Chinese Remainder Theorem

Khalil Chemali

Examensarbete för 10 p, Institutionen för datavetenskap,
Naturvetenskapliga fakulteten, Lunds universitet

Thesis for a diploma in computer science, 10 credit points, Department of Computer Science,
Faculty of Science, Lund University

Kinesisk Rest Teorem.

Sammanfattning

Kinesisk rest teorem används för att lösa problem inom områdena räkning, kodning och kryptering. Räkning innebär att man kan räkna med mindre tal istället för stora tal och detta gör räkningsprocessen enklare och snabbare. Inom kodning använder man sig av felsökning och –rättning. Kryptering innebär att man kan skicka krypterade meddelanden som ingen kan knäcka eller läsa utom den som har dekrypteringsnyckeln som baseras på primtal.

Jag skriver om matematikens historia och hur man använde tal- och bråktal -system i Babylon, Egypten, Grekland och i Kina.

Kryptering var ett intressant ämne för tusen år sedan och det är på sin topp just nu. Det finns hemligheter som är krypterade och som ingen hittills har kunnat dekryptera. Ett meddelande kodat med en publik nyckel, som är baserad på kinesisk rest teorem, är omöjligt att lösa utan den privata nyckeln.

Det har sagts att första världskriget var ett kemisternas krig. Då användes senapsgas och klorgas för första gången. Andra världskriget skulle ha varit ett fysikernas krig, eftersom det var då som atombomben sprängdes. I analogi därmed har det hävdats att ett tredje världskrig skulle bli ett matematikernas krig, eftersom de behärskar det nya, avgörande vapen som heter information.

Chinese Remainder Theorem

Abstract

Chinese Remainder Theorem is used to solving problems in computing, coding and cryptography. In computing we can compute with shorter numbers instead of large numbers and this will make the computing-process faster and easier. In coding it can be used for error-searching and error-regulating.

Cryptography means that we can send a coded message and that no one will be able to read it without the decode-key which is based on prim-numbers. I am writing about the history of mathematics and how the number- and decimal number-system is used in Babylon, Egypt, Greece and in China.

Writing in cipher code was a very interesting subject a thousand years ago and it is still used even in modern time. To this day there are still some secrets, written in cipher code, that no one has been able to decode yet.

A message which is coded with a public key, which is based on Chinese Remainder Theorem, is virtually impossible to solve without the private key which is based on prime numbers. If the First World War was the chemists war (chlorine gas used) and if the Second World War was the physicist war (atomic bombs used), that would suggest that the Third World War will be the mathematicians's war, because they master the new weapon which is called information.

Innehållsförteckning

1. Inledning

I inledningen kommer jag att kort redogöra för uppsatsens disposition och syfte, gå igenom lite matematisk historik och bakgrunden till Chinese Remainder Theorem samt beskriva ett teorem och bevisa det ur olika perspektiv. Jag kommer att nämna lite kryptering historia.

1.1 Disposition

Uppsatsen börjar med en inledning där syfte anges, matematikens historia från olika delar av världen beskrivs och historiken angående CRT berättas. Även ett teorem beskrivs och bekräftas med bevis från olika perspektiv. Jag kommer också att gå igenom hur CRT kan användas inom områdena räkningen, kodning och kryptografi. Jag kommer sedan att analysera det material jag hittat och sammanfatta uppsatsen.

1.2 Syfte

Jag vill undersöka hur användbart kinesisk rest tiorem var när man skulle lista ut gamla matematiska problem och hur man även kan lösa modernare problem inom områdena räkningen, kodning och kryptografi

1.3 Historik

1.3.1 Matematik i Babylonien

Det sexagesimala talsystemet

Det nya sättet att skriva tal hade sina rötter i de äldre talsymbolerna. Tal grupperades i större enheter om 60. På motsvarande sätt som det tidigare också förekom talsymboler för 10, mellan 1 och 60, gjordes i kilskriften också en "mellangruppering i 10-tal". Talen 1, 2, ...,9 skrevs:

