkel. Koder er et sprog i sig selv, et sprog der bygger på matematik. Matematikken gør, at mange holder op med at prøve at knække koden, fordi den hurtigt bliver for langhåret. Jeg vil gøre mit bedste for at oversætte den svære matematik til et sprog som folk, med interesse i koder, kan forstå uden at skulle læse tykke bøger for at følge med. Som Søren Brier definerer, er populærvidenskab formidling af videnskabelig viden til ikke-fagfolk, og har ikke til formål at uddanne dem til fagfolk. Populærvidenskab formidler blot videnskab og er ikke videnskab i sig selv.[3]

Formidling er nøgleordet, så det er af største betydning, at jeg gør artiklen enkel og spændende og skriver på et letforståeligt sprog. Jeg vil gøre sproget mere spiseligt ved at benytte sproglige virkemidler såsom metaforer og sammenligninger. På den måde bliver det videnskabelige sprog mere håndterbart[4] i form af ligheder mellem den svære matematik og de hverdagsoplevelser, vi er fortro-

---

[1] Singh, Simon: *Kodebogen*, Gyldendal, 2001, s. 11.

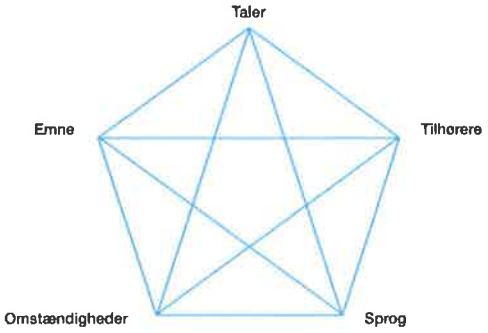
[2] Singh, Simon: *Kodebogen*, s. 307-330.

[3] Brier, Søren: *Fra fakta til fikta*, Akademisk Forlag, 2002, s. 25.

[4] Johansen, Mikkel W.: "Roser er røde, metaforer er blå" in Aktuel Naturvidenskab, nr. 5, 2004 s. 30.

lige med. Noget velkendt, som f.eks. at bage en kage, bliver brugt til at forstå et nyt og ukendt område. Her er det vigtigt at være sikker på, at metaforerne kan forstås af enhver, så artiklen henvender sig til så mange læsere som muligt. Jeg benytter desuden eksempler som et redskab til at gøre den ukendte matematik forståelig.

Foruden sprog og modtager beskriver Ciceros kommunikationsmodel, den retoriske pentagon,[5] yderligere tre faktorer, som alle afhænger af hinanden. Sprog, afsender, modtager, omstændighederne og emne skal spille sammen i enhver formidling.



Den retoriske pentagon[6]

Min modtager er den interesserede læser af et seriøst populærvidenskabeligt tidsskrift som "Aktuel Naturvidenskab." Dette tidsskrift udtaler følgende om sine artikler:[7]

"Artiklerne er primært skrevet af fagfolk og henvender sig til læsere med en bred interesse for naturvidenskab. Det faglige niveau svarer til en "studentereksamen."

Skal mit emne fange min modtager, bør jeg allerede gennem overskriften og indledningen af artiklen sikre denne fangst. Det er vigtig, at jeg forfatter en fængende overskrift og sørger for, at mine konklusioner kommer inden for de første linjer.[8]

Jeg vil forsøge at kombinere billeder og tekst på en meningsfuld måde, så læseren bliver nygerrig og samtidig får hjælp til forståelsen. Desuden vil jeg benytte mig af faktabokse til matematikken, så læseren kan vælge at springe boksene over og kun forholde sig til artiklens brødtekst.

Vil jeg fastholde min læser, er det også vigtig, at min artikel har en vis troværdighed. Saglig og klar argumentation er en god start.

---

[5] Garbers, Lis og Sten Høgel: *Grib ordet –og gør det til dit!*, Gyldendal, 2004.

[6] http://ibog.litteraturenshuse.systime.dk/index.php?id=1181, besøgt d. 16.12.2001

[7] *Om bladet,* Aktuel Naturvidenskab, besøgt d. 12.12.2012. http://aktuelnaturvidenskab.dk/om-bladet/

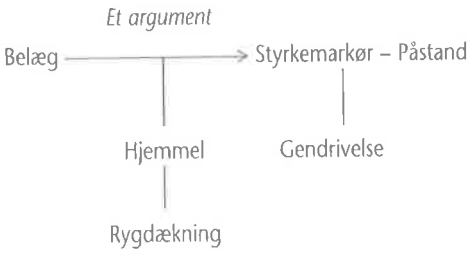
[8] *Skriv i bladet,* Aktuel Naturvidenskab, besøgt d. 10.12.2012. http://aktuelnaturvidenskab.dk/skriv-i-bladet/

For at opnå et succesfuldt argument vil jeg benytte mig af Toulmins argumentationsmodel.[9] Ifølge modellen skal tre elementer være til stede for at lave et stærkt argument: En påstand, et belæg og en hjemmel. Påstanden er det, man prøver at argumentere for og derfor det centrale element i modellen. Belægget støtter og argumenterer for rigtigheden i påstanden, men for at påstanden giver mening på baggrund af belægget, skal der være en hjemmel. En hjemmel er et generelt synspunkt, som både afsender og modtager kan være enige om. Ofte er hjemlen ikke skrevet direkte i argumentet, da den kan være så indlysende, at det er unødvendigt. Mangler blot én af de ovennævnte har man lavet en fejlslutning, og argumentet er ugyldigt.

Her er et eksempel, hvor påstanden, "Søren dumper til eksamen," underbygges af belægget, "han har ikke læst på sine lektier," og argumentet er gyldigt, da det er indforstået, at "en elev, der ikke læser sine lektier, dumper til eksamen"- argumentet har altså en indirekte hjemmel.[10]

I et argument kan der sagtens forekomme flere elementer end blot de tre obligatoriske. Gendrivelse, rygdækning og styrkemarkør er også værd at nævne, da disse bruges til at udtrykke tvivl eller belyse alternativer, så man opnår en mere avanceret argumentation. Styrkemarkøren kan både forstærke eller svække en påstand, da den angiver, med hvor stor sikkerhed påstanden er gyldig. Gendrivelse beskriver eventuelle forbehold ved hjemlen og derved også ved påstanden, mens rygdækningen er yderligere dokumentation for hjemlen.

Toulmins udvidede argumentationsmodel[11]



[9] Hegelund, Signe: *Akademisk argumentation*, Samfundslitteratur, 2002, s. 8-12

[10] Døcker, Hanne: *Argumentationsmodeller,* upubliceret powerpoint, 09.03.2010, s. 6.

[11] Døcker, Hanne: *Argumentationsmodeller,* upubliceret powerpoint, 09.03.2010, s. 10.

Når man argumenterer, er det vigtigt at være bevidst om de tre appelformer: Logos, pathos og ethos. De fleste af mine argumenter vil være baseret på logos, da det er naturvidenskabeligt stof jeg formidler. Logos er en appelform, hvor man fremfører logiske, saglige belæg og påstande, som appellerer til intellektet og noget rationelt hos modtageren. Jeg benytter også pathos i artiklen, da pathos handler om at vække følelser, og jeg kombinerer tekst og billede for at vække følelsen af nygerrighed hos læseren.

Til sidst bør jeg nævne, at da matematikken bag RSA hurtigt bliver meget omfattende, er jeg blevet nødt til at antage, at folk kender definitionen af primtal, og desuden er bekendt med begrebet kongruent, som optræder i form af tegnet ≡.

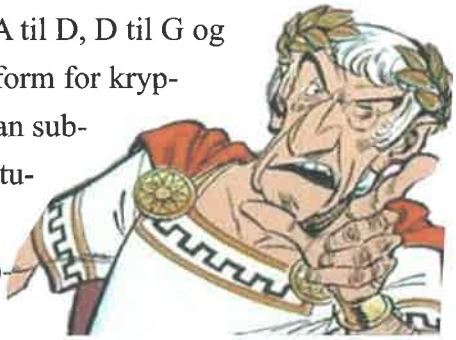
Er kryptering vores nye låse og nøgler?

