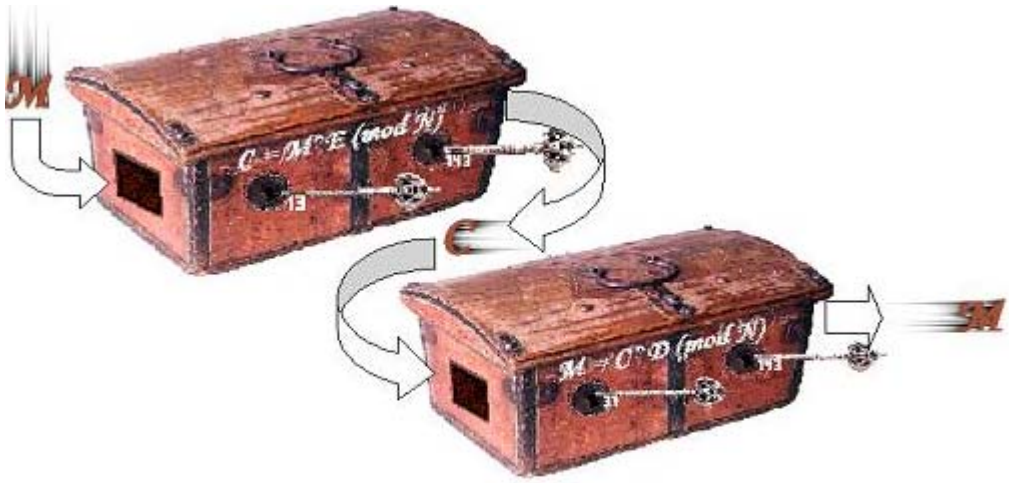
Hvordan brukes kryptering?



Samfundets Skole
Kristiansand
april 2006

Prosesslogg

Hvordan klassen kom frem til problemstillingen

November 2005

På høsten brukte vi mye tid for å komme frem til en god problemformulering. Vi startet med idéfasen. Ordet ”kommunikasjon” ble drøftet, og vi ble enige om at det har noe med å sende ei melding fra en avsender til en mottaker. Det kan skje med vanlig språk eller andre slags språk. Men det er også mange andre måter som en kommuniserer på i dag, ikke minst innen elektronisk utstyr. Følgende forslag til prosjekt ble nevnt: *tegnspråk, røverspråk (gatespråk som ble brukt i Kristiansand for 50-100 år siden), strekkoder, minibank, GPS, GPRS, e-post, MSN, Blink, mobilabonnement, kryptering i nettbank, inn-logging, bankkort, Internett, Julius Cæsar, voksent snakk, copyright på spill.* Vi diskuterte for og imot de ulike ideer, og flere og flere ble interessert i kryptering. Dette var et emnet vi visste lite om, men vi kjente til at kryptering ble brukt i dataverdenen. Ved avstemming ble vi enige om følgende prosjektformulering: *”Hva er kryptering?”* Som underemner valgte vi*: kryptering i nettbank, røverspråket, historisk kryptering, strekkoder og minibank.*

Desember 2005

Like før juleferien drøftet vi igjen problemstillingen og fant ut at formuleringen ikke var den beste. Hvis vi fant en definisjon i leksikon eller på Internett, var plutselig prosjektet over. Og hvordan kunne vi få inn matematikk i dette? Vi prøvde å komme frem til et bedre spørsmål. Disse forslag ble nevnt: Hvordan virker kryptering? Hvordan brukes kryptering? Hvordan kan en tyde kryptering? Hvorfor brukes kryptering? Etter ny diskusjon og avstemming, valgte klassen: ***”Hvordan brukes kryptering”.*** Vi mente at det var et mye bedre spørsmål, for her kunne det bli flere svar. Vi trodde også at det ville bli et godt prosjekt hvis vi kunne få med flere fag, for eksempel samfunnsfag, naturfag, norsk. Men matematikk var jo det viktigste, siden emnet hette ”Matematikk og kommunikasjon. Det var også muligheter for å studere ulike sider ved kryptering ved en slik problemformulering. Underveis i denne prosessen var det flere sider ved kryptering som enkelte elever var blitt interessert i. Klassen delte seg i 6 grupper, og vi valgte disse utdypende spørsmål: ***Hva er egentlig kryptering? Hvordan virker kryptering? I hvilke sammenhenger brukes kryptering? Hvorfor begynte mennesker å kryptere? Hvor kjent er kryptering? Hvor lett er kryptering?***

Hva som er gjort under hver arbeidsøkt

2005

Oktober – (0,5 timer)

Vi drøftet i klassen om vi skulle være med på KappAbel.

7. november – (1 timer)

Prosjektets idéfase. Hva ønsket vi å forske på som kunne hører inn under emnet: ”Matematikk og kommunikasjon”? Flere forslag ble nevnt og notert.

9. november (1 time)

Vi trener på gamle KappAbel-oppgaver i matematikktimen.

11. november (1 time)

Klassen drøftet igjen forslagene som var kommet frem i idéfasen 7.11. Nye forslag ble nevnt og mange gamle forslag ble strøket. Til slutt var det flere som ville ha noe om kryptering, men det var mange andre emner som også var aktuelle.

14.november (2 timer)

Vi gjennomførte en konkurranse med gamle KappAbel-oppgaver. Det gav oss god trening før det var alvor den 21.11.

21. november (2 timer)

KappAbel 1. runde

30. november (1 time)

Vi valgte problemformuleringen: ”Hva er kryptering?”, og vi valgte ut fem underpunkter som vi ville undersøke.