För talen 10, 20, 30, 40, 50 skrev man sneda kilar:

För talen 10, 11, 12, 13 ... satte man samman symbolerna för tiotal och ental:

Talen 60, 61, 62, ... grupperas 60, 60+1,60+2... och skrivs (undantaget 60) med två "siffror". Till höger där om följer 70 =60+10 och 71 =60+11:

"Siffrans" värde bestäms av dess placering. Slutsiffrorna gäller för tal från 1 till 59, andra siffran från höger avser tal från 1*60 till 59*60, tredje siffran från höger avser tal från $1*60^2$ till $59*60^2$. Talet 10000 skulle alltså i denna tolkning skrivas
2*3600 + 46*60 + 40 dvs:

Talet 60 kan inte skiljas från talet 1 eftersom det inte finns någon nolla. Inuti talen lämnas en bredare lucka där vi skulle ha satt ut siffran noll.
Situationen kompliceras ytterligare av att siffrorna även kan stå för bråktal.

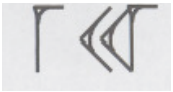
Bråktal

Bråk skrevs med positionssystem. I det babyloniska skrivsättet fanns inget "kommatecken" som markerade var gränsen går mellan enheter och bråkdelar. Siffran 1 kunde betyda 3600, 60, l, 1/60, 1/3600 ... och vad som är vad måste tolkas utifrån sammanhanget.

Nedanstående tecken:

kan betyda 30 men också 30*60 = 1800, vidare kan 30*(1/60) = 0,5 osv.

På samma sätt kan tecknen:



betyda 1*60+21 = 81 men också 1*60*60+21*60 = 4860 eller 1+21*(1/60) = 1,35.

Räknesätt

Addition och subtraktion utfördes lika enkelt då som nu. Uträkningarna skrevs inte ner och var inte heller beroende av tabeller, utan utfördes möjligen som huvudräkning.
För multiplikation av flersiffriga tal behöver man en multiplikationstabell tillgänglig upp till och med 50*50 för att det är en stor mängd för minnet. Många sådana multiplikationstabeller finns bevarade från äldre babylonisk tid, de flesta från städerna Nippur och Kish.

En multiplikationstabell bestod av talen 1, 2, 3, 17, 18, 19, 20, 30, 40, 50 samt produkterna av dessa tal med ett visst givet tal, K. Troligen beräknades exempelvis 29*K genom att slå upp 20*K och 9*K i multiplikationstabellen för K och sedan addera svaren. Tabellen för multiplikation med 15 ser ut enligt följande tabell:

Multiplikationstabell för talet 15

1	15
2	30
3	45
4	1
5	1 15
6	1 30
...	...
19	4 45
20	5
30	7 30
40	10
50	12 30

För division finns en enda tabell, som för talet n ger det inverterade talet l/n. I denna tabell ingår bara sådana tal n, där det inverterade talet, l/n, kan skrivas exakt med ändligt många (sexagesimala) siffror. Det betyder att 60 eller 60.60eller 60.60.60 osv, ska vara jämnt delbart med talet n, vilket inträffar precis då talet n inte innehåller andra faktorer än 2, 3 och 5.

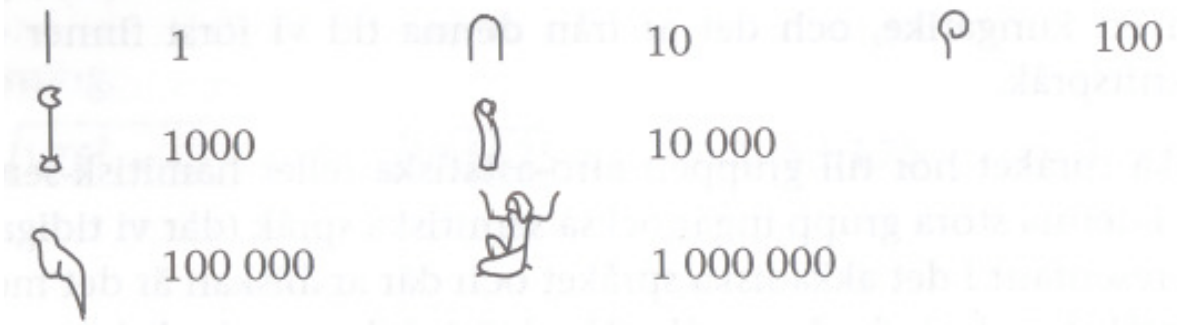
Följaktligen får man följande tabell över tal och deras inverterade värden:

