GÖTEBORGS UNIVERSITET

Sekretessens utveckling från antiken till idag

En studie om krypteringens historia och möjligheten att använda den i dagens matematikundervisning

Författare: Niklas Ekeroth
Handledare: Ulf Persson
Våren 2014

Abstract

Krypteringens historia är lång och händelserik, vilket ett system som Ceasarchiffer som snart är 2000 år gammalt kan vittna om. Den här litteraturstudien syftar till att ta dig som läsare med genom krypteringens utveckling från antikens pergament till dagens datoriserade samhälle. På vägen genom historien har studien som målsättning att förklara för läsaren hur de olika krypteringssystemen som figurerat genom tiden har fungerat, och att lyfta fram matematik bakom systemen. Mot slutet av texten beskrivs dessutom hur kryptering skulle kunna fungera som inslag i skolans matematikundervisning. Här är syftet att inspirera lärare till att pröva på något nytt i sin undervisning, vilket kan leda till ökad motivation. Studien finner att krypteringens historia är en bottenlös brunn där historierna aldrig tycks ta slut, trots att kryptografin är en vetenskap höljt i dunkel där många av dess pionjärer varit belagda med tystnadsplikt. Krypteringens historia lär oss att man aldrig kan vara säker på att man nått fram till absolut sekretess, och att krypteringen lämpar sig väl för att föra samman matematik och andra skolämnen i ämnesintegrerade projekt. Kryptering som exempel illusterar också att matematiken fortfarande är under utveckling.

Nyckelord: kryptografi, steganografi, kryptering, dekryptering, forcör, transposition, substitution, fekvensanalys, Enigma, RSA, ämnesintegration, undervisning, läroplan

Titel: Sekretessens utveckling från antiken till idag – en studie om krypteringens historia och möjligheten att använda den i dagens matematikundervisning

Författare: Niklas Ekeroth

Termin och år: Våren 2014

Kursansvarig institution: Matematiska vetenskaper

Handledare: Ulf Persson

Examinator: Laura Fainsilber

Innehållsförteckning

Sida

1 Att studera kryptologins historia

1.1 Inledning

Den svenska gymnasieskolan fick under höstterminen 2011 en ny läroplan (Regeringskansliet 2010). I den går det att finna vilka förmågor eleverna ska ha fått med sig efter en slutförd gymnasieutbildning i ämnet matematik. En av de förmågor som lyfts upp i ämnesplanen för matematik är att eleverna ska känna till matematikens betydelse ur ett ”yrkesmässigt, samhälleligt och historiskt sammanhang” (Skolverket 2011). Ett ämnesområde där matematiken (men också lingvistiken) har haft en framträdande roll genom historien fram till idag är inom vetenskapen kryptografi (Ekhall 2013, s. 2). Kryptografins historia är rik och utspelar sig under en mycket lång tidsram, där kampen mellan kryptörer och dekryptörer många gånger har haft en avgörande roll för vilken väg en betydande historisk händelse ska ta (Kahn 1973, s 1, 3). Ändå är det just nu under vår tid kryptografin är mer aktuell än någonsin tidigare. I vårt privatliv, yrkesliv och under vår skolgång använder vi mobiltelefon och datorer för att kommunicera. När vi är i ett telefonsamtal eller skickar ett e-postmeddelande finns möjligheten att avlyssna vår kommunikation på vägen mellan datorer och satelliter, vilket utgör en fara för vårt privatliv. Vi använder även tekniken för att konsumera; handeln via Internet ökar kraftigt, och företagen som erbjuder tjänsten behöver kunna garantera sina kunder en säker transaktion. Därmed behövs kryptering nu mer än någonsin tidigare i människors vardagsliv för att dölja vår kommunikation, för att garantera vår personliga integritet, för vår säkerhet, men också för att en ny växande digitalmarknad ska kunna blomstra. Dessa säkerhetsanordningar utvecklas idag av matematiker (Singh 2003, s. 10-11). Forskningsområden inom matematiken som en gång i tiden ansätts sakna praktiska tillämpningar är idag heta verksamheter som det investeras stora summor pengar i, mycket på grund av de moderna krypteringssystemen egenskaper (Thorbiörnson 2003).

1.2 Syfte, frågeställningar och avgränsningar

Syftet med denna studie är att lyfta fram hur sekretessen och dess krypteringsverktyg har utvecklas genom historien fram till idag. Vid förarbetet till denna studie framgick det tydligt att kryptografins historia är lång, och att det material som beskriver kryptografins bakgrund och systematik är väldigt omfattande. Av denna anledning kan dessvärre inte alla

kvinnor, män och historiska händelser som haft betydelse täckas in i ett arbete av detta omfång, men förhoppningsvis lyckas texten med att fånga upp vissa av de händelser som har haft särskilt stor betydelse för krypteringens evolution. Arbetet syftar vidare till att försöka förklara hur dessa olika krypteringssystem har fungerat och dessutom belysa en del av den matematik som kan lyftas fram från de olika systemen. Studiens frågeställningar ser ut som följande:

- Hur har krypteringen utveckling sett ut genom historien från antiken till idag?
- Hur fungerade eller fungerar dessa olika krypteringsverktyg som figurerat genom historien och som i vissa fall fortfarande används?
- Kan kryptering fungera som ett inslag i skolans matematikundervisning?

1.3 Metod

Detta arbete är en litteraturstudie av kryptologins utveckling, där ett flertal verk som behandlar ämnet har granskats. Den referens som främst används i denna uppsats är vetenskapsjournalisten samt fysikern Simon Singh och hans världsberömda verk *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Då flera författare har behandlat samma typ av innehåll vänder jag mig ofta till Singh. Det har även funnits ett behov av att studera mer matematikfokuserad litteratur för att i mer detalj kunna belysa matematiken som finns att lyfta fram bakom krypteringssystem så som Enigma och RSA.

2 Kryptologins historia

2.1 Sekretessens vagga - steganografin

De första redogörelserna av hur hemliga meddelanden kunde förmedlas finner vi redan så tidigt som under antiken i skrift från 400-talet f. Kr av historieskrivarnas fader Herodotos. Herodotos verk som senare skulle delas upp i nio böcker behandlar till stora delar konflikten mellan Grekland och Persien (vilket var namnet på Iran fram till 1935), från det joniska upproret 499 f. Kr till Atens erövring av Sestos 478 f. Kr. Herodotos upplevde själv inte krigen, så hans verk bygger på muntliga traditioner, och till viss del även på skriftligt material. Konflikten mellan Grekland och Persien skildras som en kamp mellan frihet och slaveri, där kunskapen att förmedla hemlig skrift bland grekerna skulle bli deras räddning från att besegras av de tyranniska perserna och deras ledare Xerxes, Kongungarnas konung (Singh 2003, s. 17-18; Nationalencyklopedin 2014).

Herodotos beskriver i en del av sitt verk hur den utvisade greken Demaratos, som under tiden för kriget var bosatt i den persiska staden Susa år 480 f. Kr, bevittnade en persisk militärupprustning för en planerad överraskningsattack mot Grekland. Trots sin exil kände Demaratos lojalitet till sitt forna hemland Grekland och beslöt sig för att skicka ett varnade meddelande till grekerna om Persiens invasionsplaner. Under denna tid användes en så kallad vaxtavla, ett skrivunderlag i trä överdragen med ett tunt lager vax där anteckningar ristades in. För att kunna få ut meddelandet ur den persiska staden till Grekland utan att det beslagtogs på vägen av de persiska vakterna dolde Demaratos sitt budskap genom att skrapa av vaxet från träskivan och ristade sedan in ett meddelande på träytan som beskrev det han hade beskådat. Därefter täckte han över meddelandet med vax och vaxtavlan uppfattades då som tom av de persiska vakterna när den sedan fraktades ut ur staden. På så sätt kunde man i Grekland efter att man fått beskedet rusta upp sin arme, och Xerxes överraskningsmoment var därmed förlorat (Singh 2003, s. 18-19; Nationalencyklopedin 2014).

Att som Demaratos dölja eller helt enkelt gömma undan sina meddelanden för att upprätthålla en hemlig kommunikation går under namnet *steganografi* och kommer från grekiskan, där *steganos* betyder dold eller övertäckt och *grafein* betyder skriva (Singh 2003, s.19). Steganografin har sedan den först beskrevs i Herodotos verk för nästan 2500 år sedan kommit i många olika former runt om i hela världen (ibid., s. 19-20). Herodotos berättar själv i sitt verk hur den grekiska politikern Histiaios försökte uppmana

Artistagoras ledare av den grekiska staden Miletos att starta ett uppror mot den persiska kungen. Kommunikationen mellan de båda upprätthölls hemligt genom att Histiaios lät raka huvudet på sina budbärare för att sedan skriva meddelandet på budbärarens hjässa. Ärendet var inte mer brådskande än att budbärarens hår sedan kunde växa ut för att dölja meddelandet. När budbäraren senare nått sin destination kunde denne raka av sig håret och visa upp meddelandet på hjässan för den rätte mottagaren (ibid., s. 19).

Även osynlig skrift går under kategorin steganografi. Den romerska författaren Plinius beskrev under 100-talet e. Kr hur man tillverkar osynligt bläck genom användning av produkter från växtriket. Bläcket blev osynligt efter att det torkat och gick endast att beskåda efter att det hettats upp, då det fick en brunaktig färg. Stegnografin har varit seglivad och användes långt senare av tyska agenter under andra världskriget i form av en metod som kallas mikropunkt. Tekniken går till så att texten fotograferads och fotot av texten förminskads sedan till en prick så liten så att den knappt är en millimeter i diameter. Pricken placerads sedan som en vanlig punkt i ett brev vars innehåll framstod som oskuldsfullt (Singh 2003, s. 20-21).

Steganografin ger avsändaren en viss säkerhet (en minimal sådan) och därför har den också hängt med under ett mycket långt tidsspann. Stenografin har emellertid en betydande svaghet. Om budbäraren stöter på en mycket nitisk vakt som kroppsvisiterar budbäraren, rakar håret eller hettar upp pappret kommer hemligheten i meddelandet direkt att avslöjas. Inte ens de tyska agenternas mikropunkt skulle visa sig vara tillräckligt säker. Den amerikanska federala polismyndigheten (FBI) fick 1941 in ett tips om att hålla uppsikt efter skimmer på de papper de beslagtagit då detta kunde vara en blank filmhinna, vartefter amerikanerna kunde läsa stor del av tyskarnas hemliga meddelanden, men inte alla. I vissa fall hade de tyska agenterna vidtagit en extra säkerhet i sin kommunikation och krypterat innehållet i texten (Singh 2003, s.21).

2.2 Kryptografins intåg

Kryptografin utvecklades parallellt med steganografin. Ordet kommer likt steganografin från grekiskan där *kryptos* betyder gömd (Singh 2003, s.20). Till skillnad från steganografin gömmer man inte själva meddelandet i sig utan man döljer i stället innehållet i meddelandet. Processen där meddelandets innebörd döljs benämns som kryptering och går till så att sändaren förvränger ett meddelande genom att använda sig av i förväg bestämda regler som även mottagaren tagit del av, så att denne sedan kan genomföra

processen eller förvrängningen baklänges så att meddelandet blir läsbart igen. I fallen där de tyska agenterna hade kombinerat steganografin med kryptografin kunde amerikanerna trots upptäckten av meddelandet inte få ut några upplysningar från det då budskapet i meddelandet blivit förvrängt. Detta gör kryptografin till ett kraftfullare verktyg än steganografin då man vill bevara sina hemligheter från fiender (Singh 2003, s. 21).

Kryptografin delas in i två underkategorier vilka benämns *transposition* och *substitution* (Singh 2003, s. 21). För dessa uttryck kommer det att redogöras i följande avsnitt.