Hver dag sender personer i hele verden millioner af private e-mails. Foruroligende nok er de såkaldte "private" e-mails ikke svære at få adgang til. Faren, for at hackere eller andre med onde hensigter kan få adgang til vores private oplysninger, er stor. Det eneste, der kan redde os fra faren, er kryptering. I dag er det muligt at kyptere sine e-mails via PGP. Pretty Good Privacy, PGP, er et krypteringsprogram, som gør folk i stand til at kommunikere uden fare for "aflytning." Selvom dette lyder lovende, har det også sine minus sider. På den ene side kan de lovlydige borgere føle sig mere sikre med hensyn til deres private affærer, på den anden side kan forbrydere og terrorister sådan set også gøre det. Det er derfor nødvendigt at staten har endnu mere kontrol over, hvad vi foretager os, så er vi virkelig blevet mere sikre?

Hvad er kryptering egentlig?

Den første sten på vejen

Historien er brolagt med koder, og en af de første sten på vejen må være Cæsars forskydningskode[1]. Julius Cæsar var tro tilhænger af kryptografiens muligheder. Kryptografi handler om at skjule budskabet i en meddelelse. Dette var essentielt for Cæsar, som på sine mange felttog skulle kunne kommunikere med sine fortrolige konsuler hjemme i Rom. Cæsar brugte et krypteringssystem, hvor han erstattede hvert bogstav i alfabetet med det bogstav, som stod tre pladser længere fremme. På den måde blev A til D, D til G og Å til C. Denne form for kryptering kalder man substitution. Substitution er en ud af to grene af kryptografien, hvor den anden gren hedder transposition. Fordelen ved kryptografi er, at hvis en fjende opsnapper en krypteret meddelelse, vil den være ulæselig. Dette gælder dog kun, hvis opsnapperen ikke kender krypteringsmetoden. Var metoden kendt og han opsnappede kodeteksten ZHQL ZLGL ZLFL, kunne fjenden hurtigt finde den oprindelige besked ved at opstille det originale alfabet, dvs. klaralfabetet, overfor de bogstaver, der indsættes i stedet for den oprindelige besked, også kaldet kodealfabet.På den måde ville kodeteksten ZHQL ZLGL ZLFL blive til meddelelsen veni, vidi, vici -*jeg kom, jeg så, jeg sejrede.* Det er interessant at tænke på, hvordan gallerkrigene var endt, hvis en galler havde haft kendskab til Cæsars forskydningskode.



Julius Cæsar på krigsstien.

Vidste du?

Ved transposition ændrer man bogstavernes placering i alfabetet, mens ved substitution har bogstaverne samme placering i alfabetet, men selve bogstavet bliver repræsenteret af et andet, ligesom D blev til G i Cæsars forskydningskode.

A lover's quarrel

I takt med at der kom flere og større sten på vejen i kryptologiens udvikling, var kryptering ikke længere forbeholdt regenter. I Viktoria-tidens England begyndte krypterede kærestebreve at dukke op i de lokale aviser.[2] Denne fremgangsmåde blev taget i brug, da de unge elskende ofte måtte skjule deres kærlighed for misbilligende forældre. Selvom disse beskeder blev trykt under "personlige" må man ikke glemme, at de var offentlige for alles nysgerrige

Klaralfabet:
a b c d e f g h i j k l m n o p q r s t u v x y z æ ø å
Kodealfabet:
D E F G H I J K L M N O P Q R S T U V X Y Z Æ Ø Å A B C

1 Singh, Simon: *Kodebogen*, Gyldendal. 2001. s. 20-25

2 Singh, Simon: *Kodebogen*, s. 93-95

blikke. Her skulle de unge mennesker måske have tænkt sig bedre om, for som den amerikanske poet Edgar Allan Poe engang skrev: en kode skabt af menneskelig genialitet kan menneskelig genialitet knække igen.

"It may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot solve.[3]

Ordet kryptologi dækker over to ting: kryptografi (kryptering) og kryptoanalyse (dekryptering)

Det tog da heller ikke lang tid før kryptoanalytikerne, folk som arbejder med at bryde krypteringer, blev tiltrukket af de krypterede kærestebreve. En kryptoanalytiker ved navn sir Charles Wheatstone dekrypterede en note i *The Times*, hvori en ung Oxford-student foreslog sin elskede at stikke af sammen og gifte sig. Wheatstone indrykkede få dage efter en meddelelse krypteret med samme kode, som stærkt frarådede det unge par den tankeløse handlig. En tredje meddelelse kom nu på banen. Denne gang en ukrypteret meddelelse fra den unge dame: *"Kære Charlie, skriv ikke mere. Vores kode er afsløret."*

Sådan kan det jo gå.

Det er elementært, min kære Watson

Med tiden dukker en større mangfoldighed af krypterede meddelelser op i aviserne. Krypterede beskeder bliver blandt andet brugt til ildesete meninger om offentlige personer. Selv i litteraturen begynder koder at optræde. En af de bedste forfattere af kryptografisk litteratur er Arthur Conan Doyle. Det giver derfor god mening, at hans mest berømte figur, Sherlock Holmes, var ekspert i kryptografi. I *Novellen om de dansende mænd* har Sherlock Holmes til opgave at analysere eller rettere sagt kryptoanalysere følgende meddelelse:

Holmes' fremgangsmåde afspejler samtidens metode til at knække koder. Holmes bruger frekvensanalyse[4] til at analysere meddelelsen. I en frekvensanalyse er hvert bogstav i alfabet blevet tildelt en speciel frekvens alt afhængigt af, hvor meget det pågældende bogstav optræder i litteraturen. På den måde vil bogstaverne E,R og N, som man ofte bruger i tekster, have en langt højere frekvens end X, Z og Q. Frekvensanalyser har vist, at man benytter bogstavet E mere end noget andet bogstav. Med den viden antager Holmes, at det bogstav, som optræder flest gange i den krypterede meddelelse, svarer til bogstavet E. Via gætteri og videre sammenligning af de andre bogstaver og deres tilhørende frekvens kan Holmes finde nøglen, som åbner den hemmelige besked. Men han kan kun bruge denne metode, hvis meddelelsen har en betydelig længde, da statistikken ellers er upålidelig. Holmes kan altså ikke knække koden ud fra den ene krypterede meddelelse, men heldigvis kommer flere til. Holmes ender med at vride fornuft ud af de meningsløse symboler i form af meddelelsen "Am here Abe Slaney" foran de måbende tilhørere, Watson og politiinspektøren. Og hvad skal det så betyde? Det er elementært min kære Watson, det ved de, som læser novellen.[5]

Holmes på sporet.

Fremskridt

Hver gang et kryptosystem bliver knækket, kommer nye til i håb om, at de kan stå distancen i kampen mod kryptoanalytikerne. Belært af svaghederne fra tidligere kryptosystemer begynder man at opfinde maskiner, der uskadeliggør kryptoanalytikernes stærkeste våben, frekvensanalysen.[6] En sådan maskine var tyskernes ENIGMA, som blev brugt til kryptering under 2. Verdenskrig. ENIGMA er et kompliceret system af bogstavserstatning, hvor den vigtigste brik er rotationen af "scrambleren" i ENIGMA-skrivemaskinen.

3 Landrock, Peter: *Kryptologi -fra viden til videnskab*. ABACUS. 1997. s. 7

4 Landrock, Peter: *Kryptologi,* s. 26-31

5 Doyle, Athur C.: *De dansende mænd,* Martins forlag, 1970, s.26.

6 Landrock,Peter: *Kryptologi,* s.48.

Scrambleren bestemmer kodealfabetet, eller sagt på en anden måde, afgør den hvilke bogstaver, der erstatter hinanden. Roterer man scrambleren, bliver et bogstavs identitet ikke længere blot repræsenteret af ét bogstav, men af flere. Frekvensanalysen er derfor ubrugelig, da E i første sætning kan være repræsenteret af N, mens det i næste sætning er repræsenteret af F. Man kan altså ikke antage at E svarer til ét bestemt bogstav i den krypterede meddelelse.[7]

ENIGMA-maskine.