n	1/n	n	1/n	n	1/n
2	30	16	3 45	45	1 20
3	20	18	3 20	48	1 15
4	15	20	3	50	1 12
5	12	24	2 30	54	1 06 40
6	10	25	2 24	1	1
8	7 30	27	2 13 20	1 4	56 15
9	6 40	30	2	1 12	50
10	6	32	1 52 30	1 15	48
12	5	36	1 40	1 20	45
15	4	40	1 30	1 21	44 26 40

Exempel:
2*30=60 men tabellen ska tolkas 2*(30/60) =1.

1.3.2 Matematik i Egypten

Den äldsta formen av egyptisk skrift är hieroglyfskriften. Denna är en bildskrift och man kan säga att den arbetar med "ikoner". Tecknen kunde skrivas lodrätt (uppifrån och ner) eller vågrätt (från vänster eller från höger, tecken som föreställer djur eller människor har ansiktena vända mot det håll man skriver från). I hieroglyfskrift skrevs tal med ett decimalt system, genom att man använde en symbol för ental, som upprepades tillräckligt många gånger (upp till nio), en symbol för tiotal, en för hundratal och så vidare.



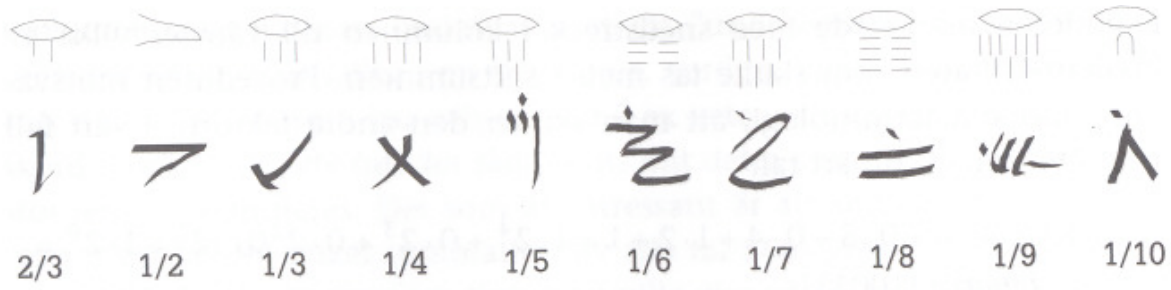
Talen skrevs med de större enheterna först. 1982 skulle alltså skrivas (från vänster till höger):

Det finns handstil som skiljer sig från originalen.
Denna text är nedtecknad under 1600-talet f.Kr. Vid denna tidpunkten hade talsymbolerna nedanstående utformning:

För att beteckna talet åtta förenklas åttan till två horisontella streck.
Det hieratiska skrivsättet gav alltså ett tecken för varje ental, ett tecken för varje tiotal och ett tecken för varje hundratal. Totalt tjugosju tecken användes för att skriva talen från ett till 999.

Bråktal

Egyptier införde ett system att uttrycka bråk i exakt form. Det fanns således beteckningar för 1/2, 1/3, 1/4, l/5 ... Dessutom fanns en särskild symbol för 2/3. I hieroglyfskrift betecknades bråken med motsvarande heltalstecken samt symbolen ⬭ ovanför. För 1/2 och 2/3 fanns särskilda tecken.