2.2.1 Transposition

Transposition fungerar så att bokstäverna i en text placeras om på samma sätt som när man skapar ett anagram. Säkerheten varierar beroende på meddelandets längd, där skyddet ökar kraftigt då meddelandet blir allt längre och bokstäverna kan möbleras om på allt fler sätt. Transposition fungerar till exempel mindre bra då man har tänkt sig att kryptera ett meddelande som bara innehåller ett ord. Ett meddelande med endast ett ord på tre bokstäver kan bara kombineras på sex olika sätt (jag, jga, gja, gaj, agj, ajg) och säkerheten i meddelandet blir därav väldigt låg. Säkerheten ökar dock snabbt om meddelandet är längre. Singh (2003) ger följande exempel: ”***betrakta till exempel denna korta mening***. Den innehåller 35 bokstäver, och ändå finns det 10 814 200 000 000 000 000 000 000 000 000 olika sätta att placera dem” (Singh 2003, s. 21). Om jordens samtliga invånare provade ett placeringssätt i sekunden skulle det ändå ta tusen gånger universums livslängd att kontrollera samtliga placeringssätt i meningen ovan (ibid., s. 22).

Exempel 1

Hur många ”ord” kan bildas genom att använda bokstäverna i ordet JAG?

JAG består av 3 bokstäver. Totalt har vi 3! ”ord”

$3! = 3 \times 2 \times 1 = 6$

Totalt finns det alltså sex stycken ”ord” eller *permutationer:*

JAG, JGA, GJA, GAJ, AGJ, AJG

Exempel 2

Hur många ”ord” kan bildas genom att använda bokstäverna i meningen BETRAKTA TILL EXEMPEL DENNA KORTA MENING?

BETRAKTATILLEXEMPELDENNAKORTAMENING består av 35 bokstäver. Totalt har vi 35! ”ord”

$35! = 35 \times 34 \times 33 \times 32 \times 31 \times 30 \times 29 \times 28 \times 27 \times 26 \times 25 \times 24 \times 23 \times 22 \times 21 \times 20 \times 19 \times 18 \times 17 \times 16 \times 15 \times 14 \times 13 \times 12 \times 11 \times 10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1$

35! = 10333147966386144929666651337523200000000 olika ”ord” vilket är ett enormt antal av kombinationer.

I meningen BETRAKTATILLEXEMPELDENNAKORTAMENING förekommer dock vissa bokstäver vid flera tillfällen, vi har till exempel två stycken olika M. Enligt Vretblad och Ekstig (2010) kan man tänka sig att alla våra bokstäver i meningen först är åtskiljbara, våra två M kan vi kalla M_1 och M_2. I detta falla är antalet ”ord” lika med 35! men flera av alla de ”ord” (permutationer) vi får fram kommer att se likadana ut:

BETRAKTATILLEXE**M_1**PELDENNAKORTA**M_2**ENING
BETRAKTATILLEXE**M_2**PELDENNAKORTA**M_1**ENING

Om vi nu avlägsnar skillnaden mellan de två M:en betraktar vi nu två ”ord” som är ekvivalenta. Vi måste alltså reducera med en faktor 2 (två bokstäver kan permuteras på 2! = 2 • 1 sätt). Men M är inte den enda bokstaven som det finns flera av, vi ser att det finns E = 6, N = 4, T = 4, A = 4, L = 3, R = 2, K = 2, I = 2, M = 2

uttrycket för antalet ”ord” som kan bildas av meningen blir därför

$$\frac{35!}{6!\times4!\times4!\times4!\times3!\times2!\times2!\times2!} = 10\ 814\ 200\ 000\ 000\ 000\ 000\ 000\ 000\ 000$$

Slumpmässig transposition som i metoden ovan verkar onekligen ge och väldigt god trygghet i kommunikationen även vid korta meningar, då det inte verkar finns en chans för fienden att tolka innehållet i meddelandet. Problemet är bara det att innehållet även blir obegripligt för den påtänkta mottagaren – anagrammet som konstrueras då bokstäverna

kastas om utan eftertanke blir helt enkelt allt för svårt att avläsa. Ska transpositionen fungera på ett bra sätt måste sändaren och mottagaren i förväg komma överens om ett fungerande system för hur bokstäverna ska omplaceras. Det finns flera exempel på sådana system, där det äldsta är en uppfinning ofta använd för militära ändamål från 400-talet f. Kr. Uppfinningen i fråga var en så kallad *scytale,* som är en cylinder med en läder- eller en pergamentremsa lindad runt sig där avsändaren kunde skriva sitt meddelande. Remsan lindas sedan av scytalen och blir då en remsa full av meningslösa bokstäver. För att mottagaren sedan ska kunna läsa budskapet på remsan behöver denna ha en scytale med samma diameter som den avsändaren använde sig av. Mottagaren kunde sedan linda remsan kring sin scytale och såg på detta vis vad som stod i meddelandet. Man behöver dock inte gå så långt tillbaka i historien som 400 f. Kr för att hitta exempel där transposition används. Scouter använder transposition för att skicka meddelande med ett system som de kallar brädgården. Det går till så att varannan bokstav i meddelandet flyttas ned en rad och när meddelandet är färdig skrivet hakas den övre och undre raden ihop för att göra texten ännu mer obegriplig och ett krypterat budskap har skapats. Mottagaren kan sedan läsa meddelandet genom att vända på processen (Singh 2003, s. 22-23).

Exempel 3

Brädgårdskryptot steg för steg

DET HÄR MEDDELANDET SKA KRYPTERAS MED BRÄDGÅRD

↓

D T Ä M D E A D T K K Y T R S E B Ä G R

E H R E D L N E S A R P E A M D R D Å D

↓

DTÄMDEADTKKYTRSEBÄGREHREDLNESARPEAMDRDÅD

2.2.2 Substitution

Alternativet till transposition är substitution och redogörelser för hur denna typ av *chiffer* fungerar går att finna redan så tidigt som på 300-talet e. Kr ur ett avsnitt från den lärde brahminen Vatsyayanas verk Kama Sutra. Kama Sutra beskriver sextiofyra användbara konster som förespråkas att kvinnor ska lära sig, varav en av dessa (nummer 45) är konsten att skapa hemliga meddelanden. Metoden som redogörs i verket går till som så att man slumpvis parar ihop alfabetets samtliga bokstäver med varandra och när meddelandet ska krypteras byter man ut originalbokstaven i meddelandet mot parbokstaven (Singh 2003, s. 24).

Exempel 4

A	D	B	M	O	R	T	I	W	V	Z	Ö	C	H
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
K	P	F	E	J	G	L	N	S	U	Ä	X	Y	Å

Klartext: DET HÄR MEDDELANDET SKA KRYPTERAS
Kryptotext: PML ÅZG EMPPMTKIPML WAK AGCDLMGKW

I det svenska alfabetet finns 29 bokstäver. Därför har en bokstav valts bort för att varje bokstav ska få en parbokstav. Bokstaven Q är den minst förekommande bokstaven i svenska alfabetet (0,007 %), och därför valdes denna bort.

Det som skiljer transposition mot substitution är att vid transposition bevaras bokstaven men den byter position till skillnad från substitution där bokstaven bevarar sin position men byts ut mot en annan bokstav (Singh 2003, s. 24). Romarna använde sig av substitutionskrypton för att dölja budskapet i deras meddelanden (Wobst 2007, s. 18). Av de dokument som beskrev hur romarnas krypteringssystem var konstruerade finns endast ett bevarat och det är ur författaren Gajus Suetonius Tranquillus berömda verk *Åtta böcker om tolv kejsares liv* ifrån 100-talet e. Kr. Här beskrivs utförligt hur den romerska fältherren och statsmannen Julius Caesar framgångsrikt använder sig av substitutionskryptering under den romerska armens fälttåg in i Gallien (Järpe 2013, s. 155; Singh 2003, s. 24-25). Caesar

bytte i sina meddelanden ut varje bokstav mot en bokstav tre steg fram i alfabetet. Metoden kallas för Ceasarkrypto, och hur Ceasarkryptot fungerar blir tydlig om man sätter upp klartextalfabetet och krypteringsalfabetet under varandra.

Klartextalfabet

a b c d e f g h i j k l m n o p q r s t u v w x y z å ä ö

Kryptoalfabet

D E F G H I J K L M N O P Q R S T U V W X Y Z Å Ä Ö A B C

I klartextalfabetet finner vi det vanliga alfabetet och i kryptoalfabetet kan vi se att det traditionella alfabetet förskjutits tre steg och vi börjar istället för på A på bokstaven D. Om man sedan vill kryptera ett meddelande genom att använda Ceasarkryptot så ersätter man samtliga bokstäver i sitt meddelande med bokstäver från kryptoalfabetet. Om en mottagare sedan vill dekryptera meddelandet vänder denna på processen och översätter från krypteringsalfabetet till klartextalfabetet (Järpe 2013, s. 155-156).

Exempel 5

Klartext: detta meddelande ska krypteras med ceasarkrypto

Kryptotext: GHWWD PHGGHODKGH VND NUÄSWHUDV PHG FHDVDUNUÄSWR

Matematiskt kan Ceasarkryptot beskrivas med hjälp av modulär aritmetik:

$C = K + 3 \bmod 29$

Här står K för klartext och C för chiffertext. Vi får här anta att varje klartextbokstav motsvarar siffrorna A = 0, B = 1, C = 2 fram till Ö = 28. Tre adderas till klartextbokstaven och vi hamnar tre steg fram i alfabetet precis som i ett Ceasarkrypto (Ceasarkrypto går även under namnet Ceasar addition). Om K + 3 skulle bli större eller lika med 29 drar vi av med 29 där av mod 29 i formeln (Wobst 2007, 18). Valet av 29 är på grund av att det finns 29 bokstäver i det svenska alfabetet.

Exempel 6

(A = 0, B = 1, C = 2, D = 3 …. Ö = 28)

(C = K + 3 mod 29)

Klartext: ABC

K = 0, 1, 2

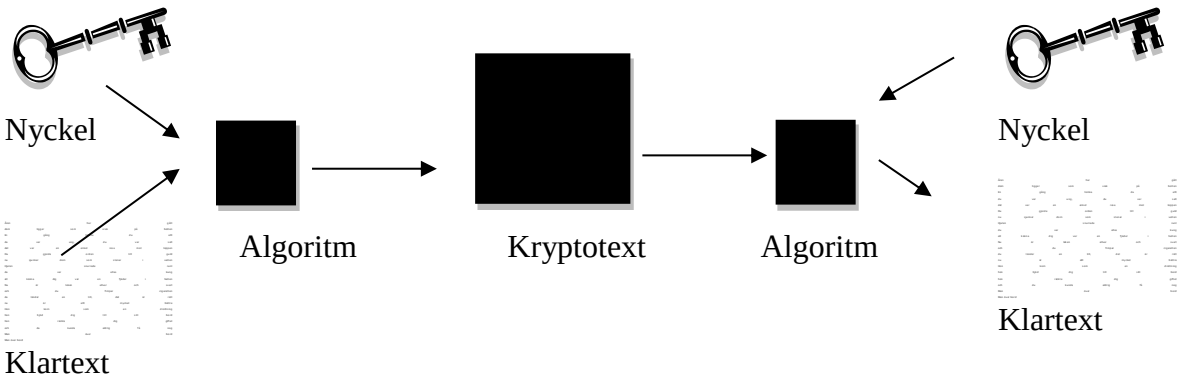
Vilket ger

C = 3, 4, 5

Kryptotext: DEF

Vid Caesarkryptering ersätts varje bokstav från klartextalfabetet till kryptoalfabetet då budskapet i texten ska döljas. Detta kan mer generellt kallas för Caesarkrypteringens *algoritm.* I kryptoalfabetet har dessutom klartextalfabetets bokstäver förskjutits tre steg framåt, vilket man skulle kunna kalla för chiffrets *nyckel*. Om någon obehörig (en fiende) skulle få tag på ett meddelande som är krypterat kan denne mycket väl ha en aning om vilken typ av algoritm som använts och i detta fall hänger hela chiffret styrka på hur många möjliga nycklar det har (Singh 2003, s. 26). Här ligger den stora svagheten i den krypteringsmetod Julius Caesar så framgångsrikt använde sig av – den har bara en enda nyckel, nämligen förskjutningen av klartextalfabetets bokstäver tre steg framåt. Det innebär att en potentiell fiende som lyckats snappat åt sig texten endast behöver pröva att förskjuta bokstäverna för att kunna ta del av innehållet i meddelandet (Järpe 2013, s. 156). Ett liknade chiffer kallas för Caesarrullning. Där används samtliga möjliga förskjutningar av klartextalfabetet ett till tjugoåtta steg framåt (vid tjugonio steg är vi tillbaka där vi började), vilket ger upphov till tjugoåtta olika krypton. Matematiskt kan det utryckas på ett liknade sätt som Ceasarkryptot ovan där trean nu är utbytt mot F som motsvara den valda förskjutningen av klartextalfabetet C = K + F mod 29. För den vane kodknäckaren blir dock Ceasarrullningen ingen större utmaning då denne systematiska bara kan testa de tjugoåtta olika nycklarna och därefter ta del av det tidigare hemliga innehållet i texten (ibid., s. 157). Krypteringsfunktionen för Ceasarrullning ser ut som följande $f(x) = (x+k) \bmod 29$, inversen till denna funktion fungerar som dekrypteringsfunktion $f^{-1}(x) = (x-k) \bmod 29$. Ett säkert kryptosystem måste alltså ha många olika nycklar att välja bland och dessutom kunna hålla den valda nyckeln hemlig (Singh 2003, s. 27).