16. desember (2 time)

Vi gjennomgikk prosjektarbeidsmetoden og hva som kjennetegner et godt prosjekt. Vi diskuterte videre vårt prosjekt. Elevene fra 9. klasse i fjor som var med under finalen i Arendal, var på besøk og fortalte om sitt prosjekt: ”Kan skjønnhet måles?” De gav oss mange gode ideer.

19. desember (1 time)
Vi drøftet vårt prosjekt og fant ut at ”Hva er kryptering” kanskje ikke var den beste problemformuleringen. Hva skulle vi da velge? Mange forslag ble nevnt og vi skulle tenke på det til i morgen.
20. desember (2 timer)
Etter diskusjon og avstemming valgte klassen: ”Hvordan brukes kryptering”. Klassen delte seg i 6 grupper. Hver gruppe valgte et spørsmål som kunne utdype hovedproblemformuleringen. Vi diskuterte også hvordan vi skulle undersøke dette.

2006
9. januar (2 time)
Klassen hadde 6 grupper med 4 elever på hver gruppe. Hver gruppe valgte sekretær og leder. Gruppen laget flere hypoteser til sitt emne. Denne dagen startet noen av gruppene med undersøkelser. Noen ringte til HiA og Universitetet i Oslo. I Forsvaret fikk vi mye informasjon om morsing. Gruppe B laget ny hypotese: ”Vi tror at morsing er kryptering”. Nå var det viktig å finne en riktig definisjonen på kryptering.
13. januar (2 timer)
Internett var flittig i bruk og her fant vi noen interessante opplysninger angående kryptering. Vi brukte også leksikon. Et par elever skulle prøve å søke etter personer som kanskje kunne noe om dette emnet og som klassen kunne sende spørsmål til. En gruppe laget en krypteringstest. De ønsket å undersøke hvor lett eller vanskelig kryptering egentlig er. Denne dagen og dagene etterpå var det flere elever som ble testet.
16. januar (2 time)
Et par elever gikk på Kristiansand Folkebibliotek og lånte ”Koder” av Simon Singh, og ”Kryptografi” av Ben Jonshen. Noen av elevene skulle prøve å lese gjennom bøkene. Klassen gjennomførte igjen en konkurranse med gamle KappAbel-oppgaver for å være oppvarmet til mandag 23.1.
18. januar (1 time)
Flere av gruppene brukte Internett for å lete etter opplysninger om kryptering. Det vi fant ut, ble lagret i mappene våre. Vi lette fortsatt etter en god definisjon på krytering.
20.januar (2 timer)
Et par elever var igjen på Folkebiblioteket og ville låne bøker. Men noen leksikon med masse opplysninger om kryptering kunne vi ikke låne med oss hjem. To av elevene lagde et dokument om hva kryptering egentlig er. En av gruppene hadde funnet svar på en av hypotesene: ”Kryptering er at du koder ei melding slik at ingen andre skjønner det, og sender det til en mottaker. Mottakeren må ha en kode-nøkkel for å finne ut av meldingen.” Derfor er morsing ikke kryptering. Ny hypotese: Det er matematikk i mye av kodene til kryptering. Vi sendte e-post til noen som har erfaring med kryptering. Vi fortsatte å lese bøkene vi hadde lånt, og fant mye interessant om historisk kryptering.

23. januar (2 timer)
KappAbel 2. runde
25. januar (1 time)
Vi jobbet igjen videre med boken om Kryptografi og Koder. Det vi spesielt leste om, var runer og kryptering før i tiden. Vi fant mye som interesserte oss alle, og vi skrev også litt notater fra det viktigste vi leste.
3. februar (2 timer)
Timene i dag ble brukt til å føre inn mye av det vi hadde funnet ut. Vi fikk orden på notatene våre
6. februar (2 timer)
Vi fortsatte å føre inn våre resultater Hvilke kilder vi hadde brukt ble også ført inn. En del av elevene var ferdige med sine oppgaver og jobbet med vanlige matematikkoppgaver.
15. februar (2 timer)
Enkelte grupper jobbet videre med intervju eller rapport. De fleste begynner nå å bli ferdige.
uke 10 og 12 (0-8 timer)
Enkelt-elever og elevgrupper finpusser på sin del av rapporten.
29. mars (1 time)
Klassens konklusjoner ble forfattet og avslutning på prosjektet.

Hvilke faglige problemer som oppstod og hva som ble gjort for å løse dem

Hvordan gjennomføre et godt prosjekt?
Det første problemet var å finne en god problemformulering på et prosjekt. Klassen hadde vært med på et prosjekt innen Nysgjerrigper i 7. klasse. Vi ønsket å bruke samme fremgangsmåte denne gangen og vi repeterte prosessen: problemformulering – hypoteser - planlegge undersøkelser - bearbeide og analysere data – oppsummering / konklusjon - fortell for andre.

Hvordan matematikken plutselig ble veldig vanskelig?