Man kan visa att alla positiva bråk kan skrivas som en summa av olika bråk med täljaren l, s.k. "enhetsbråk" eller "stambråk".

Exempel. $\frac{2}{35} = \frac{1}{18} + \frac{1}{630} = \frac{1}{20} + \frac{1}{140} = \frac{1}{21} + \frac{1}{105} = \frac{1}{30} + \frac{1}{42}$

De egyptiska matematikerna använde sig dock av enhetliga metoder genom mer än tusen år, så de uppdelningar vi möter är oftast de samma genom tiderna.

Vid addition av två lika stambråk, t.ex. 1/7 + 1/7 måste summan skrivas som en summa av enhetsbråk. I detta fall skrev man 1/4 +1/28 istället för 2/7.

Multiplikation av ett bråk med ett heltal, t.ex. 2 3/8 med 7, uttryckt i enhetsbråk: (2 1/4 1/8). 7 beräknas genom de successiva fördubblingarna i nedanstående tabell. Summan av termerna blir 16 1/2 1/8 (vilket vi i dag skriver 16 5/8).

$2\ \frac{1}{4}\ \frac{1}{8}$	1 /
$4\ \frac{1}{2}\ \frac{1}{4}$	2 /
$9\ \frac{1}{2}$	4 /

Tabell över bråken 2/n

Tabellen som ger resultatet när man fördubblar bråken l/n. De bråk, där nämnaren är ett jämnt heltal finns inte med i tabellen, eftersom de fördubblas enkelt genom att man halverar nämnaren. Inte heller finns 1/3 med bland de bråk som fördubblas, eftersom talet 2/3 har en särskild symbol.

Denna tabellen innehåller fördubblingar av bråken l/n för alla n upp till och med 101.

Om n =5 ger detta att fördubblingar av bråken l/n = 2/5.

2/5 är en summa av två enhetsbråk 1/3+1/15 som vi kan se på tabellen:

Tabell över 2 / n

n	$2\cdot(1/n)$	n	$2\cdot(1/n)$
5	1/3 1/15	53	1/30 1/318 1/795
7	1/4 1/28	55	1/30 1/330
9	1/6 1/18	57	1/38 1/114
11	1/6 1/66	59	1/36 1/236 1/531
13	1/8 1/52 1/104	61	1/40 1/244 1/488 1/610
15	1/10 1/30	63	1/42 1/126
17	1/12 1/51 1/68	65	1/39 1/195
19	1/12 1/76 1/114	67	1/40 1/335 1/536
21	1/14 1/42	69	1/46 1/138
23	1/12 1/276	71	1/40 1/568 1/710
25	1/15 1/75	73	1/60 1/219 1/292 1/365
27	1/18 1/54	75	1/50 1/150
29	1/24 1/58 1/174 1/232	77	1/44 1/308
31	1/20 1/124 1/155	79	1/60 1/237 1/316 1/790
33	1/22 1/66	81	1/54 1/162
35	1/30 1/42	83	1/60 1/332 1/415 1/498
37	1/24 1/111 1/296	85	1/51 1/255
39	1/26 1/78	87	1/58 1/174
41	1/24 1/246 1/328	89	1/60 1/356 1/534 1/890
43	1/42 1/86 1/129 1/301	91	1/70 1/130
45	1/30 1/90	93	1/62 1/186
47	1/30 1/141 1/470	95	1/60 1/380 1/570
49	1/28 1/196	97	1/56 1/679 1/776
51	1/34 1/102	99	1/66 1/198
		101	1/101 1/202 1/303 1/606

<u>Räknesätt</u>

Addition och subtraktion av heltal kan utföras mycket enkelt på abakus (som jag kommer att förklara lite senare). Hur långt tillbaka i tiden den användes vet vi inte. Gillings (1972) anser det möjligt att det kan ha funnits tabeller för addition och subtraktion.

Multiplikation av två heltal genomfördes med hjälp av upprepade fördubblingar.