Sändare **Mottagare**



En mer allmän variant av ett substitutionskrypto är att istället för att begränsa sig till förskjutning tillåta vilken omplacering som helst av bokstäverna i klartextalfabetet för att skapa ett kryptoalfabet. Exemplet som följer är ett sätt att gör detta på av många, det finns över 400 000 000 000 000 000 000 000 000 olika varianter med ett engelskt alfabet på 26 bokstäver.

Exempel 7

Klartextalfabet:

a b c d e f g h i j k l m n o p q r s t u v w x y z

Kryptoalfabet:

M V N O U H L X F G E K S D Y Z R T C B Q I W A P J

Klartext: n i k l a s

Kryptotext: D F E K M C

Denna mer generella algoritm av substitutionskryptering ger en oerhörd mycket högre säkerhet i jämförelse med Ceasarkryptot. Vid Ceasarrullningen fick vi tjugoåtta möjliga nycklar i jämförelse med den allmänna varianten där vi kan åstadkomma så många som 26! = 26 × 25 × 24 × 23 ×…× 3 × 2 × 1 möjliga nycklar (om ingen bokstav i klartextalfabetet byts

mot samma i kryptoalfabetet). Om vi börjar med A har denna 26 alternativa bokstäver att välja bland, B har sedan 25 och C har 24 alternativ och så vidare. Om en fiende skulle lyckas få tag på ett meddelande krypterat med denna mer allmänna version av substitutionskryptering och vet om att så är fallet (hen känner till algoritm) kommer denne fiende fortfarande ha den oerhört svåra uppgiften kvar framför sig att gå igenom alla potentiella nycklar som är ett enormt stort tal som vi kunde se ovan, för att kunna ta del av det hemliga innehållet. Denna typ av chiffer ger även väldigt lite utrymme till missförstånd mellan mottagare och sändare på grund av den mycket enkla nyckeln (i detta fall vilket kryptoalfabete som används) som de båda måste känna till.

En kombination av användarvänlighet med hög säkerhet gjorde att substitutionskryptot skulle fortsätta användas hela det första årtusendet e. Kr. Det fanns helt enkelt inget behov av att ta fram en ny typ av kryptering då experter under tiden menade att substitutionskryptot var omöjligt att dekryptera, man hade garanterat möjligheten till säker kommunikation. Hela problemet låg nu i knäna på kodknäckarna att försöka ta sig igenom denna ogenomträngliga vägg som utgjordes av substitutionen (Singh 2003, s. 29).

2.3 Kodknäckarnas genväg

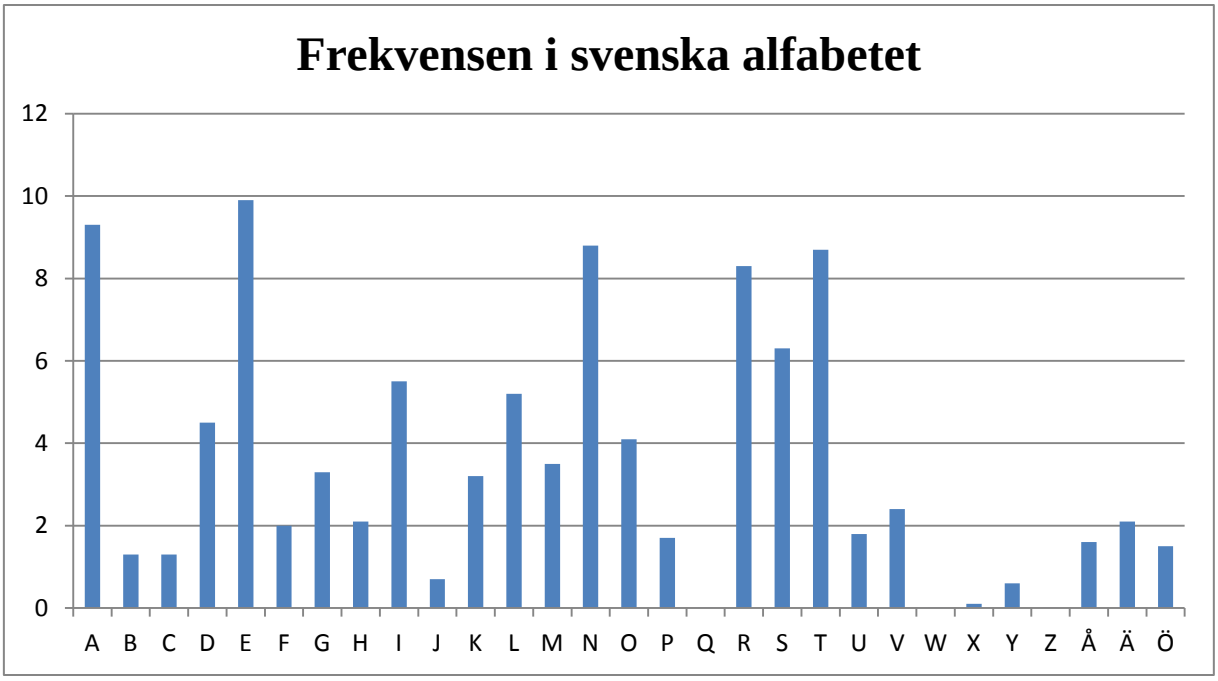
Ett genombrott för chifferbrytaren skulle ske i det vi idag kallar Mellanöstern där den abbasidiska familjen skulle ta makten år 750 och överta kalifatet. De abbasidiska kaliferna ville varken kriga och erövra utan var istället mer intresserade av att bygga upp ett välmående, stabilt och fredligt samhälle där huvudstaden skulle bli Bagdad i Irak. Kaliferna nådde sitt mål, och denna tidsperiod skulle bli den islamska kulturens guldålder (Nationalencyklopedin 2014; Singh 1999, s. 30). Som ett resultat av dessa satsningar blomstrade konsten liksom vetenskapen och de var båda på kraftig frammarsch. Kryptografin spreds och användes i stor utsträckning, men framför allt fann man här under denna tid konsten att genomföra det som tidigare sagts var en omöjlig uppgift, en metod för att dekryptera ett generellt substitutionskrypto. Det var ingen slump att *Kryptoanalysen (*vetenskapen att återställa ett krypterat meddelande utan vetskap om vilken nyckel som används) skulle uppfinnas under just denna tid; det krävdes ett samhälle vars kunskap i matematik, statistik och språk kommit till en tillräckligt avancerad nivå (Singh 1999, s. 30).

Denna revolutionerande kryptoanalysiska metod som uppfanns under den abbasidiska dynastin kallas för *frekvensanalys*, och metoden förutsätter att kryptoanalytikern sitter inne

på upplysningar kring vilket språk som meddelandet är skrivet på (Järpe 2013, s 159). Om vi nu fastställer att det krypterade meddelandet skulle vara skrivet på svenska behöver kryptoanalytikern vidare sammanställa en tabell för antalet gånger varje bokstav i alfabetet förekommer i det svenska språket (det vill säga bokstavens frekvens). För att fastställa frekvensen hos samtliga bokstäver i det svenska språket har cirka 1 000 000 tecken från tidningstexter, facklitteratur och skönlitteratur granskats i tabellen nedan (Singh 1999, s. 34).

I bokstavsordning	
Bokstav	%
A	9,3
B	1,3
C	1,3
D	4,5
E	9,9
F	2,0
G	3,3
H	2,1
I	5,5
J	0,7
K	3,2
L	5,2
M	3,5
N	8,8
O	4,1
P	1,7
Q	0,007
R	8,3
S	6,3
T	8,7
U	1,8
V	2,4
W	0,003
X	0,1
Y	0,6
Z	0,002
Å	1,6
Ä	2,1
Ö	1,5

I ordning efter förekomst	
Bokstav	%
E	9,9
A	9,3
N	8,8
T	8,7
R	8,3
S	6,3
I	5,5
L	5,2
D	4,5
O	4,1
M	3,5
G	3,3
K	3,2
V	2,4
H	2,1
Ä	2,1
F	2,0
U	1,8
P	1,7
Å	1,6
Ö	1,5
B	1,3
C	1,3
J	0,7
Y	0,6
X	0,1
W	0,03
Z	0,002
Q	0,007



När kryptoanalytikern väl har tillgång till information över hur frekventa bokstäverna är i språket måste en likadan tabell konstrueras för hur vanligt förekommande de olika bokstäverna är i det krypterade meddelandet. Låt oss här illustrera detta genom att granska ett meddelande som krypteras med substitution, där nyckeln inte är känd. För att analysera hur frekventa bokstäverna är i kryptotexten.

RMKJÅK JKYGGZQZWPZ Q ZÅGG RMGP XQJ EGYKÅ EGPZPZ EP GQTT ÅGG CYRRÅ PZEÅR

Totalt består meddelandet av 59 bokstäver, varav fördelningen av bokstäver sammanställts i tabellen nedan.

Bokstävernas förekomst i kryptotexten

Bokstav	%	Bokstav	%	Bokstav	%
A	0	K	6,78	U	0
B	0	L	0	V	0
C	1,69	M	3,39	W	1,70
D	0	N	0	X	1.69
E	6.78	O	0	Y	5,08
F	0	P	10,17	Z	11,86
G	16,95	Q	6,78	Å	10,17
H	0	R	8,48	Ä	0
I	0	S	0	Ö	0
J	5,08	T	3,39		

Frekvensanalysen går sedan till som så att den mest förekommande bokstaven i det svenska alfabetet (vilket enligt tabellen är E) ersätter den mest frekventa bokstaven i kryptotexten (vilket är G). Fortsättningsvis ersätts den näst mest förekommande bokstaven i svenska alfabetet (alltså A), mot den näst mest förekommande bokstaven i kryptotexten (vilket är Z i det här fallet). Detta utbyte sker ända tills man är framme vid den sista bokstaven (Singh 1999, s. 35). Om denna metod användes fullt ut på det hemliga meddelandet ovan skulle dock det dekrypterade meddelandet bli precis lika svårförståeligt som det krypterade. Meddelandet är alltför kort för att frekvensanalysen ska fungera optimalt, men med en kombination av list och en del gissningar kan man ändå komma fram till en lösning (Järpe 2003, s. 160). Enligt Singh (1999) kan man börja med att fokusera på det mest förekommande bokstäverna i både kryptotexten och i det svenska språket. I detta fall kan vi se att G, P, Z, och Å sticker ut i kryptotexten och är de mest förekommande. I det svenska alfabetet är motsvarande bokstäver E, A, N och T. Även om G kanske inte motsvarar E så kan vi ändå anta att G motsvarar någon av bokstäverna E, A N eller T. Alltså G = E, A, N eller T, P = E, A, N eller T, Z = E, A, N eller T och Å = E, A, N eller T. Fortsatt kan kryptoanalytikern fokusera på dubbelbokstäver (vilket även fungerar då texten är hopskriven) och ord med få bokstäver (tre eller två) (Singh 1999, s. 35). Vi kan börja med att granska ordet ÅGG som har dubbelstavningen GG. Enligt Singh (1999) är TT den vanligaste dubbelstavningen i svenskan, dessutom är T med bland de högfrekventa bokstäverna vi antog att G kunde vara, så vi kan prova att sätta G till T. Det vanligaste tre bokstavliga orden är ALL, UPP, OSS, ATT och ETT (Järpe 2013, s. 160). Om vi valt G till T borde såklart ATT och ETT vara våra bästa kandidater, både Å och G är dessutom

högfrekventa bokstäver vilket borde dra oss till slutsatsen att utesluta OSS och UPP som är längre ned på listan bland högfrekventa bokstäver. Nästa ord vi skulle kunna kolla närmare på är ordet EP. Det mest förekommande orden med två bokstäver är AV, BE, DE, DU, DÖ, ED, EK, EN, ER, FÅ, GE, GÅ, IN, JA, JU, NU, PÅ, RO, SA, SE, TA, UR, UT, VI, VY, YR, ÅR, ÅT, ÄN, ÄR, ÖL (Järpe 2013, s.160). Både E och P är högfrekventa bokstäver i kryptotexten vilket gör att vi kan tänkas korta ned listan ovan till ER, SA, SE och TA. Om vi nu väljer EP till SE och ÅGG till ATT och dessutom drar till med en gissning att den sista hög frekventa bokstaven i kryptotexten Z är vår återstående högst frekventa bokstav i svenska alfabetet N ser vi att det hemliga meddelandet ovan börjar bli allt tydligare