Fra begynnelsen jobbet vi med at bokstavene ble gjort om til tall. a=1, b= 2 osv. Dette tallet ble kodet med for eksempel + 5 eller x 4. Men dette var ikke så vanskelig matematikk. Underveis var det noen som fant ut at det var to slags kryptering: symmetrisk og asymmetrisk. På den første måten brukte en koder som + 5. Og da ble det løst ved å ta – 5 for å finne løsningen. Men i det andre tilfelle ble det brukt en kode for å kryptere meldingen, og en annen kode for å løse den opp. En skulle bruke både potensregning som vi hadde lært i høst og noe ukjent som hette modulus-regning og her måtte læreren forklare

Asymmetrisk kryptering med potens og modulus-regning
Bokstavene ble gjort om til tall (for eksempel b=2) Vi fant eksempler på tre nøkkeltall: 13, 37 og 143 som vi skulle bruke til krypteringen. For å kryptere måtte en ta 2^{13} og dele det på 143. Restverdien på dette delestykke var 41 og det var den krypterte meldingen. Mottakeren skulle da ta 41^{37} og dele det på 143. Restverdien ble da 2 som tilsvarte bokstaven b. Men nå fikk vi problemer med regnearket på datamaskinen. Tallene ble for store og regnearket valgte avrunding. Da fikk vi ikke riktige svar.

HiA hjalp oss
Vi tok kontakt med Høgskolen i Agder. De foreslo å dele opp potensstykke i flere potensstykker og finne restverdien til hvert delestykkestykke. Da ble det mindre tall som regnearket kunne klare. Når vi multipliserte disse restverdiene, måtte vi igjen dele svaret på 143 for å få restverdi.

Hvordan samarbeidet har fungert

Vi opplevde at ikke alle gruppene arbeidet like ivrig med prosjektet, og det viser også rapporten. Noen har fått mye til og andre lite. Det var heller ikke alle gruppene som fungerte 100%, noen elever kunne ødelegge samarbeidet. Klassen hadde mange ideer, men det var ikke så mange som tok ansvar for å løse alle disse ideene. Men likevel opplevde vi et spennende prosjekt der flere i klassen har gjort veldig mye.

Hvordan vi elever vurdere arbeidet som er gjort

Vi synes vi har valgt et litt spesielt prosjekt og er veldig spent på om flere klasser har valgt det samme eller hvordan de har tolket temaet: Matematikk og kommunikasjon. Da vi startet med prosjektet, visste vi ikke hva dette gikk ut på. Vi fant først en del om enkel kryptering, men etter hvert ble det mer og mer spennende når vi gikk videre med prosjektet. En del av tiden gikk med til fordypning av enkelte områder for eksempel RSA-systemet og asymmetrisk kryptering. Kryptering og regning med både potenser og modulus er ikke så veldig vanskelig når en har arbeidet med det.

Vi opplevde at ikke alle var like systematiske og flinke til å skrive i loggen. Vi var heller ikke alltid like nøye med å gjennomføre de undersøkelser vi hadde planlagt. Noen ganger kom vi over noe annet som vi hoppet på og som ikke var planlagt. Enkelte av oss tok ikke heller ansvar for at tingene ble gjort, og da vi skulle levere rapporten, var det mange ting vi burde hatt med som vi bare hadde begynt på og ikke fullført.

Hva har vi lært? Vi har lært veldig mye om kryptering som vi ikke visste fra før. Men vi har også lært mye samarbeid og mye matematikk. Vi har også fått enda mer øvelse i de forskjellige delene som hører til et prosjekt: problemformulering, hypoteser, planlegge undersøkelse, gjennomføre

undersøkelse, oppsummering, konklusjon og rapportskriving. Vi synes også det er positivt at vi har utnyttet hverandres evner. Noen var flinke på regneark, og de laget flotte krypteringsprogrammer. Andre var flinke på Internett og fant fram til mange opplysninger. Vi har også noen som kan lage animasjonsfilmer, og vi overtalte læreren til å kjøpe et dataprogram slik at vi nå har klar en spennende film til fremføringen i Arendal. Noen i klassen er dyktig i tegning og forming, og disse har også gjort mye bra. Figuren vår heter Abeluss, og han hjelper oss med vanskelig matematikk!

Faglig rapport

Forord

Temaet i år var *Matematikk og kommunikasjon*. Vi valgte å fordype oss i kommunikasjon, der en beskjed sendes fra en person til en annen. Som problemformulering har vi valgt *Hvordan brukes kryptering*? Da vi valgte kryptering, så tenkte vi på at denne beskjeden skal være hemmelig for alle andre enn sender og mottaker. Vi har også valgt å fordype oss i kryptering der tall og matematikk brukes. Er den matematikken som brukes i dagens kryptering forståelig for oss i 9. klasse? Hvordan går det an å lage en melding som er 100 % uleselig for alle andre enn den som kjenner systemet? Går det likevel an å knekke koden? Eller kan en lage et fullstendig uløselig system? Er kryptering noe nytt fra vår tid?

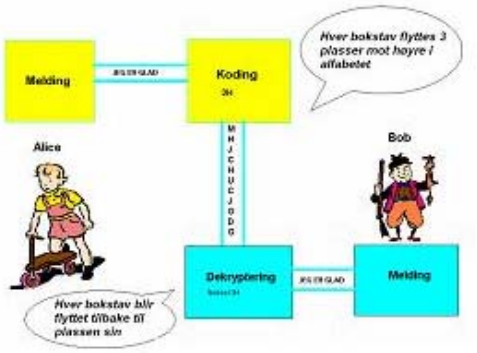
Hoveddel

Klassen delte seg i 6 grupper som arbeidet med hver sine spørsmål som skulle utdype prosjektets problemformulering.

Gruppe 1:: Hva er egentlig kryptering?

Hypoteser:

- Vi tror kryptering er et hemmelig språk.
- Vi tror kryptering er en hemmelig måte å snakke på.