Med den nyskabelsen var tyskerne sikre på, at ENIGMA-kodningen var ubrydelig. De vidste ikke, at systemet allerede var blevet brudt i begyndelsen af krigen. Polakkerne havde, ud fra kaprede ENIGMA-maskiner, fundet nøglen til dekryptering. Dette var muligt, da ENIGMA er, hvad man kalder et symmetrisk kryptosystem[8]. Her bruger man den samme nøgle til at "låse" og "åbne" meddelelsen med. Inden Tysklands invasion af Polen, nåede polakkerne at give informationerne videre til Frankrig og England. Det førte til et kryptografisk nederlag for tyskerne, og ENIGMA måtte hejse det hvide flag.

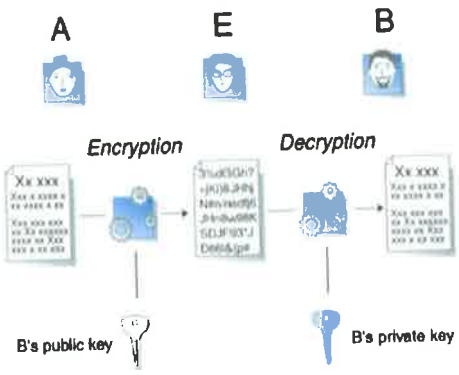
I året 1976 designede amerikanerne Whitfield Diffie og Martin Hellman en kommunikationsmodel,[9] som skulle løse problemet med symmetriske nøgler. De to mænd havde designet et asymmetrisk kryptosystem.

Nøglerne

Det assymetriske kryptosystem indeholder to forskellige nøgler, en offentlig og en privat nøgle. Sammenspillet mellem nøglerne bliver mere overskueligt, hvis man forestiller man sig, at Alice ønsker at kommunikere en besked til Bob uden at Eve kigger med. Der er 4 overordnede trin i en sådan kommunikation:

1) Alice beder Bob om en nøgle, som hun skal bruge til at kryptere med.

2) Bob skaber et nøglepar, men offentliggør kun den ene af nøglerne, f.eks. i den lokale avis, så Alice kan bruge den. Denne nøgle kalder man *den offentlige nøgle.*



A sender en besked til B uden E kan "lytte" med.

3) Alice krypterer sin besked via den offentlige nøgle, og sender derefter den krypterede besked til Bob.

4) Ved hjælp af den anden nøgle i nøgleparret kan Bob nu dekryptere den krypterede besked fra Alice. Den anden nøgle skal Bob holde hemmelig, da alle med kendskab til nøglen, kan dekryptere Alices besked. Den kalder man *den private nøgle.*

Hellman og Diffie var ikke i stand til selv at realisere modellen, men realiseret blev den.

Der gik kun et år, før RSA-systemet[10] blev udviklet af Rivest, Shamir og Adleman. De tre mænd havde ladet sig inspirere af Diffie og Hellmans model.

Vil man forstå RSA's version af offentlig og privat nøgle, kan man forestille sig to virkelige nøgler med forskellige hakker. Hakkerne i den offentlige nøgle er formet som tallene n og e, mens den private nøgle har hakkerne n og d. Videre skal man forestille sig, at den meddelelse, man vil kryptere, er formet som en lås. Vælger man at bruge en persons offentlige nøgle til denne lås, vil låsen øjeblikkeligt låses godt og grundigt i. Sender man efterfølgende låsen til den samme person, hvis offentlige nøgle man har brugt, kan han med sin private nøgle åbne låsen og læse meddelelsen. Hvad der er vigtigt at bemærke, er det fælles

7 Singh, Simon: *Kodebogen*, s.142, 163-174.
8 Singh, Simon: *Kodebogen*, s. 283-285
9 Landrock,Peter ; *Kryptologi*, s. 56-57.
10 Singh, Simon: *Kodebogen*, s. 286-292

hak i nøglerne, n. Alle kan vælge en personlig værdi for n og på den måde gøre nøglerne til sine egne. Alice vælger, som en personlig værdi for tallet n, to primtal, p og q, og ganger dem med hinanden. Alices valg af n sætter et af hakkerne i hendes nøglesæt, mens hun bruger de to primtal p og q til at bestemme det andet hak, d, i hendes private nøgle. Tallene p og q holder hun for alt i verden hemmelige, da de kan afsløre hendes private nøgle. Nogle vil måske tænke, at hvis man kender tallet n, så må man da kunne finde tallene p og q ud fra dette? Her kommer det smukke og fantastiske ved RSA-krypteringen, for så længe man giver n en tilstrækkelig stor værdi, er det praktisk talt umuligt at udlede p og q ud fra n. Men hvorfor nu det? Svaret finder man i primtalsfaktorisering.[11]

Ifølge aritmetikkens fundamentalsætning kan alle positive hele tal, der ikke selv er primtal, primfaktoriseres, dvs. omskrives til et produkt af primtal. F.eks. ville primtalsfaktorisering af tallet 60 se således ud $2^2 \cdot 3 \cdot 5$. På den måde har man faktoriseret 60 til et produkt kun bestående af primtal.

Da primtalsfaktorisering overordnet går ud på, at man splitter et tal op i primtal, burde den metode være ideel til at finde primtallene p og q. Problemet er bare, at det er uhyre vanskeligt og tidskrævende at primtalsfaktorisere store tal. Har man at gøre med et tal så stort som 10^{308}, ville det tage hundrede millioner computere mere end tusind år at knække koden. Med tilstrækkelig store værdier for p og q er RSA altså urørlig. Det er ganske betryggende eftersom de fleste banktransaktioner mindst har n lig 10^{308}. Man kan måske have lyst til at spørge: *"Kunne det ikke tænkes, at man opfandt en metode, der kan primtalfaktorisere markant hurtigere end de p.t. bedst kendte?"* De har muligvis ret, men selvom de klogeste matematikerne gennem de sidste par tusind år ihærdigt har forsøgt, er det endnu ikke lykkedes. Mange matematikere er af den opfattelse, at faktorisering er en så speciel og vanskelig opgave, at der må være en matematisk lov, som forhindrer genvej.[12] Det er derfor højst usandsynligt, at det skulle ske i den nærmeste fremtid, men skulle det lykkes én, kan man kun sige, at der vil åbne sig en stribe af muligheder. Som forfatter Peter Riber skriver i sin bog "Kryptering":[13]

Du kan bl.a. blive:

- meget berømt ved at offentliggøre din opdagelse

-uhørt succesrig kriminel via økonomisk svindel

-stinkende rig ved at sælge metoden til et større softwarefirma

-myrdet af CIA, fordi du truer hemmelig militær kommunikation.

Kunsten at bage en kage

Er man den eventyrlystne type, og kunne man godt tænke sig at oprette et nøglepar, kan man sammenligne hele processen med at bage en kage. Man skal bare følge den rigtige opskrift, så skal den nok blive god.

Der er intet som en nybagt kage.

Inden man giver sig i kast med "bagningen," er det vigtig, at man har ingredienserne. Når det er nøglepar, der er på menuen, er ingredienserne de mest lækre matematiske begreber. Foruden primtalsfaktorisering er begreber som indbyrdes primsk og modulo vældig gode at få med. Ligesom i ethvert andet køkken er det vigtigt, at man kender sine ingrediensers egenskaber. Med andre ord skal man sætte sig ind i de matematiske begreber inden start.