Man kunde också föra in multiplikation med l0, eftersom den går att utföra enkelt i språk där talen beskrivs med 10 som bas; ental byts mot tiotal, tiotal mot hundratal osv.

Exempel:

7	*hus*		
49	*katter*	2801	1
343	*möss*	5602	2
2401	*emmervete*	11204	4
16807	*hekat*	19607	*Totalt*
19607	*Totalt*		

Problemet kan närmast beskrivas som ett "underhållningsproblem" där man redovisar innehållet i en by: 7 hus, vardera med 7 katter, för varje katt finns 7 möss, som var och en äter 7 emmervete, och varje emmervete skulle ge en skörd om 7 hekat vete om det såddes ut. Allt detta summeras. Det som är intressant är att slutsumman inte beräknas genom en enkel addition av alla tal utan genom multiplikationen 2801* 7. Det är som om skrivaren ville visa på en princip att beräkna summan:

Summan av n antal termer = 7*(1 + summan av de (n-l) första termerna)
Själva multiplikationen beräknas sedan genom en serie fördubblingar av 2801, vilket ger 2801*1, 2801*2 och 2801*4. Eftersom 7 = 1+ 2 + 4 blir 2801*7 = 2801 +2801*2 + 2801*4, produkten erhålls genom summering. Hekat var en volymenhet som användes för korn eller mjöl. En hekat motsvarade cirka 4,9 liter.

Hur multiplikationen 27.19 skulle kunna utföras enligt metoden med successiv fördubbling:

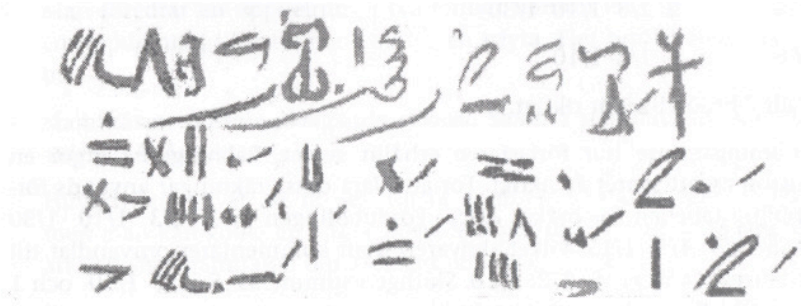
/1	27	
/2	54	
4	108	
8	216	
/16	432	
Summa: 19	513	

alternativt

/1	27
2	54
4	108
/8	216
/10	270
Summa: 19	513

Egyptierna markerade med snedstreck i kolumnen till vänster vilka av mellanresultaten som skulle tas med i slutsumman. Man skriver talet 19 som ett binärt tal:
19 = 1*16 + 0*8 + 0*4 + 1*2 + 1 = 1*24 + 0*23 + 0*2201*21 + 1* 2° =
= (binärt) [10011] och beräknar produkten genom successiva fördubblingar, där man summerar de resultat, som svarar mot en etta i den binära utvecklingen.
Division kan behandlas som multiplikation: Att utföra divisionen 513/27 innebär att man ska beräkna vad 27 ska multipliceras med för att vi ska få resultatet 513. Följaktligen får vi exakt samma uppställning som i tabellen ovan. När divisionen inte går jämnt ut med heltal, använder vi bråktal.

Ekvationsproblem



2 1/4 1/8 1 / 2 1/4 / 8 1 7 1 /
4 1/2 ¼ 2 / 1 1/8 / 16 2 /
9 ½ 4 / 4 ½ 1 1/7 /

En storhet och dess 1/7 *blir tillsammans* 19. *Vilken är storheten?*

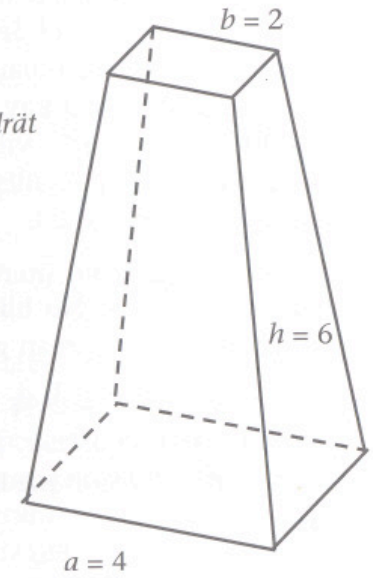
I modernt språk skulle problemet lyda: Lös ekvationen $x + x/7 = 19$.