Planlegging av undersøkelser:

Vi vil snakke med skolens IT-ansvarlig. Vi ville også prøve å finne andre personer som kunne noe om kryptering. Ellers regnet vi med å bruke Internett og leksikon. En spørreundersøkelse var også aktuell. Vi laget så følgende stikkord til vårt arbeid: Hva er og hva er ikke kryptering? Hva må til for at det skal være kryptering? Forskjellige former for kryptering? Definisjoner av kryptering. Talemåter: tegnspråk, dyrespråk.

Dette har vi funnet ut: Ordet kryptering kommer fra kryptografi som er gresk og betyr skjult skrift. Kryptering er en flere tusen år gammel metode for å skjule innholdet i en skriftlig beskjed eller dokument. De første krypterings metodene gikk ut på å flytte bokstavene i alfabetet ett vist antall plasser. For å kunne lese (dekryptere) et skjult innhold må man ha en nøkkel. Nøkkelen fortalte hva som måtte gjøres for å få fram den virkelige teksten. En nøkkel kan for eksempel være 3H. Det vil si at forskyvningen av alfabetet var 3 bokstaver til høyre. Moderne kryptering bruker mer avanserte og matematiske funksjoner for å forvrenge innhold i dokumenter eller meldinger. Moderne kryptering er også avhengig av datamaskiner for å fungere.

Ny hypotese: Det fins flere måter å kryptere på

Dette har vi funnet ut: Krypteringsmetodene blir oftest delt inn i to:

Symmetrisk kryptering: Her brukes samme nøkkel ved kryptering og dekryptering av data. Dette fører til at nøkkelen må utveksles mellom avsender og mottaker av den krypterte meldingen på en sikker måte. Symmetrisk kryptering kan ogs¨deles inn i to typer: blokksiffer og strømsiffer. Blokksiffer krypterer en blokk av et bestemt antall bits om gangen, mens strømsiffer krypterer én og én bit.

Asymmetrisk kryptering: Dette er også kalt offentlig nøkkel-kryptering for den benytter to slags nøkler: offentlige og private nøkler. Når en person (Alice) skal sende en melding til en annen person (Bob), kan dette gjøres ved at Alice bruker Bobs offentlige nøkkel til å kryptere dataene som skal sendes. Disse kan da kun dekrypteres med Bobs private nøkkel og er derfor bare leselig for Bob. Asymmetrisk kryptering kan også brukes for å finne ut hvem som har sendt data. Dette gjøres ved at Alice krypterer dataene med sin private nøkkel slik at de bare kan dekrypteres med hennes offentlige nøkkel. Dette fører til at alle kan lese dataene, og de er sikre på at dataene kommer fra Alice siden det kun er hun som har tilgang til den private nøkkelen. Ved å slå sammen disse to metodene kan man sikre at ingen uvedkommende kan løse den hemmelige meldingen, heller ikke endre den, og en har en metode slik at avsenderen kan ikke nekte for å ha sendt dataene.

Koding og chiffrering er også to ulike måter å kryptere på:

- Kode er å kryptere slik at hele ord eller setninger blir gjort om til andre symboler eller ord.

- Enchiffrere betyr å kryptere en tekst ved hjelp av chiffer slik at hver bokstav blir erstattet med noe annet. Chiffer-alfabetet kan bestå av tall, bokstaver eller hvilket som helst tegn, men i alle tilfeller er det bestemt hva som skal erstatte bokstavene i den opprinnelige meldingen.

Før en melding er kryptert, blir den kalt klartekst og etter kryptering heter den chiffertekst. Utrykket kryptering kan bety både å enchiffrere og kode.

Gruppe 2: Hvordan virker kryptering?

Hypoteser:

Kryptering virker slik at bokstaver blir til tall.
Kryptering virker slik at en kode blir sendt av gårde.
Kryptering virker slik at en bokstav eller et tall blir til en lyd (morsing)
Kryptering virker slik at en bokstav blir byttet ut med en annen bokstav.
Kryptering virker slik at noe blir kodet slik at ingen kan se det når det sendes

Dette planla vi:

Vi ville spørre IKT-ansvarlig i Spareskillingsbanken. En i gruppa skulle finne ut noe mer om forskjellige typer kryptering på Internett. En annen skulle lese om kryptering.

Stikkord til vår undersøkelse:

Hvordan fungerer kryptering i minibank? Hvordan kodes det? Hvordan kodes det i nettbank?

Dette har vi gjort:

Vi har ringt til sjøforsvaret, HIA, universitetet i Oslo, og sendt e-post til folk som vet noe om emnet. Vi har også blant annet sett litt på Internett.

Dette har vi funnet ut:

Det finnes to måter å kryptere på, symmetrisk og asymmetrisk. Vi har også funnet ut at morsing ikke er kryptering fordi det er noe som alle kan lære, det er som et annet språk. Vi trodde at kryptering virket slik at noe blir kodet slik at ingen kan se det når det sendes, men det er feil. Alle kan se at det blir sendt noe, men det går ikke an å tyde det.

Ny hypotese:

Kryptering virker slik at det må være matematikk i det.
Vi tror det fins en kryptering som er fullstendig uløselig.

Dette har vi funnet ut:

Vi har funnet ut at RSA-systemet er en form for kryptering der det brukes mye matematikk. RSA er en asymmetrisk kryptering og er nesten uløselig. Verdens beste datamaskiner må bruke mange år for å komme frem til en løsning. Symmetrisk kryptering kan også bruke mye matematikk, men da har avsender og mottaker den samme nøkkelen. Detter er letter å løse. Fra Heimevernet fikk vi rede på at analog tale blir gjort om til digitale impulser (1 og 0-tall) som blir kryptert og sendt av gårde til den som skal motta det. Her bruker mottakeren den samme nøkkelen, og de digitale impulsene blir gjort om til analogt igjen og blir til tale igjen.