Har man fulgt opskriften til punkt og prikke, står man tilbage med et fuldt nøglesæt. F.eks. i form af den offentlige nøgle (n,e) = (119,53) og den hemmelige nøgle d=29. Det valgte nøglesæt har en

11 Landrock, Peter:*Kryptologi,* s. 84-85.

12 Jankvist, Uffe T.: *Et undervisningsforløb i RSA*, 2007 s. 87.

13 Riber, Peter: *Kryptering*, Systime, 2007, s.36

Jeg valgte i den ånd at droppe det formelle bevis og i stedet demonstrere nogle af de konkrete regnetekniske operationer bag RSA-kryptering. En anden grund var, at jeg ikke ville risikere at stå tilbage med en artikel kun bestående af faktabokse. Det er endnu en udfordring i populariseringen af naturvidenskab, at der næsten ingenting skal til, før artiklen bliver usammenhængende. Tekniske termer, beviser og regnetekniske operationer må helst ikke optræde i brødteksten, så skal man lave en fusion mellem et humanistisk og et naturvidenskabeligt område, er den eneste løsning ofte faktabokse. Problemets størrelse afhænger dog af det naturvidenskabelige område, der beskrives, f.eks. er geografiske begreber tit nemmere at inddrage i selve artiklen end matematiske begreber.

Et andet bevis, jeg havde tænkt mig at inddrage, er beviset for $\phi(n)=(p-1)(q-1)$. Beviset er måske ikke så væsentligt, men jeg tænkte, at det kunne lette forståelsen af $\phi(n)$. Funktionen ϕ er ny for mange læsere, og da det er en matematisk betegnelse, vil nogle læsere muligvis stå af. Endnu engang måtte jeg ændre mine planer, da beviset igen blev for langt og irrelevant i forhold til artiklen. I sidste ende nøjedes jeg med at lave en faktaboks om $\phi(n)$, så den ikke længere var helt fremmed for læseren.

I udarbejdelsen af min artikel stod jeg overfor en række valgmuligheder med hensyn til min artikels "blikfang". Med blikfang mener jeg det emne i min artikel, som gør den relevant at læse i en bredere kreds. Brier nævner, at det er typisk for populærvidenskab at inddrage emnet i en kulturel sammenhæng[15]. Jeg besluttede på det grundlag, at det bedste blikfang måtte være den nutidige stridighed om kryptering, da det fanger og er relevant for læseren. Samtidig er det et tidspunkt i kryptologiens udvikling, som stærkt inddrager RSA, som jo er mit fokus i opgaven.

I god populærvidenskab må man ikke bruge for mange tekniske udtryk og de, der bruges, skal løbende forklares. Jeg har derfor undladt fagudtryk såsom monoalfabetisk kryptosystem og polyalfabetisk kryptosystem, og i stedet givet eksempler på, hvad de går ud på. Her skal det nævnes, at Cæsars forskydningskode er et monoalfabetisk kryptosystem, mens ENIGMA er et polyalfabetisk kryptosystem. Jeg giver kun et overfladisk indblik i teknikken bag ENIGMA, hvilket skyldes, at teknikken er meget omfattende og sammen med min detaljerede gennemgang af teknikken bag RSA-kryptering, ville artiklen blive for teknisk. Visse fagudtryk, såsom symmetriske og asymmetriske kryptosystemer, blev jeg nødt til at få med, da de er essentielle, når man sammenligner RSA med tidligere kryptosystemer.

---

[15] Brier, Søren: *Fra fakta til fikta*, Akademisk Forlag, 2002, s. 25.

Jeg havde vanskeligt ved at redegøre for kryptografiens udvikling og betydning generelt, da de mest relevante ting ikke nødvendigvis er de mest spændende og omvendt. Cæsars forskydningskode er et af de mere simple krypteringssystemer, som samtidig kan kobles til en skikkelse, de fleste læsere kender. Angående kryptoanalyser, valgte jeg igen den simpleste, jeg kunne finde. På trods af mine anstrengelser blev afsnittet med frekvensanalyse lidt tungt i starten, da frekvensanalyser ikke er det mest appetitvækkende. Jeg fandt heldigvis en kobling til den berømte Sherlock Holmes, så det nye område blev gjort mere velkendt.

Et sidste valg, jeg tog, var ikke at fokusere på fremtiden for RSA. I fremtiden vil man muligvis være i stand til at bryde RSA-kryptering via en kvantecomputer, men jeg valgte ikke at gå nærmere i detaljer med det, da jeg blev nødt til at begrænse min opgave.[16]

Konklusion

I populærvidenskabelige artikler er formidling nøgleordet. En god populærvidenskabelig artikel er gjort enkel og spændende og er skrevet på et letforståeligt sprog.

Jeg har benyttet mig af sproglige virkemidler såsom metaforer og sammenligninger, da disse gør det videnskabelige sprog mere håndterbart. Jeg bruger virkemidlerne til at udpege ligheder mellem den svære matematik og de hverdagsoplevelser, vi er fortrolige med.

En god og troværdig formidling er nødvendig for at fastholde læseren. Jeg har brugt den retoriske pentagon, som beskriver at sprog, afsender, modtager, omstændighederne og emne skal spille sammen i enhver formidling. Desuden har jeg brugt Toulmins argumentationsmodel for at sikre en saglig og klar argumentation.

Igennem tusinder af år har mennesket haft behov for at kommunikere hemmeligt med hinanden ved hjælp af krypterede meddelelser. Simple kryptosystemer, såsom Cæsars forskydningskode, er undervejs blevet erstattet af mere avancerede maskiner heriblandt ENIGMA, men gang på gang har kryptoanalytikerne knækket koden. Indtil RSA-kryptosystemet så dagens lys var alle kryptosystemer symmetriske. I et symmetrisk kryptosystem er det den samme nøgle, man bruger til at kryptere og dekryptere meddelelsen med. RSA er et asymmetrisk kryptosystem, som indeholder to nøgler, den private og den offentlige nøgle. Sikkerheden ligger i, at det er uhyre tidskrævende og vanskeligt

[16] Singh, Simon: *Kodebogen*, Gyldendal, 2001, s.331-345.

at primtalsfaktorisere store tal. Desuden er mange matematikere af den opfattelse, at faktorisering er en så speciel og vanskelig opgave, at der må være en matematisk lov, som forhindrer at tage genveje. De har muligvis ret, for selvom de klogeste matematikerne gennem de sidste par tusind år ihærdigt har forsøgt, er det endnu ikke lykkedes. I dag bruger banker RSA til at beskytte deres transaktioner. Den almindelige borger er også i stand til at beskytte sit privatliv via PGP, som står for Pretty Good Privacy. RSA er nøgleelementet i PGP.

En udfordring i populariseringen af naturvidenskab er, at der næsten ingenting skal til, før artiklen bliver usammenhængende. Tekniske termer, beviser og regnetekniske operationer må helst ikke optræde i brødteksten. Så skal man lave en fusion mellem et humanistisk og et naturvidenskabeligt område, er den eneste løsning ofte faktabokse. Problemets størrelse afhænger dog af det naturvidenskabelige område, der beskrives, f.eks. er geografiske begreber tit nemmere at inddrage i selve artiklen end matematiske begreber.

Popularisering af matematik er ikke en let opgave, da matematik ofte bliver betragtet som kedelig. Svær matematik kræver normalt tid og koncentration for at forstå. Jeg ville gerne have haft beviset for Eulers sætning og beviset for $\phi(n)=(p-1)(q-1)$ med i min artikel, men det kom hurtigt til at fylde alt for meget, hvis jeg skulle give en grundig og letforståelig forklaring. Jeg valgte derfor at udelade beviserne i min endelige artikel.

Litteraturliste

Bøger

Brier, Søren: *Fra fakta til fikta*, Akademisk Forlag, 2002.

- Benyttede afsnit:
  "Hvad er populærvidenskab?" og "Populærvidenskabelige tidsskrifter til forskellige aftagergrupper."

Doyle, Athur C.: *De dansende mænd –og andre noveller,* Martinsforlag, 1970.