RMKJa**K JKY**ttn**Q**n**W**en **Q** natt **RM**te **XQJ** st**YK**a stenen se t**QTT** att **CYRR**a ensa**R**

Ordet ensa**R** ser ut att kunna vara ensam vilket gör att R skulle vara M. det ger oss ordet m**M**te vilket skulle kunna vara möte, M kan alltså vara Ö. Den näst vanligaste dubbelbokstaven i svenskan är LL (Singh 1999, s. 39). Vilket antyder att t**QTT** skulle vara ordet *till* vilket även styrks av ”Q natt” vilket ser ut att vara ”i natt”. Vi har ett hemligt meddelande just nu som börjar bli allt mindre hemligt.

mö**KJ**a**K JKY**ttnin**W**en i natt möte **XiJ** st**YK**a stenen se till att **CY**mma ensam

Ordet **CY**mma ser ut att kunna vara *komma,* vilket ger oss sto**K**a som skulle kunna vara stora.
C är alltså lika med ett K, Y är O och K är R. Meningen ser nu ut så här:

mör**J**ar **J**rottnin**W**en i natt möte **X**i**J** stora stenen se till att komma ensam

Redan nu skulle en fiende som snappat upp meddelandet fått en hel del upplysningar. Men denna skulle nog kunnat se att mör**J**ar är *mördar,* vilket ger oss drottnin**W**en. Vilket med all säkerhet är drottningen. W är alltså g och J är d. Ett ord återstår nu att dekryptera i det hemliga meddelandet vilket är **X**id. Tre bokstäviga ord som slutar på *id* är lid, kid, nid, sid, tid och vid (Scrabbleförbundet 2011). Ut av dessa är *vid* det som ser ut att passa bäst in i meningen och hela hemligheten är därefter avslöjad och ser ut som följande:

Mördar drottningen i natt, möte vid stora stenen se till att komma ensam.

Som sagt var meddelandet ovan allt för kort för att frekvensanalysen skulle fungera fullt ut. Under hundra tecken kommer dekrypteringen att bli problematisk (Singh 1999, s. 35). Ändå vid endast femtionio bokstäver kunde frekvensanalysen ge oss tillräckligt bra start i det här fallet för att kunna lyckas dekryptera budskapet i kryptotexten och ett längre meddelande skulle i det allra flesta fall följa standardfördelningen i tabellen ovan ännu bättre. Man vet idag inte vem som först upptäckte att man kan använda frekvensen av bokstäverna i en text för att dekryptera ett meddelande. Den första beskrivningen av frekvensanalysen vi idag känner till är ifrån 800-talet, avhandlingen *Manuskript om dechiffrering av kryptografiska budskap* av författaren al-Kindi (Singh 1999, s.32). Samtidigt som al-Kindi på 800-talet skrev om kryptoanalysen och den islamska kulturen hade sin guldålder skulle man i Europa under samma tid fortfarande inte ha upptäckt det mest grundläggande inom kryptografin. Det skulle dröja ända in på 1300-talet innan kryptografin började användas i Europa av lärda män och Europas förste framstående kryptoanalytiker Giovanni Soro skulle träda fram först under 1500-talet (Singh 1999, s. 45-46).

Flera stater fortsatte att försöka dölja innehållet i sina meddelanden med hjälp av monoalfabetiskt substitutionskrypton (den kategori samtliga substitutionskrypton som nämns ovan faller under), utan att veta om att duktiga forcörer kunde läsa innehållet med hjälp av frekvensanalysen. Allt fler länder fick dock kännedom om substitutionens svagheter och försökte då stärka kryptot på olika sätt. Några exempel på dessa försök var att stava orden fel i texten eller att sätt in så kallade nollor vilket var bokstäver i kryptotexten som egentligen inte motsvara någon bokstav i det riktiga meddelandet. Till exempel om vi vill sända ett HEJ kan vi skriva H1E2J och låta H = B, E = T, J = R, 1 = C och 2 = P. klartexten H1E2J vilket har budskapet HEJ vilket en mottagare med en nyckel hade förstått, får en kryptotext BCTPR vilket för en kryptoanalytiker ser ut att vara ett ord på fem bokstäver istället för tre som HEJ.

Ett annat försök att stärka säkerheten i ett substitutionskrypto var införandet av koden. Här lät man en bokstav motsvara ett helt ord (kodord), P kunde till exempel motsvara ANFALL och L kunde vara I NATT, P-L utläses alltså ANFALL I NATT. Den stora nackdelen med koder är den enormt stora kodbok som måste konstrueras för samtliga sändare och mottagare som vill använda sig av denna typ av meddelande och om en fiende skulle få tag i kodboken måste detta mycket mödosamma arbete göras om från början.

Trots försöken att förstärka substitutionskryptot kunde de skickligaste kryptoanalytikerna dechiffrera dessa och knäcka samtliga koder. Detta ledde till att deras ledare sedan kunde ta del av hemlig information vilket skulle leda till en rad avgörande beslut i Europa och den övriga världens historia. Den säkra kommunikationen var hotad och det var numera helt klart att kryptografin och kodmakarna återigen behövde sätta fart framåt för att ta fram en starkare typ kryptering. ”Nöden är ju uppfinningarnas moder” (Singh 1999, s.29).

2.4 Enigma

Vi kommer nu ta ett stort steg framåt i tiden till den historiska period som skulle komma att kallas mellankrigstiden. Året var 1923, det första världskriget var avslutat och ett brittiskt dokument skulle komma att publiceras av Winston Churchill som innehöll uppgifter om att de brittiska kryptoanalytikerna regelbundet under första världskriget hade kunnat läsa hemliga tyska meddelanden. Den tyska armen hade helt enkelt spelat med öppna kort inför engelsmännen, vilket hade inneburit en oerhörd fördel för de allierade under kriget. Detta kom som ett chockbesked för Tyskland som genast började se sig om efter ett säkrare sätt att kommunicera – ett sådant grovt misstag fick inte upprepas en gång till (Singh 1999, s.166).

Fram till slutet av första världskriget hade de mest avancerade kryptografiska systemen använt sig av vanlig kryptering med papper och penna. De här systemen kändes nu föråldrade och man ville införa den tidens nya teknik i krypteringen (Gilman u.å.). Tyskland som nu var ute efter det absolut säkraste och senaste inom kryptografin skulle komma att vända sig till en man vars namn var Arthur Scherbius. Scherbius var en tysk affärsman som år 1918 patenterade en maskin han kallade Enigma (ibid.). Enigma var en maskin som skulle komma att bli det mest kända och fruktade chiffret genom historien, då Tyskland år 1923 beställde en specialtillverkad version av maskinen till militären. Enigma ansågs vara helt omöjlig att knäcka och skulle komma att användas av den tyska flottan tre år senare följt av armen 1928, flygvapnet 1933 och fortsatt in under den ”mest omfattande och blodiga konflikten i människans historia” (SO-rummet, 2014), det andra världskriget (Ellis 2005; Lycett, u.å).

Med hjälp av en simulation av Scherbius maskin (Enigma Simulator v 7.0) kan meddelandet MATEMATIK göras om till enigmakod, vilket ser ut så här: DDHWHWHBS.

Klartext:	M	A	T	E	M	A	T	I	K
Enigmakod:	D	D	H	W	H	W	H	B	S

Här har vi något som vi inte sett i de tidigare chiffren. D, W och H dyker alla upp flera gånger i kryptotexten och de motsvara inte samma bokstäver i klartexten. Exempelvis krypteras M till D och senare krypteras också A till D. En annan märklig sak vi kan se i enigmakoden är att A dyker upp två gånger i ordet MATEMATIK men krypteras i enigmakoden till två olika bokstäver. Det första A:et krypteras till D och det andra till H. I de äldre krypteringssystemen som skrevs med papper och penna som vi såg exempel på ovan skulle en bokstav från klartextalfabetet hela tiden blivit samma bokstav i kryptoalfabetet. Enigmasystemet är annorlunda och det var därför Tyskland trodde att de hade en obrytbar kod (Numerphile, 2013). Om meddelandet MATEMATIK återigen matades in i maskinen kommer vi denna gång att få ut enigmakoden VKELRMWYP och varje gång meddelandet MATEMATIK skrivs in i maskinen kommer bokstäverna krypteras på ett nytt sätt. Det skulle dock visa sig att Enigma, i motsats till vad Tyskarna själva trodde, inte alls var omöjlig att dekryptera. Brittiska och polska krypteringsanalytiker lyckades år 1940 knäcka enigmakoden, något historiker menar förkortade andra världskriget med hela två år (Ellis, 2005).

2.4.1 Så fungerar Enigmamaskinen

Trots sin komplexitet kan Scherbius Enigmamaskin brytas ned till tre huvudsakliga beståndsdelar. Den första är ett tangentbord där operatören kan skriva in sitt klartextmeddelande och samtliga bokstäver på tangentbordet är därefter kopplade till en slumpkodningsenhet. Denna slumpkodningsenhet består i sin tur av en skiva tätt isolerad i gummi, där fullt av elledningar är utplacerade. Var och en av dessa elledningar går sedan vidare från slumpkodningsenheten till den slutliga delen av Scherbius uppfinning, vilket är en tavla full av lampor som kommer lysa upp en ny bokstav. Alltså en ledning går från exakt en klartextbokstav på tangentbordet vidare genom slumpkodningsenheten där elledningarna placerats ut på ett hemligt vis, där sedan varje ledning leder fram till en lampa som lyser upp kryptobokstaven för operatören (Singh 1999, s. 151; Wobst 2001, s. 40-41). Om operatören till exempel skriver in bokstaven B på sitt tangentbord går sedan den elektriska impulsen fram till en lampa som tänder upp en ny bokstav vilket skulle kunna vara A (beroende på hur maskinen är inställd). Det här motsvarar ett

substitutionskrypto som vi känner igen sen tidigare, men nu framtaget på ett nytt mer effektivt sätt där man istället för att utföra kryptot med penna och papper, nu använder en elektrisk maskin (Wobst 2001, s. 40). Scherbius hade emellertid tagit sin maskin längre än att endast motsvara ett föråldrat substitutionskrypto. Han lät slumpkodningsenheten i Enigmamaskinen rotera ett steg (eller ett tjugosjättedelsvarv om vi ser till hela det engelska alfabete som fanns på maskinens tangentbord) varje gång operatören slog in en bokstav (Singh 1999, s. 152). Det ger oss också svaret på varför en klartextbokstav kunde motsvara flera olika kryptobokstäver. Om en operatör slår in klartextbokstaven B kommer lampan för kryptobokstaven A att lysa upp som i exemplet ovan, om operatören återigen slår in klartextbokstaven B kommer slumpkodningsenheten att ha roterat ett steg och kablarna möbleras då om på ett nytt sätt vilket leder till att B inte längre kommer att bli A utan en annan lampa kommer istället lysa upp kryptobokstaven C (beroende på hur kablarna är anordnade). Trycker operatören igen på B roterar slumpkodningsenheten åter ett steg och kryptobokstaven E lyser upp och så vidare. På det här viset skapar Enigmamaskinen tjugosex olika kryptoalfabet, och man får här ett så kallat polyalfabetiskt krypto (Singh 1999, s. 154). Det polyalfabetiska kryptot är en vidareutveckling av substitutionskryptot som först togs fram av fransmannen Blaise de Vignere som en reaktion mot att man lyckas dekryptera substitutionskryptot med hjälp av frekvensanalysen. Tack vare att en klartextbokstav kan motsvara flera olika kryptobokstäver i ett polyalfabetiskt krypto kommer man här bort från problemet med dubbelbokstäver som substitutionskryptot led av och som också utnyttjades av kryptoanalytiker genom att använda sig av dekrypteringsmetoden frekvensanalys (Järpe 2005, s.162-163).