Fins det en kryptering som er uløselig? Ja, kvantekryptering. Det er en form for kryptering som skal være teoretisk umulig å knekke. Dataen sendes som fotoner eller lys, som går i forskjellige retninger. Hvis en hacker skulle prøve å gripe tak i datastrømmen, vil lysene bare skifte retning og dataen blir uleselig. Selv om krypteringsmetoden blir omtalt som "teoretisk umulig å knekke", er den likevel ikke 100% sikker, fordi dataen i teorien kan snappes opp før og etter den sendes.

Hvordan finner vi nøklene i RSA-systemet?

- Vi trenger tre nøkkel-tall N, D og E for å kryptere i RSA-systemet.
- Først velger vi to primtall: 11 og 13 . Nøkkel **N** blir da 11*13 **= 143**
- Du trenger også et tall **X** som er (11-1)*(13-1) = 10*12**=120**
- Nøkkel E og X må ikke ha felles faktorer med unntak av 1
- Hvis du tar E*D og deler dette svaret på X, må restverdien på delestykket være 1.
- Vi velger E=13 og D=37 fordi E*D=481 (test: 481:120 = 4 og 1 til rest)

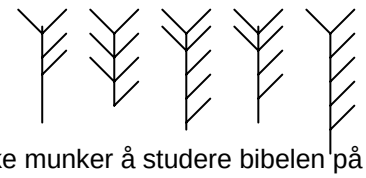
Bankene som bruker RSA-systemet, starter med mye større primtall, gjerne tall med 100-200 siffer.

Gruppe 3: I hvilke sammenhenger brukes kryptering?

Hypotese:
Vi tror politiradioen bruker kryptering.
Dette planla vi:
Først skulle vi stille noen spørsmål til politiet om kryptering. Så hadde vi også lyst til å lete etter krypteringsmotorer på Internett.
Dette har vi funnet ut:
Politiet bruker kryptering til Telefaks og PC-er, men ellers er ingen ting kryptert. Det er flere som har laget kryteringsmotorer på Internett. Vi fant denne som vi likte svært godt: http://www.javascriptkit.com/script/script2/encrypt.shtml

Gruppe 4: Hvorfor begynte mennesker å kryptere?
Hypoteser:
Vi tror de begynte å bruke det i krig.
Vi tror de begynte å bruke det for å holde ting hemmelig
Vi planla følgende undersøkelse: Spørre noen vi kjenner om historie og kryptering, kanskje skolens IT ansvarlig. Spørreundersøkelse om historisk kryptering. Spørre folk på HIA om hvorfor mennesker begynte å kryptere. Spørre eldre folk om de husker om det ble brukt kryptering i krigen. Lese i leksikon. Se etter på internett om vi finner noe interessant der.
Vi gjorde disse undersøkelsene:
Først ringte vi til universitetet i Oslo. De visste lite om historisk kryptering. Dette overrasket oss ganske mye. Vi ble sendt fram og tilbake mellom forskjellige fagfolk, men de viste lite eller fortalte oss ting vi allerede visste. Vi var på biblioteket og lånte noen bøker. *Kryptografi – den hemmelige skriften* av Ben Johnsen. Vi lånte også *Koder* av Simon Singh.

Dette har vi funnet ut: Folk brukte kryptering som et hemmelig språk for å kommunisere med hverandre. I krig brukte de ofte kryptering. Hvorfor begynte mennesker å kryptere? Fordi informasjon kan sikres ved at den krypteres. Ingen andre får vite det uten at de knekker koden. Da det var krig i romerriket, ble Cæsar tilkalt. Krypteringa han brukte var å skrive på gresk slik at ingen forsto det. Da mottakeren fikk meldingen, forstod han det fordi han kunne gresk. Cæsars chiffer er at du skal sette inn fjerde bokstav i alfabetet. Det vil si D for A og E for B osv. Keiser Augustus chiffrerte tilsvarende, ved å forskyve alfabetet 2 trinn. Slike systemer som Julius Cæsar brukte, kalles substitusjonssystem. Hver bokstav erstattes fast med en annen bokstav. Ett alfabet kunne også erstattes av et annet, som da det latinske ble erstattet av det greske. Julius Cæsar var en av historiens første som skrev kryptiske meldinger. I mange år har konger og generaler kryptert. Det er den eneste måten som de kunne beskytte hemmeligheter på. Det var ikke mange som har stor kunnskap om kryptering. Kryptografi handler om kommunikasjon.
Vi fant ut at kryptografi også ble brukt i runeinnskrifter. Runegåtene var skjult i mange år, men i 1963 ble det fremsatt et forslag til løsning. Runene ble brukt av germanske stammer i de første århundrene e.kr. Det fins flere varianter av runealfabetet. I vikingtiden var det på 24 tegn. Et yngre runealfabet var forenklet til 16 runer. For å kryptere runeskriften, delte de alfabetet inn i grupper på 6-5-5 bokstaver. Et runealfabet kunne da se slik ut: *fu(th)ork : hnias : tbmlR*
Hvis de skulle kryptere ordet "thlsar" gjorde de om bokstavene til to tall. Det første tallet fortalte hvilken gruppe det tilhørte og det andre tallet fortalte hvilken plassering bokstaven hadde i sin gruppe. Eksempel: **o** ble til 1.4 og **i** ble til 2.3. - (th)lsar: ble da kryptert til 1.3 – 3.4 – 2.5 – 2.4. – 1.5. Som runeskrift så det slik ut:



På 800 tallet begynte arabiske munker å studere bibelen på jakt etter skjulte meninger. De var fascinerte av Det gamle testamentes kryptografi. Det var klare eksempler på kryptering og metoden som ble brukt heter atbash. Den går ut på at du gir hver bokstav ett tall etter hvor de er plassert i alfabetet. A = 1, B = 2 også videre. Så snur du alfabetet og gir den siste bokstaven 1, mens den første bokstaven får 29. Når du har gjort det bytter du de bokstavene med samme tall med hverandre.