- Benyttede afsnit:
  Novellen: " De dansende mænd."

Garbers, Lis og Sten Høgel: *Grib ordet –og gør det til dit!*, Gyldendal, 2004.

- Benyttede afsnit:
  Underkapitel: "Elocutio."

Hegelund, Signe: *Akademisk argumentation*, Samfundslitteratur, 2002.

- Benyttede afsnit:
  Kapitel 2: "Toulmins argumentationsmodel."

Jankvist, Uffe T.: *Et undervisningsforløb i RSA og den heri anvendte matematiks historie*, IMFUFA, 2007.

- Benyttede afsnit:
  Kapitel 3: "Tre vigtige sætninger for RSA", og kapitel 4: "RSA-algoritmen."

Landrock, Peter og Knud Nissen: *Kryptologi -fra viden til videnskab*, ABACUS, 1997.

- Benyttede afsnit:
  Kapitel 1: "Den hemmelige skrivekunst" og kapitel 5: "RSA-kryptosystemet."
  Underkapitel 2.5: "Kryptoanalyse af et monoalfabetisk kryptosystem", 2.10: "ENIGMA, HAGELIN og PURPLE", 3.4: "Public key kryptosystemer", 4.2: "Fælles divisorer", 4.3: "Primtal" og 4.4: "Kongruenser."

Riber, Peter: *Kryptering*, Systime, 2007.

- Benyttede afsnit:
  Kapitel 5: "RSA-kryptering."

Singh, Simon: *Kodebogen*, Gyldendal, 2001.

- Benyttede afsnit:

Kapitel 4: "Enigma knækkes", kapitel 6: "Alice og Bob i det offentlige", kapitel 8: "Et kvantespring ind i fremtiden" og kapitel 7: "Pokkers Godt Privatliv: PGP."
Underkapitel: "Udviklingen af hemmelig skrift", "Fra kvidespalter til begravet skat" og "Udviklingen af cif-fermaskiner - fra cifferskiver til Enigma."

Artikler

Johansen, Mikkel W.: "Roser er røde, metaforer er blå" in Aktuel Naturvidenskab, nr. 5, 2004 s. 30-32.

Hansen, Vagn L.: "Popularisering af matematik" in Aktuel Naturvidenskab, nr. 2, 2000 s. 34-35.

Andre ressourcer

Døcker, Hanne: *Argumentationsmodeller,* upubliceret powerpoint, 33 slides, 09.03.2010

- Benyttede afsnit:
  Slide 6 og 10.

Jonathan Kjeldsen: *En rejse ud i det uendelige*, upubliceret opgave, 2008/2009.

- Benyttet som inspiration til opgavens opbygning.

Hjemmesider

Skriv i bladet, Aktuel Naturvidenskab, Besøgt d. 10.12.2012. http://aktuelnaturvidenskab.dk/skriv-i-bladet/

Om bladet, Aktuel Naturvidenskab, Besøgt d. 12.12.2012. http://aktuelnaturvidenskab.dk/om-bladet/

Billeder

http://ibog.litteraturenshuse.systime.dk/index.php?id=1181

- Benyttet materiale: Billede af den retoriske pentagon. Besøgt d. 16.12.2001

http://rejoice.bloggbyen.com/julius-cæsar-og-det-nye-testamentet/

- Benyttet materiale: Billede af Cæsar. Besøgt d. 16.12.2001

http://www.magicdragon.com/SherlockHolmes/

- Benyttet materiale: Billede af Sherlock Holmes. Besøgt d. 16.12.2001

http://universer.dk/kvanteinformation.htm#ville%F8nske

- Benyttet materiale: Billede af kommunikation ved offentlig og privat nøgle. Besøgt d. 17.12.2001

http://www.andersbeck.dk/?page_id=648

- Benyttet materiale: Billede af ENIGMA-maskine. Besøgt d. 17.12.2001

http://missrasmus.blogspot.com/2011_05_01_archive.html

- Benyttet materiale: Billede af forelsket mand. Besøgt d. 17.12.2001

http://www.hvitstenvel.no/website.aspx?displayid=4372

- Benyttet materiale: Billede af indbrudstyv. Besøgt d. 17.12.2001

http://popze-popze.blogspot.com/2010_03_01_archive.html

- Benyttet materiale: Billede af kage. Besøgt d. 17.12.2001

http://modkraft.dk/nyheder/article/fagforening-traener-journalister-i

- Benyttet materiale: Billede af nøgle. Besøgt d. 17.12.2001

http://madogmening.blogspot.com/2010_10_01_archive.html

- Benyttet materiale: Billede af et stykke kage. Besøgt d. 18.12.2001

http://lady-simone.blogspot.com/2010/09/i-love-you.html

- Benyttet materiale: Billede af hjerteformet ring. Besøgt d. 18.12.2001

Kildekritik: Jeg har forsøgt at vælge fagbøger for at undgå utroværdige kilder. Bøgerne er tilgængelige på de fleste biblioteker. Mine artikler kan desuden hentes på Aktuel Videnskabs hjemmeside, hvilket jeg selv har benyttet mig af. Resten af mine hjemmesider involverer billede, og jeg antager disse kilder som pålidelige.

Underskrift og dato

Pernille Græsholt 20.12.2011

Opgave 1

Tabel for 12^{53} (mod 119)

BILAG

Pernille Græsholt

$\mathrm{mod}(12^2,119) \to 25 \quad m^2$

$\mathrm{mod}(25^2,119) \to 30 \quad (m^2)^2$

$\mathrm{mod}(30^2,119) \to 67 \quad ((m^2)^2)^2$

$\mathrm{mod}(67^2,119) \to 86 \quad (((m^2)^2)^2)^2$

$\mathrm{mod}(86^2,119) \to 18 \quad ((((m^2)^2)^2)^2)^2$

Beregninger: $\mathrm{mod}(18 \cdot 12,119) \to 97 \quad ((((m^2)^2)^2)^2)^2 * m$

$\mathrm{mod}(97 \cdot 86,119) \to 12 \quad ((((m^2)^2)^2)^2)^2 * m * (((m^2)^2)^2)^2$

$\mathrm{mod}(12 \cdot 30,119) \to 3 \quad ((((m^2)^2)^2)^2)^2 * m * (((m^2)^2)^2)^2 * (m^2)^2$

Tabel for 3^{29} (mod 119): $\mathrm{mod}(3^2,119) \to 9 \quad m^2$

$\mathrm{mod}(9^2,119) \to 81 \quad (m^2)^2$

$\mathrm{mod}(81^2,119) \to 16 \quad ((m^2)^2)^2$

$\mathrm{mod}(16^2,119) \to 18 \quad (((m^2)^2)^2)^2$

Beregninger: $\mathrm{mod}(18 \cdot 3,119) \to 54 \quad (((m^2)^2)^2)^2 * m$

$\mathrm{mod}(54 \cdot 16,119) \to 31 \quad (((m^2)^2)^2)^2 * m * ((m^2)^2)^2$

$\mathrm{mod}(31 \cdot 81,119) \to 12 \quad (((m^2)^2)^2)^2 * m * ((m^2)^2)^2 * (m^2)^2$

1.1

Opgave 2

Tabel for 15^{53} (mod 119)

$\mathrm{mod}(15^2,119) \rightarrow 106$ m^2

$\mathrm{mod}(106^2,119) \rightarrow 50$ $(m^2)^2$

$\mathrm{mod}(50^2,119) \rightarrow 1$ $((m^2)^2)^2$

$\mathrm{mod}(1^2,119) \rightarrow 1$ $(((m^2)^2)^2)^2$

$\mathrm{mod}(1^2,119) \rightarrow 1$ $((((m^2)^2)^2)^2)^2$

Beregniger: $\mathrm{mod}(1\cdot15,119) \rightarrow 15$ $((((m^2)^2)^2)^2)^2*m$

$\mathrm{mod}(15\cdot1,119) \rightarrow 15$ $((((m^2)^2)^2)^2)^2*m*(((m^2)^2)^2)^2$