Ett problem som kommer att uppstå med systemet vi beskrivit ovan är när B tryckts på tjugosju gånger (tjugosex bokstäver i det engelska alfabetet). Då kommer krypteringssystemet att ha gått runt ett helt varv och börjat om från början (B blir åter A). Upprepningar ger struktur och regelbundenhet vilket är egenskaper en kodknäckare kommer att använda emot krypteringssystemet och är därför något man vill undvika (Singh 1999, s. 154). Scherbius löste problemet genom att installera fler slumpkodningsenheter. När två slumpkodningsenheter installeras fungerar dessutom systemet som så att den andra slumpkodningsenheten i ordningen inte rör sig ett steg framåt förens den första har gått ett helt varv. Detta på grund av en monterad kugge på den första slumpkodningsenheten som efter att den gått ett helt varv skjuter fram den andra slumpkodningsenheten ett steg. Fördelen med att montera in ytterligare en slumpkodningsenhet är att det fördröjer krypteringssystemet att komma tillbaka till utgångsläget – det krävs nu att den första

slumpkodningsenheten rör sig tjugosex hela varv för att detta ska ske eller att operatören krypterar 26•26 = 676 bokstäver. Detta innebär att maskinen nu skulle ha 676 olika inställningar eller med andra ord 676 möjliga kryptoalfabet. Men Scherbius nöjde sig inte med två slumpkodningsenheter utan installerade i Enigma tre stycken vilket ger oss 26•26•26 = 17576 potentiella inställningar (Singh 1999, s.156).

När en operatör vill skicka ett meddelande med Enigmamaskinen måste denne först välja en av de 17576 olika inställningarna, vilket utgör maskinens startposition och kan också sägas vara kryptots nyckel (Sing 1999, s. 157). När en startposition valts ut kan sedan meddelandet skrivas in på Enigmamaskinens tangentbord och för varje klartextbokstav som matas in kommer en ny kryptobokstav att lysa upp på en panel framför operatören. Kryptobokstäverna som lyses upp antecknas av operatören. Flera mil bort kan en tysk officer befinna sig och nås via radio från operatören och få tillgång till kryptot. Officeren har själv en Enigmamaskin exakt likadan som operatörens. Officeren behöver sedan ställa in sin Enigmamaskin på samma startposition som operatörens och kan sedan skriva in kryptotexten på sitt tangentbord och få tillbaka klartexten som operatören skrev in. Hur visste då officeren vilken startposition operatören hade på sin Enigmamaskin? Ingångsinställningarna (nyckeln) fanns tillgängliga i en kodbok som varje månad skickades ut till samtliga användare och ingångsinställningarna ändrades varje dag efter manualen (Perimeter institute for theoretical physics 2014). Så länge en fiende inte hade tillgång till denna kodbok spelade det ingen roll om de hade stulit eller konstruerat sin egen Enigmamaskin då det ändå inte kände till startpositionen (Singh 1999, s. 158-159). Scherbius valde dock att ytterligare säkra kommunikationen och gjorde det möjligt att själv välja position på de tre slumpenheterna, vilka gick att placera på sex olika sätt för att öka antalet möjliga nycklar. Man kunde exempelvis välja att byta plats på den första och tredje slumpenheten (ibid, s. 159). Den här typen av Enigmamaskin sålde Scherbius bland annat till banker, men de maskiner som såldes till militären hade något extra, vilket var en kopplingstavla med stickkontakter som satt mellan tangentbordet och den första slumpenheten (Numberphile 2013). Med hjälp av kopplingstavlan kan man para ihop bokstäver, säg att vi kopplat samman A och B. Om nu en operatör trycker in klarbokstaven A på tangentbordet kommer maskinen istället uppfatta det som att det var B som trycktes in och följa Bs elledning fram till dess kryptobokstavs lampa (Singh 1999, s.159). Möjligheten att para ihop tjugosex bokstäver ger en jättelik mängd kombinationer. Låt oss nu räkna på de olika variablerna i en Enigmamaskin och se just hur många nycklar där finns att välja bland.

Vi börjar med stickkontakterna. För att göra det hela lättare börjar vi med fyra bokstäver A, B, C och D och två stycken kablar. För den första kabeln finns fyra möjliga val för den första änden av kabeln och tre val för den andra änden, vilket ger totalt 4•3 = 12 val. Den första kabeln skulle alltså kunna para ihop dessa par:

AB, AC, AD, BA, BC, BD, CA, CB, CD, DA, DB, DC.

Som vi kan se i listan ovan kommer dock vissa par att dyka upp två gånger, till exempel är AB samma par som BA. Vi måste alltså dela med två och vi får (4•3)/2 = 6 möjliga par med den första kabeln. Paren vi har att välja på för den första kabeln är alltså:

AB, AC, AD, BC, BD, CD

För den andra kabeln kan man tänka sig att den första kabeln nu ockuperar två bokstäver. Den andra kabelns ena ände har därför två bokstäver kvar att välja bland och den andra änden har en bokstav kvar och med samma tanke sätt som innan borde vi då få ((4•3)/2) • ((2•1)/2) = 6 möjliga par för två kablar. Paren är för två kablar är följande:

(AB, CD), (AC, BD), (AD, BC), (BC, AD), (BD, AC) och (CD, AB)

Vi märker dock i listan ovan att vissa par återkommer två gånger:
(AB, CD) = (CD, AB)
(AC, BD) = (BD, AC)
(AD, BC) = BC, AD)

Vi har alltså inte sex stycken par, vi har räknat ut ett för stort tal av möjliga par. Det vi måste göra för att få det hela rätt är att dela med två och kommer då fram till sanningen vilket är tre möjliga par för två kablar

(½)•((4•3)/2) •((2•1)/2) = 3

(AB, CD), (AC, BD) och (AD, BC) totalt tre par.

Om vi nu istället för fyra bokstäver räknar med samtliga tjugosex bokstäver som finns tillgängliga på Enigmamaskinens tangentbord (A-Z) kommer vi på samma sätt som ovan att få:

(1/2) • ((26•25)/2) •((24•23)/2) = 44850

Antal sätt att kombinera två par bokstäver av tjugosex och där med att låta dem byta plats är alltså 44850. Där (1/2) i uttrycket ovan står för antalet sätt att arrangera ett par (Standford University u.å). Vanligt vis fanns det sex kablar till en Enigmamaskin (Singh 1999, s. 159). Med sex stycken kablar och tjugosex bokstäver skulle vi istället få 100 391 791 500 kombinationer, ett tal Scherbiu**s,** konstruktören av Enigmamaskinen, sägs var väldigt belåten över (Perimeter institute for theoretical physics 2014).

(1/6!) • ((26•25)/2) • ((24•23)/2) • ((22•21)/2) • ((20•19)/2) • ((18•17)/2) • ((16•15)/2) = 100 391 791 500

En allmänformel för vilken mängd kablar som helst ser ut som följande:

(1/k!)((26•25•24•.. •(26-(2k-1)))/2^k)
(Standford University u.å)

Antalet möjligheter för kopplingstavlan är alltså 100 391 791 500 stycken. Om vi nu går vidare till de tre slumpenheterna gick var och en av dessa ställa in på tjugosex olika sätt. Vi får därmed 26• 26 •26 = 17576 olika inställningar. Dessa tre slumpenheter kunde dessutom placeras om så att den första enheten som placeras har tre olika platser att välja bland, den andra enheten som placeras ut har de två platserna som den första lämna efter sig att välja bland och den tredje kan placeras ut på den plats som blir över efter de två andra slumpenheterna. Detta ger 3! = 3•2•1 = 6 olika placeringar (123, 132, 213, 231, 312, 321). Totalt kommer vi alltså av Enigmamaskinen att få 100 391 791 500 • 17576 • 6 = 1,058691676•10^16 ≈ 10 000 000 000 000 000 möjliga nycklar (Singh 1999, s. 161). Om någon av det allierade skulle få tag på en av Tysklands Enigmamaskiner och avlyssna ett radiomeddelande där en kryptotext meddelas skulle de alltså finnas 10 000 000 000 000 000 olika startinställningar på maskinen att prova för att kunna få tillbaka meddelandet med maskinen.

2.5 RSA skyddar din e-post

Ett problem som finns bland samtliga krypteringssystem som diskuterats hittills är distributionen av nyckeln till kryptot mellan sändaren och mottagaren. För att ha möjlighet att göra budskapet i ett krypterat meddelande förståligt igen måste mottagaren känna till nyckeln, och den enda metoden man kände till för att ge mottagaren tillgång till nyckeln var att personligen eller med hjälp av en budbärare lämna över denna till mottagaren. Att använda sig av en budbärare för dessvärre med sig vissa problem, för hur tryggt kryptosystemet än är kommer ändå sändaren och mottagaren vara beroende av en tredje part som av misstag eller av vilja kan lämna nyckeln till fel mottagare. Med andra ord blir ett krypteringssystem i teorin inte starkare än sin nyckeldistribution. Före 1960 var nyckelhanteringen problematisk, men det gick fortfarande att hantera då det i stort sätt bara var regeringen och militären som använde sig av kryptering. På 1960-talet skulle detta komma att förändras. Datorerna blev allt kraftfullare och billigare vilket förde med sig att allt fler företag började köpa in dem. Dessa företag använde datorn bland annat för bankärenden, och kryptering behövdes för att skickad ekonomiska transaktioner. Bankerna var i behov av att dela ut nycklar till sitt krypteringssystem till alla företagare det hade för avsikt att ha en elektronisk förbindelse med, där av anställdes kvinnor och män som kurirer som varje dag levererade enorma mängder disketer, kort och all annan möjlig nyckelförvaring till företagen. Det hela var mycket kostsamt och ur logistisk synpunkt var det hela en mardröm (Singh 1999, s. 279-280). Under samma tid pågick det kalla kriget, en maktkamp mellan de två nationerna USA och Sovjetunionen (Nationalencyklopedin 2014). De två länderna var inte i öppet krig, men ut ifall att bomberna skulle falla ville man från det amerikanska försvarsministeriet sida säkra sin datakommunikation. Man valde därför att finansierar en organisation som kallades Advanced Research Projects Agency (ARPA). Organisationen fick uppdraget att sammanbinda militärens datacentraler som var utspridda över ett stora geografiskt område till ett nätverk, så att datorerna kunde kommunicera med varandra även om någon av centralerna skulle bombas och slås ut. 1969 bestod ARPAnet av fyra datorer men skulle snabbt växa till sig och bli det vi idag kallar Internet (Singh 1999, s. 282). Om nu till och med banker och storföretag hade problem med sin nyckeldistribution, skulle det bli näst intill omöjligt att garantera en ostörd kommunikation för de 2,4 miljarder (motsvara cirka 1/3 av jordens befolkning) människor som idag använder internet (Nationalencyklopedin 2014). För att allmänheten skulle få rätten till ett ostört privatliv på Internet behövdes en ny metod för nyckelhanteringen.

2.5.1 Diffie-Hellman-Merkelsmetoden – en lösning till nyckeldistributionen

Trots datorns genombrytning under 1960-talet, var det ändå ett nytt sätt att hantera nyckeldistributionen som skulle bli kryptografins största genombrott sen antikens substitutionskrypto. Problemet skulle få sin första lösning år 1976 då Diffie-Hellman-Merkelsmetoden offentligt publicerades (Singh 1999, s. 281, 293).