Da blir A til Å og B blir Ø også videre. I Jeremias 25,26 og 51,41 finner man eksempler på atbash. Navnet Babel skrives Sheshach. Den første bokstaven i Babel B eller beth som den heter på hebraisk, blir erstattet med den nest siste i det hebraiske alfabetet shin. Den siste bokstaven i Babel, L eller lamed som er nummer tolv blir erstattet med den hebraisk bokstaven kaph som er nummer tolv bakvendt. De fleste mener at krypteringen i bibelen ikke ble laget for å skjule innholdet, men som et mystisk element i teksten. Dette funnet førte til at mange ble interessert i virkelig kryptografi.
Omkring 1905 i forbindelse med unionsoppløsningen, måtte kommunikasjonslinjene sikres. Det kom

en krypteringsmaskin som ble kjent som Strømdahls kryptograf. Den bestod av 2 metall skiver som kunne dreies om en felles akse. Langs kantene på skivene var bokstavene fra A til Ø skrevet inn i alfabetisk rekkefølge, men motsatt vei. Et av de viktigste våpnene til Nazi-Tyskland var Enigma, en maskin som kunne krypterer meldinger. Den mest avanserte Enigma maskinen var så vanskelig å knekke kodene på, at tyske ubåter kunne kommunisere fritt med de, uten at de allierte skjønte noe av det. Britene brukte store ressurser på å prøve å knekke kodene. Det var et hovedkvarter i England for matematikere som jobbet hardt, men til slutt fikk de tak i en maskin og kodebøker, og da klarte de å knekke de fleste kodene. 60 år etter 2.verdenskrig klarte noen amatører å knekke de kodemeldinger som de allierte måtte gi opp.

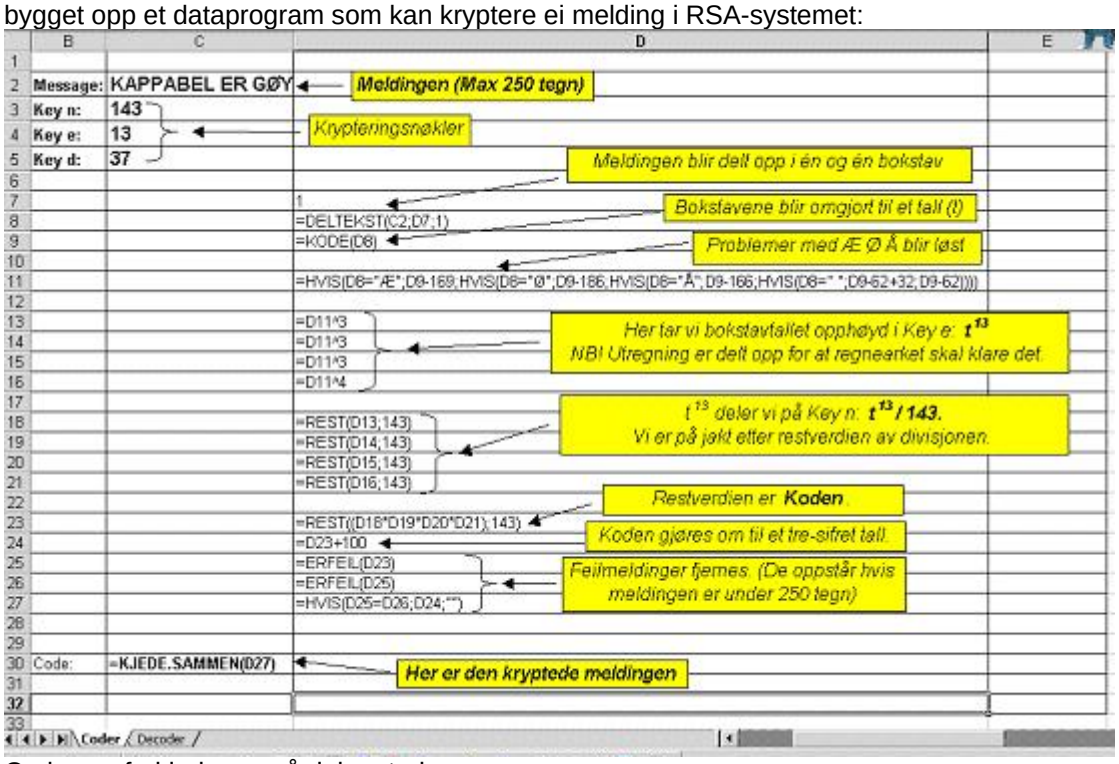
Gruppe 5: Hvor kjent er kryptering?
Hypotese:
Vi tror at folk ikke kjenner selve ordet ”kryptering”
Vi planla følgende undersøkelser: En spørreundersøkelse: Vet du hva kryptering er?
Hva vi har gjort:
Vi gikk på byen og spurte 72 personer om de visste hva kryptering var.
Dette har vi funnet ut:
19 personer svarte ”ja” at de visste hva kryptering var, mens 53 svarte ”nei”. Det gir 26,4% ja og 73,6 % nei. Det viser at ikke mange mennesker vet noe om kryptering.