$\mathrm{mod}(15\cdot50,119) \rightarrow 36$ $((((m^2)^2)^2)^2)^2*m*(((m^2)^2)^2)^2*(m^2)^2$

Tabel for 36^{29} (mod 119): $\mathrm{mod}(36^2,119) \rightarrow 106$ m^2

$\mathrm{mod}(106^2,119) \rightarrow 50$ $(m^2)^2$

$\mathrm{mod}(50^2,119) \rightarrow 1$ $((m^2)^2)^2$

$\mathrm{mod}(1^2,119) \rightarrow 1$ $(((m^2)^2)^2)^2$

Beregninger: $\mathrm{mod}(1\cdot36,119) \rightarrow 36$ $(((m^2)^2)^2)^2*m$

$\mathrm{mod}(36\cdot1,119) \rightarrow 36$ $(((m^2)^2)^2)^2*m*((m^2)^2)^2$

$\mathrm{mod}(36\cdot50,119) \rightarrow 15$ $(((m^2)^2)^2)^2*m*((m^2)^2)^2*(m^2)^2$

2.1

Tabel 22^{53} (mod 119):

$\mathrm{mod}(22^2,119) \to 8 \quad m^2$

$\mathrm{mod}(8^2,119) \to 64 \quad (m^2)^2$

$\mathrm{mod}(64^2,119) \to 50 \quad ((m^2)^2)^2$

$\mathrm{mod}(50^2,119) \to 1 \quad (((m^2)^2)^2)^2$

$\mathrm{mod}(1^2,119) \to 1 \quad ((((m^2)^2)^2)^2)^2$

Beregniger: $\mathrm{mod}(1 \cdot 22,119) \to 22 \quad ((((m^2)^2)^2)^2)^2 * m$

$\mathrm{mod}(22 \cdot 1,119) \to 22 \quad ((((m^2)^2)^2)^2)^2 * m * (((m^2)^2)^2)^2$

$\mathrm{mod}(22 \cdot 64,119) \to 99 \quad ((((m^2)^2)^2)^2)^2 * m * (((m^2)^2)^2)^2 * (m^2)^2$

Tabel 99^{29} (mod 119): $\mathrm{mod}(99^2,119) \to 43 \quad m^2$

$\mathrm{mod}(43^2,119) \to 64 \quad (m^2)^2$

$\mathrm{mod}(64^2,119) \to 50 \quad ((m^2)^2)^2$

$\mathrm{mod}(50^2,119) \to 1 \quad (((m^2)^2)^2)^2$

Beregninger: $\mathrm{mod}(99 \cdot 1,119) \to 99 \quad (((m^2)^2)^2)^2 * m$

$\mathrm{mod}(99 \cdot 50,119) \to 71 \quad (((m^2)^2)^2)^2 * m * ((m^2)^2)^2$

$\mathrm{mod}(71 \cdot 64,119) \to 22 \quad (((m^2)^2)^2)^2 * m * ((m^2)^2)^2 * (m^2)^2$

2.2

Opgave 3

Tabel for 5^{53} (mod 119):

$\text{mod}(5^2,119) \to 25$ m^2

$\text{mod}(25^2,119) \to 30$ $(m^2)^2$

$\text{mod}(30^2,119) \to 67$ $((m^2)^2)^2$

$\text{mod}(67^2,119) \to 86$ $(((m^2)^2)^2)^2$

$\text{mod}(86^2,119) \to 18$ $((((m^2)^2)^2)^2)^2$

Beregniger: $\text{mod}(18\cdot5,119) \to 90$ $((((m^2)^2)^2)^2)^2*m$

$\text{mod}(90\cdot86,119) \to 5$ $((((m^2)^2)^2)^2)^2*m*(((m^2)^2)^2)^2$

$\text{mod}(5\cdot30,119) \to 31$ $((((m^2)^2)^2)^2)^2*m*(((m^2)^2)^2)^2*(m^2)^2$

Tabel for 31^{29} (mod 119): $\text{mod}(31^2,119) \to 9$ m^2

$\text{mod}(9^2,119) \to 81$ $(m^2)^2$

$\text{mod}(81^2,119) \to 16$ $((m^2)^2)^2$

$\text{mod}(16^2,119) \to 18$ $(((m^2)^2)^2)^2$

Beregninger: $\text{mod}(18\cdot31,119) \to 82$ $(((m^2)^2)^2)^2*m$

$\text{mod}(82\cdot16,119) \to 3$ $(((m^2)^2)^2)^2*m*((m^2)^2)^2$

$\text{mod}(3\cdot81,119) \to 5$ $(((m^2)^2)^2)^2*m*((m^2)^2)^2*(m^2)^2$

3.1

Ingredienserne

Hvis tallet d går op i tallene a og b, siger man, at d er fælles divisor i a og b. For den største fælles divisor i a og b bruger man betegnelsen (a,b). Man kan bruge primtalsfaktorisering til nemt at udlede (a,b). Hvis (a,b) = 1 er a og b indbyrdes primiske, det vil sige, at det kun er tallet 1, som går op i både a og b. F.eks. er tallene $8=2^3$ og $21=7\cdot3$ indbydes primiske, da de ingen tal har tilfælles i primtalsopløsningen. 1 er derfor det eneste tal, som både går op i 8 og 21, altså er (8,21) = 1.

Modulo betegner den rest man får ved heltalsdivision. Med andre ord den hele rest, som fremkommer, når man dividerer to tal med hinanden. F.eks. er den hele rest for 13 divideret med 10 lig 3, da 10 går op i 13 én gang med 3 i rest. Generelt skriver man "mod" som betegnelse for modulo. F.eks. er $13 \pmod{10} \equiv 3$ og $11 \pmod{3} \equiv 2$.

Funktionen $\phi(n)$ betegner antallet af tal som både er lavere end n, og samtidig indbyrdes primske med n. F.eks. er $\phi(8) = 4$, da det kun er fire tal 1, 3, 5 og 7, som både er lavere end 8, og hvor ingen af tallene har nogen fælles divisor med 8 andet end 1. Altså er tallene indbyrdes primske med 8. [1]

Opskrift[2]

- *Vælg to store primtal p og q, beregn derefter $n=pq$ og $\phi(n)=(p-1)(q-1)$.*
- *Vælg det hele tal e, således at $0<e<\phi(n)$, og $(\phi(n),e)=1$.*
- *Beregn d således at $ed \equiv 1 \pmod{\phi(n)}$.*

Der er altid plads til et stykke til.

Bagning

Eksempel med små primtal: Først vælger man to primtal p=7 og q=17. Ud fra p og q finder man n ved at gange de to primtal med hinanden, dvs. n er lig $7\cdot17=119$.

Derefter kan man finde værdien for $\phi((96)$, ved at indsætte p og q i $\phi((n)=(p-1)(q-1)$:

$\phi(96)=(7-1)\cdot(17-1)=6\cdot16=96$.

Man vælger tallet e således at $0<e<96$ og $(e,96)=1$. Der er mange muligheder for e, da der jo er flere tal mindre end 96, som er indbydes primske med 96. Man kan vælge tallet 53, da man via. primfatorisering kan se, at 53 og 96 har 1 som største fælles divisor. Da 53 er et primtal kan dette tal pr. definition ikke primtalsfaktoriseres. Allerede her ved man, at 1 er det eneste tal som både kan gå op i 53 og 96, men nu primtalsfaktoriseres 96 alligevel for at vise at 53 ikke indgår. Primtalsfaktorisering af $96=3\cdot2\cdot4^2$, altså indgår 53 ikke og (53,96)=1 gælder.

Tilsidst har man den offentlige nøgle (n,e) = (119,53), og mangler kun den private nøgle, d. Man kan benytte d=29, hvilket opfylder at $ed \equiv 1 \pmod{\phi(n)}$ da $29\cdot53 \pmod{96} \equiv 1$.