Hur kan då två personer som aldrig träffats personligen dela en nyckel? De kan inte prata klarspråk på telefonnätet på grund av risken att bli avlyssnad utifrån. För att tackla det här problemet började Martin Hellman och Whitfield Diffie undersöka en rad olika matematiska funktioner, där de speciellt intresserade sig för envägsfunktioner. En envägsfunktion kan beskrivas som att den är lätta att utföra, men svår att sen återställa. Ett exempel skulle kunna vara att det är lätt att blanda ihop två färger för att få en tredje färg, men det blir svårt att återställa de två färgerna som blandades om man från början bara tilldelas den blandade färgen (Singh 1999, s. 289-290). För att kunna genomföra exemplet med färgerna matematiskt vände sig Hellman och Diffie till den modulära aritmetiken, vilken kan illustreras med hjälp av en digital klocka. Om klockan just nu skulle vara 22:00 och någon säger till dig att vi ses om åtta timmar, brukar man räkna framåt och komma fram till att man ska ses 06:00 och inte klockan 30:00 (som talen 22 och 8 skulle bli om de adderas på vanligt vis). Eftersom timmarna på en digital klocka startar om vid midnatt (24) kan vi säga att vi befinner oss i mod 24. Vi har nu beräknat 22+8 mod 24, som blir $22+8 \equiv 6 \bmod 24$. Ett snabbare sätt att tänka är att addera de två talen som vanligt 22+8 = 30, för att sedan få svaret i mod 24 dividerar vi 30 med 24 och får då 30/24 = 1, med en rest 6. Alltså $22+8 \equiv 6 \bmod 24$. Anledningen till att Hellman och Diffie var så intresserade av just det här räknesättet var för att det kan fungera precis som färgen. Om vi först tar ett exempel inom den traditionella aritmetiken säg 3^x och väljer x till 5 kommer vi att få $3^5 = 3 \bullet 3 \bullet 3 \bullet 3 \bullet 3 = 243$. Om vi nu istället blir tilldelade 243 och ska ta reda på vilket tal trean upphöjdes med är detta en ganska enkel uppgift eftersom att värdet hela tiden ökar i den vanliga aritmetikens värld när x i 3^x blir allt större. Därför kan vi bara chansa på ett tal, säg att x är fyra och snabbt se att det var för litet ($3^4 = 81$). Därefter kan man istället prova ett högre tal och därmed komma tillbaka till femman som användes för att få fram 243. Om vi nu istället får samma uppgift i den modulära aritmetiken och befinner oss i mod 17 kommer uppgiften att bli svårare. Säg att vi vet att $3^x \bmod 17$ ska bli 12, vad är då x för att detta ska stämma? Vi kan som förut försöka pröva oss fram och gissa ett tal x ska bli. Säg

att vi börjar med att gissa på x = 4 vilket blir 3^4 mod17 ≡ 13. 13 är högre än 12 och med samma tanke sätt som i den vanliga aritmetiken kan vi då prova ett lägre tal på x. Men det kommer då visa sig att man är på väg åt helt fel håll då x inte är lägre utan ett högre tal i den rätta lösningen vilket är x = 13, 3^{13} mod17 ≡ 12. Hellman och Diffie hade nu sin envägsfunktion, lätt att utföra men svår att återställa (Singh 1999, s. 291-292).

Låt oss kalla de två personerna som nu vill sända ett meddelande till varandra Sofia och Anna. Diffie-Hellman-Merkels metoden fungerade sedan som följande. Sofia och Anna kommer först överens om en envägsfunktion som i exemplet ovan. Detta görs offentligt så att vem som helst skulle kunna höra. Anna och Sofia bestämmer sig i det här fallet för att använda sig av envägsfunktionen 3 mod 17. Sofia väljer sedan ett för henne helt privat nummer, hon bestämmer sig för 15. Sofia beräknar sedan 3^{15} mod 17 ≡ 6 och skickar sedan offentligt resultatet (i detta fall 6) till Anna. Anna väljer sen sitt egna privat nummer, säg att hon väljer 13. Anna räknar ut 3^{13}mod 17 ≡ 12 och skickar sedan sitt resultat öppet till Sofia. Sofia tar sedan Annas resultat 12 och höjer upp detta med sitt privata nummer 15, 12^{15} mod 17 ≡ 10. Anna tar Sofias resultat 6 och höjer upp detta med sitt privata nummer 13, 6^{13} mod 17 ≡ 10. Det har nu båda kommit fram till samma resultat 10, vilket blir deras nyckel. Hur kunde då Anna och Sofia komma fram till samma resultat? Om vi utgår från Sofia så fick hon 12 av Anna som hade räknats ut ifrån 3^{13} mod 17. Sofia kommer då fram till 10 genom att beräkna 12^{15} mod17. Hon skulle lika gärna kunna byta ut 12 mot 3^{13} och får då $(3^{13})^{15}$ mod17. På samma sätt kan Anna byta ut 6 som hon fick av Sofia till 3^{15} och kommer då fram till nyckeln 10 genom att använda $(3^{15})^{13}$ mod17. De har alltså gjort samma uträkning med den skillnaden att exponenterna är omvända vilket inte spelar någon roll då $(x^a)^b = x^{ab}$ vilket ger samma resultat som $(x^b)^a = x^{ba}$ (Computer science uc santa barbara 2014; Mathinsight 2014).

Samtidigt som Anna och Sofia skickade sin nyckel blev det avlyssnade av Carolina. Vad fick då Carolina för uppgifter av samtalet ovan? Hon fick deras envägsfunktion 3 mod 17 samt resultaten 12, 6 och med hjälp av dessa upplysningar kan Carolina inte komma fram till nyckeln (Singh 1999, s. 295). Sändaren och mottagaren kunde nu genom att använda Diffie-Hellman-Merkels metoden bestämma sin nyckel i hemlighet utan att varken behöva träffas eller skicka en budbärare. Problemet med nyckelöverföringen var nu äntligen ur vägen, men ett mer effektivt sätt att lösa samma problem skulle utvecklas redan året därpå 1977. Detta mer effektiva krypteringssystem som togs fram av Ron Rivest, Adi Shamir och Leonard Adelman skulle få namnet RSA efter upphovsmännen (ibid, s. 297, 304).

2.5.2 RSA – asymmetrisk kryptering

RSA är än idag världens mest kända krypteringssystem och används så väl av privatpersoner som stora multinationella företag som till exempel Microsoft, IBM, Adobe och Apple. RSA försvarar även Amerikas kärnvapen från att fel händer (Thorbiörnson 2004).

Hur fungerar då krypteringssystemet RSA? Systemet bygger på idén om att multiplikation av två stora primtal är en envägsfunktion. Det är lätt att multiplicera ihop det två primtalen 5689 och 2917 och med en miniräknare få fram 16594813. Men om vi istället blir tilldelade produkten 16594813 och tillbes plocka fram primtalsfaktorerna (alltså de två primtal som multiplicerades ihop) kommer detta att bli en mycket mer krävande uppgift (Silverman 2014, s. 455; Thorbiörnson 2004). Idag känner man inte till någon tillräckligt effektiv faktoriseringsalgoritm för att RSA-krypteringen ska vara i fara, men det ska här också tilläggas att det inte bevisats att en sådan faktureringsmetod inte skulle existera vilket är en osäkerhet RSA-användaren får leva med tills vidare (Björner u.å., s. 7).

Om primtalen väljs tillräckligt stora för att vår produkt ska bli 130 siffror långt skulle en modern dator ta fem år på sig att faktorisera talet (Thorbiörnson 2004). Dagens banker använder sig år 2012 av tal som är 617 siffror långa (man brukar säga att talet är $10^{617} \approx$ 2048-bit stort). Detta kan jämföras med antalet atomer i universum som är ett 79 siffror långt tal (Universtoday 2009; Numverphile 2012). Ett så stort tal som 2048-bit är idag omöjligt att faktorisera. Det största talet som man har lyckats att knäcka är 768-bit långt, och det tog två år för en grupp akademikers samlade datorkraft att genomföra detta. Den tekniska utvecklingen går fort framåt och 1024-bit långa tal kan vara möjliga att faktorisera inom några år; Gmail, Google+ och Facebook använder idag 1024-bit vilket snart borde bytas ut (Numberphile 2012).

Om vi nu vill försöka kryptera ett meddelade med RSA kan vi börja med att välja två primtal och kalla dessa p och q. Efter att de två primtalen valts ut multipliceras dessa $N = p \cdot q$ för att få vår produkt N, och om p och q är tillräckligt stora kommer N att bli ett massivt tal som kommer att bli oerhört svårt att faktorisera. p och q kommer att vara privata för den som väljer att kryptera med RSA (Thorbiörnson 2004). Efter att vi fått tag på N behöver vi använda oss av den schweiziska matematikern Leonhard Eulers berömda φ-funktion (där symbolen φ uttalas fi). Om vi skriver φ(N) kommer vi ta reda på hur många heltal som är mindre än N och som inte delar någon gemensam delare med N större

än 1, man brukar säga att det talet då är relativt prima till N. Till exempel blir φ(10) = 4 på grund av att det finns fyra tal mindre än 10 som inte har någon gemensam delare större än 1. Dessa är 1, 3, 5,och 7. När det kommer till primtal är φ-funktion lätt att beräkna.

$$\varphi(p) = p - 1$$

För funktionen gäller dessutom att

$$\varphi(p \cdot q) = \varphi(p) \cdot \varphi(q)$$

Tidigare sa vi att våra två valda primtal multiplicerades ihop till N (N = p • q). Det borde föra med sig att φ(N) = φ(p•q) = φ(p) • φ(q). Funktionen är enkel att lösa för primtal vilket p och q är, och vi kan därför skriva om φ(N) = φ(p) • φ(q) som φ(N) = (p-1) • (q-1) (Thorbiörnson 2004). Nästa steg blir att välja ett tal mellan 0 och φ(N) som vi kallar e, talet e får heller inte ha någon gemensam nämnare med φ(N) större än 1. Talen N och e kan sedan delas med omvärlden, det blir kryptots offentliga nycklar (Silverman 2014, s. 132; Thorbiörnson 2004). Dessa två nycklar kan sedan användas för att kryptera ett meddelande med följande formel

$$C \equiv M^e \bmod N$$

där e och N är våra offentliga nycklar. C är det krypterade meddelandet och M är klartextmeddelandet. M består av bokstäver som har konverterats till siffror enligt något välkänt system som till exempel The American Standard Code for Information Interchange (ASCII) (Thorbiörnson 2004).

En sändare kan alltså hitta mottagarens utlagda nycklar e, N och med dessa enkelt kryptera sitt klartextmeddelande M genom att beräkna $M^e \bmod N \equiv C$ och skickar därefter det krypterade meddelandet C till mottagaren. Eftersom detta är en envägsfunktion är det enkelt att beräkna $M^e \bmod N \equiv C$, men det är svårt att få tillbaka M om man bara känner till $?^e \bmod N \equiv C$. Så hur kan då mottagaren när denna nås av C som sändaren skickat få tillbaka M? Hemligheten är att mottagaren har en hemlig nyckel d så att

$$C^d \bmod N \equiv M$$

Den hemliga nyckeln d återställer alltså C till M igen, så att mottagaren kan läsa det krypterade meddelandet från sändaren (Thorbiörnson 2004). Var kommer då den hemliga nyckel d ifrån? d är inversen till e mod φ(N), vilket beräknas med formeln

$ed \equiv 1 \bmod \varphi(N)$

Det betyder att om man delar e•d med φ(N) måste d uppfylla att operationen får resten 1. $ed \equiv 1 \bmod \varphi(N)$ kan beräknas genom att använda sig av Euklides algoritm. $ed \equiv 1 \bmod \varphi(N)$ kan dessutom skrivas som $(e \cdot d) -1 = k\, \varphi(N)$ (där k är något heltal). Detta kan sedan skrivas som $e \cdot d = 1 + k\, \varphi(N)$. d blir alltså

$d = (1 + k\varphi(N))/e.$

Följande beräkning visar varför vi får tillbaka klartextmeddelandet M när vi höjer upp krypteringstexten C med d:

$M^e \bmod N \equiv C$
$C^d \bmod N \equiv M$
$d = (1 + k\varphi(N))/e$

$C^d = (M^e)^d = M^{e\,d} = M^{e(1 + k\varphi(N))/e} = M^{1 + k\varphi(N)} = M \cdot M^{k\varphi(N)}$

Eulers sats säger att $a^{\varphi(N)} \equiv 1 \bmod n$, därav blir

$M \cdot M^{k\varphi(N)} = M \cdot 1^k \equiv M \bmod N$
Alltså $C^d \equiv M \bmod N$

(Maxey 2012, s. 7)

Låt oss nu avsluta genom att ge ett exempel där ett meddelande krypteras och dekrypteras med hjälp av RSA.