Geometri

De längdmått som användes hade en *aln* som grundmått (cirka 52 cm), som indelades i 7 händer. En hand delades in i 4 fingrar. Längdmåttet över aln i storlek hette *khet* och innehöll 100 alnar. För areor användes 1 aln x 100 alnar som grundmått, vilket också kallades aln. 100 sådana alnar motsvarade då en kvadrat med sidan en khet. Tio sådana områden bildade "ett tusental".

Volymer slutligen, baserades på måttet hekat, som motsvarade cirka 4,9 liter. 20 hekat motsvarade en khar, en säck, alltså cirka 98 liter. Volymen av en kub med sidan 1 aln omvandlas till khar genom multiplikation med l,5. För stora volymer användes ett mått, "100-kvadrupelhekat", som omfattade 400 hekat, dvs. 20 khar, cirka 2 m^3.

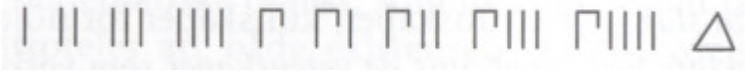
Exempel att beräkna en avhuggen pyramid.
Om du har en avhuggen pyramid med lodrät höjd 6 *alnar,*
med basen 4 *alnar och med* 2 *på översidan.*
Räkna med dessa 4 *kvadrerade. Det blir* 16.
Fördubbla 4. *Det blir* 8.
Räkna med dessa 2 *kvadrerade. Det blir* 4.
Addera dessa 16 *och dessa* 8 *och dessa* 4.
Det blir 28.
Beräkna 1/3 *av* 6. *Det blir* 2.
Räkna med 28 2 *gånger. Det blir* 56.
Se, det är 56. *Du har funnit det riktigt.*



Beräkningarna motsvarar den nutida formeln $V = (a^2 + ab + b^2) \cdot \frac{h}{3}$.

1.3.3 Matematik i Grekland

Grekernas äldsta talsystem liknar det romerska, de s.k. Herodianska siffrorna. Mängder grupperades i enheter om fem och tio, så tal från ett till tio skrevs:



Det Herodianska systemet innebär att det kan bli omständligt och utrymmeskrävande att skriva ner tal. Addition och subtraktion utfördes på abakus. Man kan markera ental och femtal i samma kolumn och alltså räkna som på en modern abakus. Multiplikation och division utfördes också med abakus. Beräkningar, utförda genom att skriva ner talsymbolerna, blir däremot ohanterliga, men det har knappast funnits behov av sådana. Grekerna utvecklade tidigt ett eget, betydligt smidigare sätt att skriva tal: de använde alfabetets tecken. Med bruket av präglade mynt kom de i officiellt bruk och genom att bara ett par tre tecken behövs för årtalen blir de mycket enklare än de Herodianska symbolerna i de sammanhangen, eftersom de lättare ryms på myntet.