Nu har man et fuldt nøglesæt bestående af den offentlige nøgle (n,e) = (119,53) og den hemmelige nøgle d=29, og man kan begynde at kryptere sin meddelelse.

1 Landrock, Peter: *Kryptologi*, s. 74, 83, 87-89.

2 Landrock, Peter: *Kryptologi*, s. 101-103.

Kryptering og dekryptering af L O V E

Meddelelsen er blevet omskrevet til tallet 12 15 22 05. Her er den kodede tekst blevet opdelt i blokke á to cifre, da det tal hver blok repræsenterer skal være mindre end n=119. Kryptereringen sker blokvis ved, at man benytter $c=m^e$

Skal man beregne $c=12^{53}$ (mod 119), dvs. den helrest man får ved at dividere 12^{53} med 119, opstår der hurtigt et problem. Man skal regne på et tal så stort, at det er udenfor lommeregnerens og computerprogrammers rækkevidde. Heldigvis kan man omskrive tallet 12^{53} ved at dele den høje eksponent op i "blokke" som hver især er potenser med eksponenten 2:[1]

$$12^{53} = 12\cdot 12^{52} = 12\cdot(12^{26})^2 = 12\cdot((12^{13})^2)^2 = 12\cdot((12^{12}\cdot 12)^2)^2 = 12\cdot(((12^6)^2\cdot 12)^2)^2$$

$$= 12\cdot(((12^6)^2)^2)^2\cdot(12^2)^2 = 12\cdot((((12^3)^2)^2)^2)^2\cdot(12^2)^2 = 12\cdot((((12^2\cdot 12)^2)^2)^2)^2\cdot(12^2)^2$$

$$= 12\cdot((((12^2)^2)^2)^2)^2\cdot(12)^2)^2)^2\cdot(12^2)^2.$$

Nu kan lommeregneren igen være med, og man kan tage modulo til hver blok. Det giver mest overskuelighed, hvis man opstiller en tabel.

Tabel:

$12^2 \equiv 25 \pmod{119}$	
$25^2 \equiv 30 \pmod{119}$	$(12^2)^2$
$30^2 \equiv 67 \pmod{119}$	$(((12)^2)^2)^2$
$67^2 \equiv 86 \pmod{119}$	$((((12)^2)^2)^2)^2$
$86^2 \equiv 18 \pmod{119}$	$((((12^2)^2)^2)^2)^2$

Man kan nu bruge tabellen til udregningerne:

$12\cdot 18 \equiv 97 \pmod{119}$	$12\cdot((((12^2)^2)^2)^2)^2$
$97\cdot 86 \equiv 12 \pmod{119}$	$12\cdot((((12^2)^2)^2)^2)^2\cdot(12)^2)^2)^2$
$12\cdot 30 \equiv 3 \pmod{119}$	$12\cdot((((12^2)^2)^2)^2)^2\cdot(12)^2)^2)^2\cdot(12^2)^2$

Man får altså $12^{53} \pmod{119} = 3$, dvs. c=03.

Vil man afkryptere c=03, må man bruge den omvendte funktion af $c=m^e$: $m=c^d \pmod{n}$.

Man beregner $m=3^{29} \pmod{119}$ ved samme metode som med krypteringen:

$$3^{29} = 3\cdot 3^{28} = 3\cdot(3^{14})^2 = 3\cdot((3^7)^2)^2 = 3\cdot((3^6\cdot 3)^2)^2 = 3\cdot(((3^3)^2\cdot 3)^2)^2$$

$$= 3\cdot(((3^3)^2)^2)^2\cdot(3^2)^2 = 3\cdot(((3^2\cdot 3)^2)^2)^2\cdot(3^2)^2 = 3\cdot(((3^2)^2)^2)^2\cdot(((3)^2)^2)^2\cdot(3^2)^2$$

Opstiller man sin tabel, kommer udregningerne til at se således ud:

$3\cdot 18 \equiv 54 \pmod{119}$	$3\cdot(((3^2)^2)^2)^2$
$54\cdot 16 \equiv 31 \pmod{119}$	$3\cdot((((3^2)^2)^2)^2\cdot((3)^2)^2)^2$
$31\cdot 81 \equiv 12 \pmod{119}$	$3\cdot(((3^2)^2)^2)^2\cdot(((3)^2)^2)^2\cdot(3^2)^2$

LOVE.

Nu er det fantastiske sket. Man får at $3^{29} \pmod{119} = 12$. Dvs. at dekrypteringen er lykkedes, da 12 var originalværdien.

1 Landrock, Peter: *Kryptologi.* s. 103-104.

eksportere.[19]

Truslen består i, at PGP på lige fod beskytter de lovlydige borgeres og forbrydernes private kommunikation. Politiet har store problemer, for de kan ikke længere benytte aflytning til at fange forbryderne. I modsætning til NSA mener Ron Rivest, en af opfinderne af RSA, ikke, at man skal begrænse kryptering bare fordi nogle forbrydere vil kunne udnytte den til deres fordel. Han påstår, at kryptering kan sammenlignes med handsker. Enhver amerikansk statsborger kan frit købe et par handsker, selvom en indbrudstyv vil kunne bruge dem til at plyndre et hus uden at efterlade fingeraftryk. Kryptografi er en teknik til databeskyttelse, ganske som handsker er en teknik til håndbeskyttelse.[20]

Der er mange perspektiver i denne sag. Den bedste løsning ville være, hvis man kunne tillade offentligheden og forretningslivet at bruge kryptering på en måde, som samtidig forhindrer forbrydere i at misbruge krypteringen. En sådan løsning er stadig ikke fundet, og kampen om kryptering fortsætter. Det er ikke til at sige, hvad udfaldet vil blive, men det store spørgsmål er stadig:

Hvis kryptering er blevet vores nye låse og nøgler, er vi så sikre?

Handsker forhindrer politiets fingeraftryksanalyse.

Af Pernille Græsholt

19 Landrock, Peter: *Kryptologi,* s.115
20 Singh, Simon: *Kodebogen*, s. 322

Diskussion

Popularisering af matematik er ikke en let opgave, da matematik ofte bliver betragtet som kedelig. Nogle mener, at 50% af læserne falder fra efter den første ligning i en tekst, og at den anden ligning dræber artiklen.[12] Jeg mener ikke, man kan generalisere matematiske tekster på den måde, men det er nødvendigt at begrænse teknisk sprog i sin artikel. Jeg har selv ladet to ligninger optræde i min artikel, da jeg ikke følte, jeg kunne demonstrere krypteringsprocessen uden.

Et andet problem opstår, hvis man står med svær matematik, som normalt kræver tid og koncentration at forstå. Jeg løb undervejs ind i et sådant problem, da jeg gerne ville have matematikken bag RSA med. Matematikken bag RSA-kryptosystemet er baseret på tre matematiske sætninger: *Eulers sætning, Fermats lille sætning og den kinesiske restsætning.*[13] Jeg ville gerne have haft beviset for Eulers sætning med i min artikel, da den forklarer, hvordan man finder frem til den matematiske sammenhæng mellem kryptering og dekryptering: $c^d \pmod n = (m^e)^d \pmod n = m^{ed} \pmod n = m$.

Eulers sætninger siger, at hvis (a,n) = 1 gælder, at $a^{\phi(n)} \equiv 1 \pmod n$

Man bruger sætningen til at bevise det sidste lighedstegn i $c^d \pmod n = (m^e)^d \pmod n = m^{ed} \pmod n = m$. Ud fra Eulers sætning, har man udledt sætning 3.1:[14]

3.1 For alle $a \in \mathbb{Z}$ og $s,n \in \mathbb{N}$ med (a,n) = 1 , gælder $a^s \pmod n = a^{s \pmod{\phi(n)}} \pmod n$.