Exempel 8

Börja med att välja två primtal p och q

p = 17 q = 41

Räkna sedan ut den första publika nyckeln N

N = p • q = 17 • 41 = 697

N = 697

Räkna sedan ut φ(N)

φ(N) = (p-1)(q-1) = (17-1)(41-1) = 640

Välj sedan ut den andra publika nyckeln e, där e är ett tal mellan 0 och φ(N) som inte har någon gemensam delare med φ(N), SGD(e, φ(N)) =1.

Vi väljer

e = 11

För att kontrollera att SGD(11, 640) = 1 använder vi Euklides algoritm

640 = 11·58 +2

11 = 2·5 + 1

2 = 1·2 + 0

När vi har resten 0 går vi ett steg tillbaka till resten vi fick innan nollan, detta är den största gemensamma delaren för 11 och 640 vilket är 1

Den privata nyckel d måste uppfylla att ed ≡ 1 mod φ(N) alltså

11d ≡ 1 mod 640

d finner vi genom att lösa den diofantiska ekvationen 11d +640y = 1

Denna ekvation kan lösas genom att först utföra Euklides algoritm på 11 och 640 som ovan

640 = 11·58 + 2

11 = 2·5 + 1

Sedan utför vi algoritmen baklänges för att få fram d. Där det andra ledet ovan (11 = 2·5 + 1) kan skrivas om som

$1 = 11 \cdot 1 - 2 \cdot 5$

$1 = 11 \cdot 1 - 5(640 \cdot 1 - 11 \cdot 58)$

$1 = 11 \cdot 1 - 640 \cdot 5 + 11 \cdot 290$

$11 \cdot 291 + 640 \cdot (-5) = 1$

$d = 291$

$(d \equiv e^{-1} \bmod \varphi(N) \equiv 11^{-1} \bmod 640 \equiv 291 \bmod 640)$

De publika nycklarna är nu alltså e = 11 och N = 697, dessa kan nu sändas ut till alla som kan tänkas villa skicka ett krypterat meddelande till oss.

Nu vill någon sända meddelandet HEJ till oss. Sändaren börjar då med att göra om bokstäverna H, E och J till heltal efter en standard som både sändaren och mottagaren använder. I detta exempel kan vi använda systemet nedan:

D	E	F	G	H	I	J
0	1	2	3	4	5	6

H = 4, E = 1 och J = 6
Meddelandet HEJ representeras alltså av siffrorna 416

M som står för meddelande är alltså
M = 416

Nu kan sändaren använda sig av de publika nycklarna e = 11 och N = 697 och sätta in sitt M i formeln:
$C \equiv M^e \bmod N$
$C \equiv 416^{11} \equiv 274 \bmod 679$

416^{11} kan beräknas med hjälp av räknereglerna för modulär aritmetik

$416^{11} = 416 \cdot 416^{10} = 416 \cdot (416^2)^5 \equiv 416 \cdot (200)^{5 =} 416 \cdot 200 \cdot (200^2)^{2} \equiv 257 \cdot (200^2)^{2}$
$\equiv 257 \cdot (271)^2 = 257 \cdot 256 \equiv 274$

Alltså är C = 274, som sändaren kan skicka tillbaka till oss

Vi kan sedan använda vår privata nyckel d = 291 för att få tillbaka meddelandet M genom att använda formeln
$M \equiv C^d \bmod N$
$M \equiv 274^{291} \equiv 416 \bmod 2623$
M = 416

Därefter använder vi samma alfabete som ovan för att kunna tolka budskapet i meddelandet

4 = H, 1 = E, 6 = J

Meddelandet är HEJ

Om någon skulle avlyssna kommunikationen skulle de få reda på N, e och C. Men för att kunna få tillbaka M behöver de känna till den hemliga nyckeln d och för att kunna veta vad d är måste den som avlyssnat känna till φ(N), vilket bara är möjligt om personen i fråga känner till vilka två primtal som multiplicerades ihop då φ(N) =(p-1)(q-1). För att ta reda på vilka dessa primtal var måste den som avlyssna samtalet faktorisera N vilket är en tuff uppgift speciellt om vi väljer ett ännu större värde på N.

3 Kryptering som inslag i skolans matematikundervisning?

I Skolverkets (2011) läroplan för gymnasieskolan går det för samtliga kurser i matematik att finna vilket innehåll som ska ha behandlats under kursens gång. I läroplanen för en av gymnasieskolans senare kurser (Matematik 5) framgår det att följande avsnitt ska ha gåtts igenom när kursen är avslutats:

- Matematiska problem med anknytning till matematikens kulturhistoria
- Begreppet kongruens hos hela tal och kongruensräkning
- Begreppen *permutation* och *kombination*
- Metoder för beräkning av antalet kombinationer och permutationer

”Kunskap blir kunskap först när den kan sättas in i ett sammanhang” skriver Liedman (Liedman 2002, s. 18-19). Kryptering kan i detta fall fungera som ett sammanhang för matematisk kunskap eftersom kryptering kan ses som en praktisk tillämpning för de två matematiska verktygen (kongruensräkning och kombinatorik) som nämns ovan. Både kongruensräkning (modulär aritmetik) och kombinatorik (vilket handlar om att studera kombinationer) finner vi i hög grad bland flera av de krypteringssystem som tidigare nämnts i studien, och kryptering är dessutom en självklar del av matematikens kulturhistoria.

Lotta Wedman är gymnasielärare i matematik och beskriver i artikeln *Kryptering på gymnasiet* (2005) hur hon sökte efter områden som kunde visa eleverna att matematikinnehållet i de senare kurserna på gymnasiet hade praktiska tillämpningar. Valet föll på kryptering, vilket undervisningen sedan utgick från. Hon menar att nästan hela gymnasiets kombinatorikavsnitt kunde täckas in genom att undervisa om Enigmamaskinen och dess olika beståndsdelar (däribland det antal slumpenheter i maskinen som kan ge upphov till olika kombinationer av kryptoalfabeten). Eleverna var optimistiska till projektet och bidrog själva med förslag till undervisningen, vilket resulterade i en pappersmodell av Enigmamaskinen. Wedman (2005) berättar också att hon själv tyckte att denna tillämplig gjorde att undervisningen ”blev roligare och mer motiverande” (Wedman 2005, s. 4).

När eleverna arbetade med Enigma lärde de sig förutom kombinatorik mer om andra världskriget (Wedman 2005, s. 1). Det är sällsynt att reella teman och fenomen följer den traditionella ämnesindelningen. Att arbeta ämnesintegrerat har många pedagogiska

fördelar; bland dem finner vi möjligheten att ge eleverna en helhetssyn på ämnet och att arbeta på ett mer verklighetsnära sätt eftersom man får chansen att släppa läromedlet och söka efter andra källor (Sjöberg 2010, s. 501; För det vidare 2012). Matematik har en tendens kombineras med de naturvetenskapliga ämnena så fort ett projekt ska startas upp, medan matematikläraren har svårare att hitta områden att samarbete kring med de övriga skolämnena (Purdue university 2006). Temat kryptering skulle fungera som ett ämnesintegrerat projekt där matematiken kan arbeta ihop med alla skolämnen. Krypteringens historia är rik som vi har sätt i genomgången i kapitel 2, och en naturlig ämnespartner till matematiken skulle kunna vara historieämnet, men också samhällsvetenskapen. Precis som Wedman (2005) beskrev så lärde sig eleverna om matematik, men också om andra världskrigets historia i arbetet om Enigma, vilket skulle kunna fungera som ett projekt mellan elever och lärare i matematik, historia och samhällsvetenskap (Wedman 2005, s. 1).

Som vi också har sett i vid genomgång av krypteringens historia, har matematiken men också lingvistiken (språkvetenskap) haft en betydande roll för kryptografins utveckling. Ytterligare ett exempel på ämnesintegrering är användningen av frekvensanalysen som beskrivs i avsnitt 2.3 som kan fungera som en bro mellan språkämnena (svenska men också andra språk) och matematiken. I Matematik 1A, den först gymnasiekursen, ska procentbegreppet behandlas men även sannolikhetslära och statistik är en del av kursen. Här skulle eleverna i samarbete med språkämnena kunna arbeta med dekryptering och frekvensanalys. Eleverna kan till exempel tilldelas en kryptotext och därefter sammanställa hur frekventa bokstäverna är och jämföra med bokstavsfrekvensen för svenska språket (eller annat valt språk) för att kunna dekryptera meddelandet. Vid dekryptering kommer även sannolikhetslära och grammatik in i bilden då eleverna använder sig av dekrypteringsknep som att granska bland annat dubbelstavningar. Ett sådant här projekt skulle kunna göra matematiken mer attraktiv för elever som är intresserade av språk (Purdue university 2006).

Ceasarrullningssystemet skulle fungera vid flera områden i matematikundervisningen. Systemet skulle kunna fungera som introduktion och som praktisk tillämpning av modulär aritmetik i kursen Matematik 5. Dekryptering av Caesarrullningen skulle även kunna lära eleverna hur man hittar inversen till en funktion:

Krypteringsfunktionen för Ceasarrullning $f(x)$= (x+k)mod26

1. Byt ut $f(x)$ mot y
   y = (x+k) mod26
2. byt plats på x och y
   x = (y+k) mod 26
3. lös ekvationen för y
   y = (x-k)mod 26

Dekrypteringsfunktionen för Ceasarrullning $f^{1}(x)$ = (x-k)mod 26

Ceasarrullningen ger eleverna möjlighet att använda både funktionen och dess invers på ett användbart och roligt sätt (Castaneda 2009, s. 16). En fråga man kan ställa eleverna i kombinatorikundervisningen är hur många olika förskjutningar eller nycklar det finns i Ceasarrullningen. I Matematik 1B ska eleverna dessutom för första gången arbeta med formler, algebraiska uttryck och därtill begreppet funktion. Även här skulle Ceasarrullningen och formeln C = K + F (C för chiffertext, K för klartext och F för förskjutning) kunna användas för att belysa för eleverna hur en formel fungerar, eller ännu bättre att de själva får komma fram till hur uttrycket ska formuleras. Med hjälp av algebra kan eleverna dessutom dekryptera meddelanden genom att subtrahera förskjutningsvärdet från båda led (K + F - F = C – F) (Cryptosmith 2013). RSA-krypteringen kan fungera som en praktisk tillämpning som kopplar samman de olika grenarna i gymnasiets talteori då systemet berör områden som primtal, binära tal, kongruensräkning och Euklides algoritm (dock behandlar gymnasiet inte Eulers φ-funktion) (Wedman 2005, s. 4).

Utöver matematikens produkter, dess begrepp, lagar och modeller förespråkar även Skolverket (2011) i ämnesplanen för matematik att eleverna efter slutförd gymnasieutbildning ska kunna relaterat till matematikens betydelse för individen och dagens samhälle. Eleverna använder dagligen mobiltelefonen och datorn för att kommunicera och konsumera via en allt mer växande digital marknad. För att inte elevernas privatliv och ekonomiska transaktioner vid handel ska hotas finns krypteringen tillhands. När det här arbetet skrivs 2014 är det valår, och många av gymnasieeleverna är gamla nog för att kunna ta ställning och rösta. Krypteringssystemen har idag blivit så säkra att rättsväsendet inte längre kan använda sig av avlyssning som metod för brottsbekämpning (Singh 2003, s. 11). En het debatt pågår just nu kring vad politiken ska

prioritera, där polisens arbete att bekämpa kriminell verksamhet ställs mot medborgarnas rätt till att slippa insyn i deras privatliv. RSA-systemet kan tas upp i undervisningen för att visa på matematiken som en del av samhället. Detta kan bli en diskussion som går bortom det matematiklärarna lärt sig under sin utbildning, men här kan återigen ämnesintegration fungera på ett bra sätt mellan historia, samhällsvetenskap och matematik.