Bokstäverna har följande värden:

1	Α α	10	Ι ι	100	Ρ ρ
2	Β β	20	Κ κ	200	Σ σ
3	Γ γ	30	Λ λ	300	Τ τ
4	Δ δ	40	Μ μ	400	Υ υ
5	Ε ε	50	Ν ν	500	Φ φ
6	Ϝ ϛ	60	Ξ ξ	600	Χ χ
7	Ζ ζ	70	Ο ο	700	Ψ ψ
8	Η η	80	Π π	800	Ω ω
9	Θ θ	90	Ϟ ϙ	900	Ϡ ϡ

Man kan uttrycka tal från 1 till 999 med högst tre tecken, men till skillnad från dagens skrivsätt är detta inget positionssystem $\delta\xi\omega$ betecknar samma tal som $\omega\xi\delta$, nämligen 864; symbolen ω betecknar i båda skrivsätten talet 800 oberoende av placeringen. Grekerna valde att använda alfabetets tecken istället för att hitta på nya. Man kunde beteckna tal upp till 999. För tusental och högre krävdes nya symboler eller skrivsätt men för tusental använde de på nytt symbolerna för talen 1-10 med en apostrof upptill eller nertill till vänster:

$\acute{\alpha}$ $\acute{\beta}$ $\acute{\gamma}$ $\acute{\delta}$ $\acute{\varepsilon}$ $\acute{\varsigma}$ $\acute{\zeta}$ $\acute{\eta}$ $\acute{\theta}$ eller $,\alpha$ $,\beta$ osv.

För att skilja tal från text, strök man ett streck över symbolerna

$\overline{\mu\beta}$ $\overline{\tau\varepsilon}$ $\overline{,\beta\rho\kappa\alpha}$

Användningen av alfabetet till att beteckna tal har till följd att ord får talvärden genom att man summerar de bokstäver som ingår i ordet. Odjurets tal, 666, som nämns i Uppenbarelseboken är ett känt ord.

Rationella tal

Vad bråktal beträffar, finner man i grekisk matematik flera olika metoder i användning. Från Egypten övertog grekerna principen att framställa bråk som summor av enhetsbråk, bråk med täljaren 1, exempelvis 1/2, 1/3, 1/4 osv. För 1/2 fanns dessutom en särskild symbol,  , och ibland skrevs 2/3 med  Detta skrivsätt fanns redan i t.ex. Arkimedes' texter, men Arkimedes skrev också bråk med godtyckliga heltal i täljaren och han skrev då först täljare sedan nämnaren med accent. Exempelvis i ett manuskript där Arkimedes beräknar π skriver han  för $10/71$.

Inom astronomiska beräkningar tog istället den babyloniska traditionen över. Det finns värden där bråkdelar skrivs med det sexagesimala systemet för att göra noggranna beräkningar. När vi i dag mäter tid och vinklar i timmar/grader, minuter, sekunder och sedan 10-delar, 100-delar osv. av en sekund har vi alltså gjort en "återkorsning" av sexagesimala system med det decimala systemet.
Slutligen kan man nämna att symbolen för noll dyker upp redan i papyrusfragment från århundradena e.Kr. som nu finns i Lund, visar tecknet  (Neugebauer 1969). I bysantinska manuskript ser man senare symbolen o, som till formen är lik en modern nolla. Den första symbolen för noll är dock en äldre symbol än så, den visar sig i kilskrifttexter från 300-talet f.Kr.

Aristoteles logik

Sex av Aristoteles bevarade arbeten behandlar logik och vetenskapsteori:
Kategorierna, De Interpretatione (Peri hermeneias), Första analytiken, Andra analytiken, Topiken och Sofistiska vederläggningar (Sophistici elenchi). Dessa arbeten sammanfattades under namnet Organon, "redskapet". Även senare var Aristoteles mycket inflytelserik och man finner spår av hans logik ända in i 1900-talet. En utredning "i vilken man gör påståenden, där det med nödvändighet följer någonting annat än vad som sägs i påståendena", kallar Aristoteles en syllogism. Det handlar alltså om vad vi skulle kalla en logisk slutledning, där man logiskt visar något nytt.