Sætning 3.1 beviser at $m^{ed} \pmod n = m$, da det ud fra sætningen må gælde at $m^{ed} \pmod n \equiv m^{ed \pmod{\phi(n)}} \pmod n$ og da $ed \equiv 1 \pmod{\phi(n)}$ pr. definition, må $m^{ed \pmod{\phi(n)}} \pmod n = m^1 \pmod n = m$ (da $0<m<n$). Hermed er sætningen bevist.

Det ville være oplagt at tage beviset for Eulers sætning efterfulgt af det enkle bevis for $m^{ed} \pmod n = m$ med i artiklen. Desværre viste det sig, at beviset for Eulers sætning var knap så enkelt. Beviset kom hurtigt til at fylde alt for meget, hvis jeg skulle give en grundig og letforståelig forklaring. En af Briers "teser" om god populærvidenskabelig kræver, at trivialiserende fakta-formidling undlades.

---

[12] Hansen, Vagn L.: "Popularisering af matematik" in Aktuel Naturvidenskab, nr. 2, 2000 s. 34-35.

[13] Jankvist, Uffe T.: *Et undervisningsforløb i RSA og den heri anvendte matematiks historie*, 2007 s. 39.

[14] Landrock, Peter og Knud Nissen: *Kryptologi -fra viden til videnskab*, ABACUS, 1997, s. 90-91.

meget lav sikkerhed, da man på få minutter kan primtalsfaktorisere n=119, men det fungerer fint som illustration.

Er man blevet inspiret af de krypterede kærestebreve, eller vil man bare vise sin kærlighed på en lidt mere original måde, skal man følge godt med nu. Man krypterer meddelelsen "Love" ved først at give hvert bogstav det tal, der svarer til dets placering i alfabetet. På den måde bliver A=01, B=02…, Å=29. Det er vigtigt at bruge foranstillede 0'er, så man skriver alle bogstaver med to cifre.[14]

"Love" bliver nu til en kodet meddelelse i form af tal:

L O V E
12 15 22 05

Selve kryptereringen sker talvis, ved at man benytter at $c=m^e \pmod n$, hvor m er ens originalbesked, og c er den krypterede besked. Til krypteringen bruger man den offentlige nøgle som tilhører personen, som meddelelsen er tiltænkt. Men da det endnu ikke er muligt at slå offentlige nøgler op, må man i dette tilfælde bruge ovenstående offentlige nøgle. Beregner man $c=12^{53} \pmod{119}$ får man den krypterede udgave af første bogstav, L.

Krypterer man alle tal bliver meddelelsen 12 15 22 05 (LOVE) til den krypterede besked 03 36 99 31.[15] Man sender nu den krypterede meddelelse til den heldige mand, som kan dekryptere den med sin private nøgle. Skal han dekryptere beskeden, bruger han den omvendte funktion af den til krypteringen: $m=c^d \pmod n$, hvor m stadig er den rigtige besked, mens c er den krypterede.

Love never fails.

Når dekrypteringen er overstået, står han tilbage med den oprindelige meddelelse 12 15 22 05 lig "LOVE", og så vanker der nok et kys eller to.

Pretty Good Privacy

En sikker kryptering med n lig 10^{308} er meget vanskeligere at beregne, blandt andet fordi det er meget svært at finde så store primtal. Nogle vil nu tænke, *hvordan laver man så selv en sikker kryptering?* PGP er svaret. PGP[16] blev designet af Phil Zimmermann. Zimmermann drømte om at gøre kryptering tilgængelig for alle. RSA er grundstenen i PGP, og målet var at lave et program, hvor den svære proces med at skabe et nøglesæt blot var nogle klik væk. PGP endte med at blive en blanding af et asymmetrisk og et symmetrisk kryptosystem. Zimmermann udnyttede sikkerheden i det asymmetriske RSA og af hurtigheden i det symmetriske system IDEA.[17] Han havde som den første, taget det bedste fra allerede opfundne kryptosystemer og sat det sammen til et brugervenligt computerprogram. I 1991 placerer Zimmermann programmet som frit tilgængeligt software på internettet. Verden over spreder PGP sig som en løbeild.

Udbredelsen af PGP vakte stærke følelser hos kryptografer, politikere, borgerretsforkæmpere og lovhåndhævere. Modstandsgrupper i Burma, menneskerettighedsgrupper i Guatemala og eksilregering i Tibet lovpriste PGP. Førhen havde beslaglagte ukrypterede dokumenter garanteret arrestation, totur og i værste tilfælde henrettelse.[18]

Folk havde endelig et middel til at beskytte deres privatliv, og derved dem selv. Men hvis kryptering virkelig er blevet vor tids nøgler og låse, hvorfor vil nogen så forhindre os i at kunne bruge låsen?

Kryptering er vores nye nøgler og låse.

Ingen roser uden torne

I USA mener National Security Agency, NSA, at PGP udgør en alvorlig trussel. Kryptologisk software står således side om side med missiler, bomber og maskingeværer på en liste af produkter, som man ikke må

14 Landrock, Peter: *Kryptologi,* s.103
15 Se bilag
16 Singh, Simon: *Kodebogen*, s.312
17 Landrock, Peter: *Kryptologi,* s.115
18 Singh, Simon: *Kodebogen*, s. 316-317

Kemi : 10↑
Mat : 10↑

- Sprogligt lidt rodet.

0-LineBedømmelse

KARAKTER: 10????

Indledning. Begrænser opgaven. Fint.
Klar struktur
Litteraturliste OK. Ingen matematikbøger!
KOnklussion samler i store træk op på hele opgaven

Teori: Klar fremstilling

Spektrofotometri: Overskueligt. Jeg forstår ikke det mere kemiske.

{ rigtig godt (exitere π-elektron, gode forklaringer, nævn konjugerede dobbeltbindinger, når anv. af L-B lov → bør absorbansen ligge inde for det intermediære område.)

Promilleberegner:
Udmærket.

Lambert-Beer

i formlen s 10 er x vist i ml mens x på grafen er i g $\frac{100}{60 \times 0.55}$ $\frac{100}{33}$ 3.030303030303

Tallene passer med at x i grafen er i gram. } Ja det er noget rod! Det eneste af

Differentialligning (for nedbrydning af alkohol)
Fint

Differentialligningen for nedbrydning af THC
Smukt. Klar formulering. Omskrivning. Grafisk tolkning. Løsning.
Men hendes EXCEL-grafer er vist lidt for "bulede".
Mangler vi ikke gyldighedsområdet? jo!! $x > 0$?

Det står indirekte fx mojst 4-5‰ s. 14 øverst.

Forsøgsrækken har jeg svært ved at kommentere. Jeg forstår ikke udregningerne. Det ser pænt og overskueligt ud. Det er fint. overskueligt!

Hun svarer på alt hvad hun bliver spurgt om.

Klar og formålsrig opdeling af besvarelsen
"rød tråd".
Sproglig formulering i top ←
Høj fagligt niveau
teorien for forsøgene forklares tip, top. → Forsøgsgangen beskrives flot og systematisk.
Kemisk sprog i top.
Kan inddrage sin kemiske viden fra den daglige undervisning.
Lidt svag konklusion.

Go

SRP-Pernille HD Kryptering

Fremragende opgave.

Det lykkes hende at fastholde et populærvidenskabeligt niveau og samtidig fastholde et rimelig matematikfagligt indhold.

Hun redegør grundigt for de valg hun har foretaget og får endda introduceret Eulers sætning og Fermats lille sætning i kommentaren.

Der er en del hun IKKE får med, som man vil forvente inden for dette emne, men det er alt sammen velbegrundet og kommenteret.

Den formidlingsmæssige del virker grundig og hendes brug af den på det matematiske stof viser en god faglig fornemmelse.

Jeg har svært ved at se hun kunne gøre noget bedre bortset fra at hun gerne måtte have nævnt

a*b mod n = (a modn) *(b mod n)

Det formelle i opgaven er fint

Hun får formidlet et matematisk kompliceret stofområde forståeligt

Karakter: 12 Jeg har svært ved at se hvad der skal trække ned.