I ämnesplanen för Matematik 5 finner vi även under rubriken ”Centralt innehåll” att eleven ska fått kunskap om ”Matematikens möjligheter och begränsningar” (Skolverket 2011). Klembalski (u.å) menar att RSA-kryptering och en fråga som *finns det något effektivt sätt att finna primtalskomponenterna för stora tal?* kan visa eleverna i klassrummet på att vetenskapen matematik har saker kvar att lösa och upptäcka. Matematiken är inget projekt som redan är absolut färdigställt. Klembalski (u.å) menar vidare att kryptering motiverar många elever i hög grad då många associerar det med hemligheter, spioneri och att knäcka koder, vilket de finner spännande. Listan kan göras lång över mjöliga tillämpningar av kryptering i skolansundervingen, speciellt då arbete med historiska inslag och digitala verktyg nu förespråkas och lyfts upp som en viktig del i Skolverkets (2001) ämnesplan för matematik.

4 Slutsats

RSA är än idag den bästa krypteringsmetoden vi känner till och används till exempel av program som PGP (Pretty Good Privacy) vilket säkrar e-post kommunikation (Järpe 2003, s. 167). Om två tillräckligt stora primtal väljs ut sägs RSA dessutom vara omöjligt att knäcka. Har vi nu alltså nått fram till absolut sekretess? Har kodmakarna tillslut vunnit över kodknäckarna? Att försöka förutspå framtiden är såklart en svår uppgift, men är det något vi har lärt oss av att gå tillbaka i tiden och granska kryptots historia så är det att kryptoanalytikerna alltid har funnit genvägar och svagheter i de olika krypteringssystem som figurerat. Substitutionskryptot och Enigmamaskinen ansågs både osårbara innan de föll för den tidens briljanta forcörer. Vignerekryptot som nämns kort i texten kallades under sin tid *Le chiffre indechiffrable* vilket betyder *det oknäckbara kryptot*, vilket kryptoanalytikern Charles Babbage senare skulle motbevisa (Singh 1999, s. 349). Ett av de största hoten mot dagens krypteringssystem som hägrar i horisonten är en extrem kraftfull typ av dator som bygger på den moderna fysikens kvantteori, därav namnet kvantdator. Nationella säkerhetsmyndigheten (NASA) och företaget Google påstår att de redan idag har tillgång till en kvantdator vid namn D-Wave System, men forskarvärlden ställer sig mycket skeptisk till detta, och menar att tekniken är tiotals år bort från att kunna färdigställas (Sverigesradio 2013). Ingen vet emellertid helt säkert, kryptografin är en vetenskap höljt i dunkel där många av dess pionjärer är belagda med tystnadsplikt. Ett exempel på detta är RSA-systemet, som är uppkallat efter de tre männen Rivest, Shamir och Adleman. Dessa ansågs under många år vara de första som utvecklat RSA, men man skulle senare få skriva om historieböckerna då de brittiska matematikerna James Ellis, Clifford Cocks och Malcom Williamson efter 30 års tystnadsplikt kunde gå ut med att de tre år innan Rivest, Shamir och Adleman tagit fram RSA-metoden (Singh 1999, s. 318). Så vem vet, kanske har NASA eller någon annan topphemlig organisation redan idag utvecklat en kvantdator eller en annan typ av metod för att dekryptera RSA på ett snabbt och smidigt sätt. Hur som helst är det en diskussion som skulle kunna tas upp i klassrummet vid arbetet med primtal för att visa på att matematiken fortfarande har saker kvar att upptäcka, och för att ge eleverna förståelse i vad en matematiker kan tänkas arbeta med.

För att koppla krypteringen till skolan så innehåller gymnasiekursen Matematik 5 moment som bland annat kongruensräkning (modulär aritmetik) och kombinatorik (permutationer och kombinationer) (Skolverket 2014). Detta är alla verktyg som kan

används för att förstå och knäcka de krypteringssystem som tagits upp i denna text. Genom att använda konkreta exempel på hur matematik kan implementeras tror jag som författare till denna text att man kan öka motivationen hos både elever och lärare, och det leder förhoppningsvis till förbättrad prestation hos båda parter.

Avslutningsvis finns det ett behov av att diskutera hur man kan gå vidare och utveckla studierna på detta område. Vid litteraturgenomgången framgick det tidigt att det finns väldigt liter material om hur implementering av kryptering fungerar i matematikens skolundervisning. Här önskar jag att det kunde göras vidare studier om kryptering som matematikundervisning, då Wedmans (2005) projekt blivit så uppskattat. Det finns även stort utrymme för att göra liknande studier på andra områden som kan fungera för att illustrera matematikens kulturhistoria och öka ämnesintegrationen.

Referenser

Litterära källor:

Ekstig, Kerstin & Vretblad, Anders (2010). *Algebra och geometri,* Malmö: Gleerups

Järpe, Eric (2013). *Räkna med rester – Matematik att tillämpas inom kryptologi*, Lund: Studentlitteratur

Khan, David (1973). *The codebreakers- the story of secret writing*, New York: The new American library

Liedman, Sven-Eric (2002). *Ett oändligt äventyr – om människans kunskaper,* Stockholm: Alber Bonniers Förlag AB

Silverman, Joseph H (2014). *A Friendly Introduction to Number Theory,* Edinburgh: Pearson Education Limited

Singh, Simon (1999). *Kodboken- Konsten att skapa sekretess – från det gamla Egypten till kvantkryptering,* Stockholm: Nordstedts Förlag

Singh, Simon (2003). *Kodboken- Konsten att skapa sekretess – från det gamla Egypten till kvantkryptering,* Stockholm: Pan

Sjöberg, Svein (2010). *Naturvetenskap som allmänbildning – en kritisk ämnesdidaktik,* Lund: Studentlitteratur.

Wobst, Reinhard (2007). *Cryptology unlocked*, Chichester: John Wiley & Sons Ltd

Elektroniska källor:

Björner, Anders (u.å). *Kryptografi och primalitet*. Hämtad 2014-08-20, från http://www.math.kth.se/~boij/5B1118/Material/Krypto.pdf

Castaneda, Rigoberto G (2009). *Using classical ciphers in secondary mathematics.* Hämtad 2014-08-20, från http://www.mcm.edu/mathdept/rigoberto_castaneda/thesis.pdf

Computer science uc santa barbara (2014). *Diffie-Hellman Key Exchange.* Hämtad 2014-08-20, från http://cs.ucsb.edu/~koc/ns/docs/slides/08-dh.pdf

Cryptosmith (2013). Grade school crypto. . Hämtad 2014-08-20, från https://www.youtube.com/watch?v=GpQeOT0Mqys

Ekhall, Stig-Arne (2013). *Nämnarens kryptoskola.* Hämtad 2014-08-20, från http://ncm.gu.se/media/namnaren/kryptoskola/01_krypto_introduktion.pdf

Ellis, Claire (2005). *Exploring the Enigma*. Hämtad 2014-08-20, från http://plus.maths.org/content/exploring-enigma

För det vidare (2012). *Tema lärarrollen – Varför arbeta ämnesövergripande.* Hämtad 2014-08-20, från http://fordetvidare.se/carlmikael/2012/04/varfor-arbeta-amnesovergripande/

Gilman, Larry (u.å). *Enigma*. Hämtad 2014-08-20, från http://www.faqs.org/espionage/Ec-Ep/Enigma.html

Klembalski, Katharina (u.å). *Cryptography and number theory in the classroom -- Contribution of cryptography to mathematics teaching.* Hämtad 2014-08-20, från http://math.unipa.it/~grim/21_project/klembalski323-327.pdf

Lycett, Andrew (2014). *Enigma*. Hämtad 2014-08-20, från http://www.bbc.co.uk/history/topics/enigma

Math insight (u.å). *Basic rules for exponentiation*. Hämtad 2014-08-20, från http://mathinsight.org/exponentiation_basic_rules

Maxey, Megan (2012). *A modern day application of Euler's theorem: The RSA cryptosystem.* Hämtad 2014-08-20, från http://math.gcsu.edu/~ryan/12capstone/papers/maxey.pdf

Nationalencyklopedin (2014). *Arabien*, Hämtad 2014-08-20, från http://www.ne.se.ezproxy.ub.gu.se/arabien/historia

Nationalencyklopedin (2014). *Herodotos*, Hämtad 2014-08-20, från http://www.ne.se.ezproxy.ub.gu.se/lang/herodotos

Nationalencyklopedin (2014). *Internet.* Hämtad 2014-08-20, från http://www.ne.se.ezproxy.ub.gu.se/lang/internet

Nationalencyklopedin (2014). *Kalla kriget.* Hämtad 2014-08-20, från http://www.ne.se.ezproxy.ub.gu.se/lang/kalla-kriget

Nationalencyklopedin (2014). *Persien.* Hämtad 2014-08-20, från http://www.ne.se.ezproxy.ub.gu.se/lang/persien

Nationalencyklopedin (2014). *Vaxtavla.* Hämtad 2014-08-20, från http://www.ne.se.ezproxy.ub.gu.se/sve/vaxtavla?i_h_word=vaxtavla

Numberphile (2013). *158,962, 555, 217, 826,360, 000.* Hämtad 2014-08-20, från https://www.youtube.com/watch?v=G2_Q9FoD-oQ

Numberphile (2012). *Encryption and huge numbers.* Hämtad 2014-08-20, från https://www.youtube.com/watch?v=M7kEpw1tn50

Perimeter institute for theoretical physics (2014). *The inner workings of an Enigma machine.* Hämtad 2014-08-20, från https://www.youtube.com/watch?v=mcX7iO_XCFA

Purdue university (2006). *Caesar cipher: an introduction to cryptography*. Hämtad 2014-08-20, från http://www.purdue.edu/discoverypark/gk12/downloads/Cryptography.pdf

Regeringskansliet (2010). *Nya läroplanen sätter tydliga mål för lärare och elever*. Hämtad 2014-08-20, från http://www.regeringen.se/sb/d/12466/a/153375

Scrabbleförbundet (2011). *Ordlistor*. Hämtad 2014-08-20, från http://www.scrabbleforbundet.se/index.php?option=content&task=view&id=18&Itemid=41

Skolverket (2011). *Läroplan, examensmål och gymnasiegemensamma ämnen för gymnasieskola 2011*. Hämtad 2014-08-20, från http://www.skolverket.se/om-skolverket/publikationer/visa-enskild-publikation?_xurl_=http%3A%2F%2Fwww5.skolverket.se%2Fwtpub%2Fws%2Fskolbok%2Fwpubext%2Ftrycksak%2FRecord%3Fk%3D2705

SO-rummet (2014). *Andra världskriget*. Hämtad 2014-08-20, från http://www.so-rummet.se/kategorier/historia/det-korta-1900-talet/andra-varldskriget

Stanford University (u.å). *Some mathematics of the Enigma*. Hämtad 2014-08-20, från https://ccnet.stanford.edu/cgi-bin/course.cgi?cc=ee45&action=handout_download&handout_id=ID111463895719768

Sveriges radio (2013). *Chalmers orolig för att kvantdator är bluff*. Hämtad 2014-08-20, från http://sverigesradio.se/sida/artikel.aspx?programid=104&artikel=5602093

Thorbiörnson, Johan (2003). *Något om RSA-algoritmen*. Hämtad 2014-08-20, från http://www.math.kth.se/~johantor/foredrag/lusttur/ht03/rsa/index.html

Universetoday (2009). *Atoms in the universe*. Hämtad 2014-08-20, från http://www.universetoday.com/36302/atoms-in-the-universe/

Wedman, Lotta (2005). *Kryptering på gymnasiet*. Hämtad 2014-08-20, från http://ncm.gu.se/pdf/namnaren/4043_05_2.pdf