Gruppe 6: Hvor lett er kryptering?
Hypotese
Det kommer an på måten en krypterer på
Vi planla disse undersøkelsene
spørreundersøkelse – test, lage kryptering på data, krypteringsspill
Hva vi har gjort: Vi har laget en undersøkelse, med forskjellige oppgaver. Der tester vi mange mennesker for å se hvor vanskelig det er med kryptering. Vi laget også et spill som vi har kaldt *Krypteringsfjellet.* Det er 5 forskjellige vanskelighets grader. En på gruppen laget et regneark der en kunne kode om ei melding.
Dette har vi funnet ut:
Vi har jobbet litt med å knekke matematikken i asymmetrisk kryptering. Og vi laget et regneark som tok for seg denne utregningen både til kode og dekrytering tilbake til meldingen. Vi laget et regneark som kunne klare ei melding på 200 tegn! Se vedlegg.
Asymmetrisk kryptering fungerer på denne måten: Hvis Ole skal sende ei melding til Janne, trenger de til sammen tre nøkler: Disse nøklene fant vi som kan brukes i asymmetrisk kryptering: N =143, E = 13 og D 37. En an de andre gruppene fant hvilke regler som gjelder og forholdene mellom nøkkeltallene.

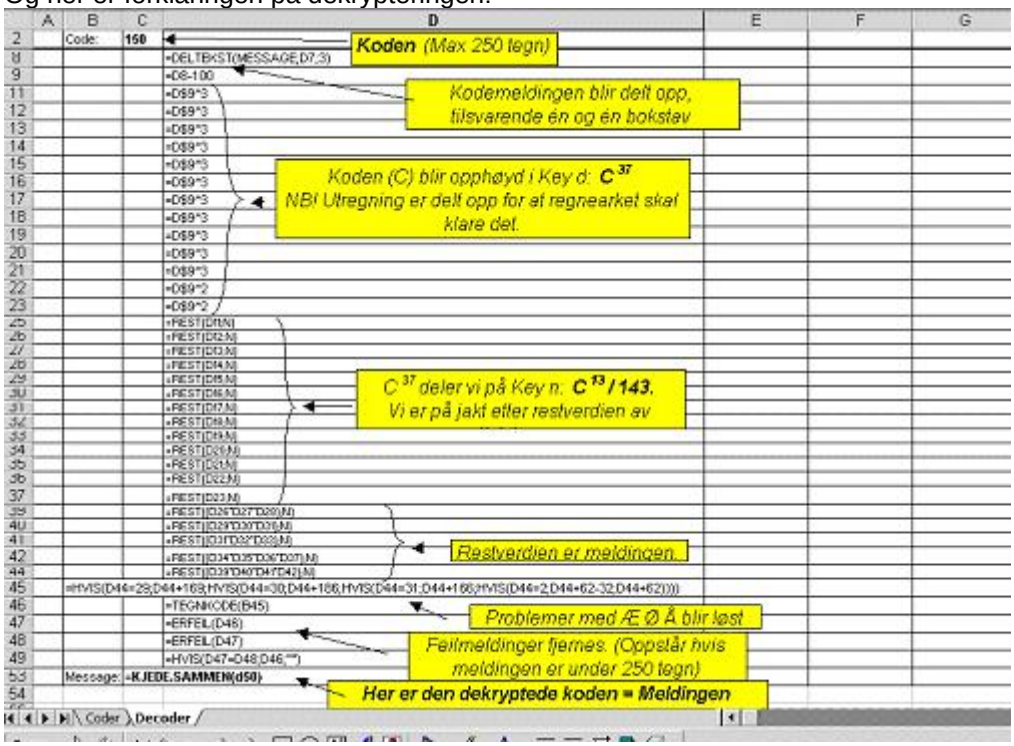
N er felles for begge (den må begge bruke). Men det er bare Ole som vet hva N er og Janne vet hva D er. Ole krypterer ved hjelp av N og E og Janne dekrypterer med N og D.
Først deles meldingen opp i ett og ett tegn og hvert tegn

gjøres om til et tall. Hvert tall (M) gjennomgår en komplisert regneoperasjon for å bli en Kode (C): $C = M^{13}$ *(modulus 143).*
Modulus-regning vil si *å finne resten av et delestykke*. F.eks. 25 modulus 2 = 1 fordi 25:2 gir 1 til rest. Hvis Ole skal sende bokstaven A til Janne, og vi velger å gjøre om A til tallet 3. Så blir koden: (3^{13}): 143. Restverdien på dette delestykket blir koden. Janne kan dekryptere ved utregningen M = C^{37} (modulus 143). Hvis koden Janne har fått er 16, tar hun (16^{37}): 143. Restverdien på dette delestykket blir 3 som kan gjøres om til bokstaven A.

Men da vi ville prøve dette ut på et regneark, fikk vi store problemer. Ei celle klarte ikke denne utregningen. Heller ikke læreren fikk det til. Vi kontaktet et par lærere på HiA. Der fikk vi det råd å dele potens-oppgaven opp i flere celler og gjøre modulusregningen flere ganger. Her ser du hvordan vi bygget opp et dataprogram som kan kryptere ei melding i RSA-systemet:

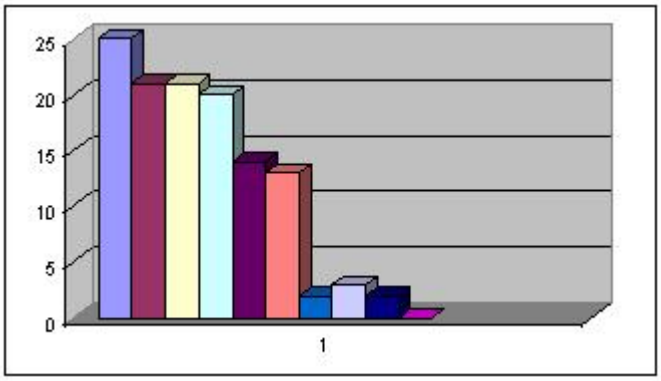


Og her er forklaringen på dekrypteringen:



Hvor vanskelig er kryptering?
Vi ville undersøkelse hvor vanskelig kryptering vanlige mennesker mestrer. Og hvor mange som klarer de forskjellige oppgavene. Vi laget 10 oppgaver med stigende vanskelighetsgrad.

Oppg. nr	Antall som løste oppg.	kommentar	Hva slags kryptering
1	25	Denne klarte alle	Kort ord, bokstavene stokket rundt.
2	21	Vanskelig for noen	Kort setning, bokstavene stokket rundt.
3	21		Litt lengre enn den forrige
4	20	Lett for mange. 5.–klassinger	Bokstavene gjøres om til tall: A = 1 B = 2 osv.
5	14	Hertil kom 5.–klassinger.	Et lengre ord, men følger samme systemet.
6	13	Her kom 10.–klassinger.	Tallet er nå blitt * 2: A=2, B=4, C=6
7	2		Alfabetet er forkjøvet 5 ganger mot høyre.
8	3		Alfabetet forkjøvet 10 mot høyre.
9	2	Hit nådde IKT- ansvarlig på skolen og en annen lærer	Tallet som symboliserer bokstavene er blitt delt på et annet tall.
10	0	Ingen klarte denne.	Jeg brukte femtallssystemet, A = 1*7 F=10*7 K=20*7



Vi fant ut: Vanlige folk klarer å løse enkle krypteringer, men får problemer hvis bokstavene forskyves i alfabetet.

Klassens konklusjon

Kryptering brukes i mange sammenhenger i det daglige liv: nettbank, minibank, krig, nettsider, politi, forsvaret osv. Kryptering er en hemmelig melding. En beskjed eller tekst gjøres om slik at det blir uforståelig og noen ganger også uleselig. Vi kan kryptere både tall og tekst, og vi kan gjøre det om til mye uforståelig. Det kan være tall, bokstaver, tegn, runetegn, figurer, tegninger, lyd, lys, toner osv. Språk som mange skjønner eller som vi kan lære, er ikke kryptering. Derfor kan en ikke kalle morse, tegnspråk, dyrelyder og lignende for kryptering. Vi har funnet ut at det er flere ulike måter å gjøre det på, og vi har forsket på både symmetrisk og asymmetrisk kryptering. Begge bruker matematikk, men asymmetrisk kryptering har en vanskelig, men spennende matematikk. Vi får bruk for både potens- og modulusregning. Det første hadde vi lært, men det siste klarte vi å finne ut av til slutt: Restverdien til delestykker som ikke går opp. Hvis vi kaller meldingen for M og koden for C blir asymmetrisk kryptering slik: **$C = M^e$ (modulus n)** og dekryptert: **$M = C^d$ (modulus n).**

n, d og e er 3 nøkler som står i et bestemt forhold til hverandre. F.eks kan en bruke 143, 37 og 13.

Kryptering er vanskelig for vanlige folk, selv enkel symmetrisk kryptering, og det er faktisk få som kjenner ordet og vet hva det betyr. Ved kryptering blir f.eks. Nettbank sikker for hackere (datasnikere) som vil ha tak i pengene dine. Kryptering ble brukt helt tilbake til Julius Cæsar sin tid, Vi har også funnet ut at de krypterte ved hjelp av runer i middelalderen og under 2. verdenskrig.

Kilder

Sjøforsvaret
Heimevernet
Forsvaret
Universitetet i Oslo
Anne Berit Fuglestad ved Høgskolen i Agder, matematikkseksjon
IKT-ansvarlig i Spareskillingsbanken i Kristiansand
Ben Johnsen: Kryptografi – den hemmelige skriften. Tapir forlag 2001
Simon Singh: Koder.
http://www.magnusson.info/lukas/krypto/index.html
http://www.magnusson.info/lukas/krypto/nycklar.html
http://www.magnusson.info/lukas/krypto/dekrypto.html
http://www.magnusson.info/lukas/krypto/kryp.html
http://www.matematikk.org/pub/mattetekst/RSA/
http://odin.dep.no/fad/norsk/dok/andre_dok/nou/002001-020005/hov003-bn.html#hov3.noteref1
http://www.brreg.no/sikkerhetsportal/pki_spm.html
http://efn.no/krypto-notat.html
http://www.gtf.ol.no/~pil/rundskr/pgp.html
http://www.linuxguiden.no/index.php/The_GNU_Privacy_Guard#Kryptering
http://www.root.no

Raymod Langbraaten raylang@stud.hisf.no 930 88 002
Per Sandrød persa@stud.hisf.no 95 88 44 60
Vidar Bråtun vidarbr@stud.hisf.no 971 82 598
Lars mailto:lks@nextra.com

Vedlegg

Krypteringsundersøkelse
Asymmetrisk kryptering og dekryptering med Excel
Intervju med Rein Sigve Karlsen