De satser som han behandlar är sådana som innehåller ett subjekt B och ett predikat A, som säger att någonting, A, är en egenskap hos, eller är närvarande hos något annat, B. De termer, A, B, ... som Aristoteles använder kan förekomma både som subjekt och som predikat; vi kan alltså möta både satsen "några B är A" och satsen "några A är B". En första indelning av satserna är:

universella	*alla B är A*	*inga B är A*
partikulära	*något B är A*	*inte alla B är A*
obestämda	(om det inte framgår huruvida de är universella eller partikulära)	

Vidare kan satserna vara affirmativa, bekräfta något om något, eller negativa, förneka något om något. Vi får följande fyra huvudtyper av satser

(a) *Alla B är A*
(e) *Inga B är A*
(i) *Några B är A*
(o) *Några B är inte A*

Aristoteles' syllogismer innehåller två satser, premisser, med termerna A, B och C. Ur dessa härleds slutsatsen, som bara innehåller termerna A och C.
Predikatet i slutsatsen kallas överterm och subjektet underterm.
Aristoteles inleder sin behandling med två grundläggande syllogismer:

Alla B är A
Alla C är B
Alla C är A

Inga B är A
Alla C är B
Inga C är A

Sedan visar han genom att ge konkreta motexempel att man ur de två premisserna

Alla B är A, Inga e är B

inte kan bilda en syllogism och inte heller ur premisserna

Inga B är A, Inga e är B.

Därmed är alla möjliga kombinationer undersökta där båda premisserna är universella och är bildade efter mönstret:

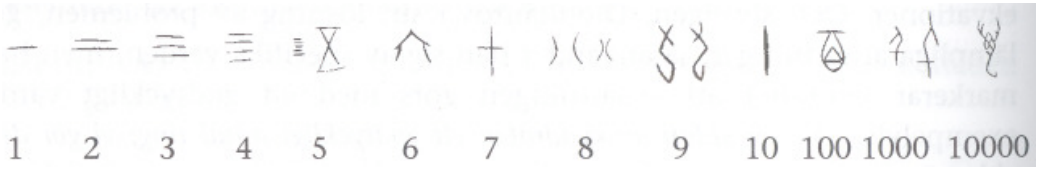
... B är A
... C är B
... C är A

Aristoteles tolkar en sats av formen "Alla B är A" så, att den dels innebär att allt som har egenskapen B också har egenskapen A, men dessutom att det verkligen finns minst ett objekt som har egenskapen B. Därav följer att om "Alla C är A" så måste också ”Några C är A” gälla. Aristoteles synsätt speglar det faktum att noll inte sågs som ett tal under antiken (och långt fram i medeltiden). I modern logik har man frångått kravet på existens, alltså kravet att "Alla B är A" innebär att det också måste finnas något objekt som har egenskapen B. I den medeltida logiken tillkom ytterligare en figur, där mellantermen var predikat i första satsen och subjekt i andra. Bortsett från ordningsföljden mellan premisserna är det samma slags slutledningar som i första figuren.

Exempel: Alla A är B, alla B är C, alltså: några C är A. Då erhöll man ytterligare fem syllogismer: Bramantip, Camenes, Dimaris, Fesapo och Fresison.
Aristoteles logik är den första axiomatiskt uppbyggda vetenskapen i historien.

1.3.4 Matematik i Kina

Väldigt lite har varit känt om kinesisk matematik fram till 1960-talet.
Tecken ristats in i ben under perioden från 1500-talet till 1000-talet f.Kr. Dessa så kallade ”orakelben” användes vid kontakter med förfädernas andar. De talsymboler som återfinns på orakelbenen och i samtida inskriptioner på bronser är symboler för ental och för tio, hundra, tusen och tiotusen.



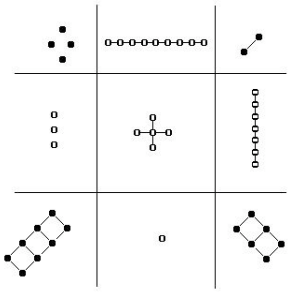
Tecknen för 5, 8 ,9 och 1000 återges i två former.

Tecknen för tio, hundra och så vidare användes också för att beteckna tiotal, hundratal. Talet 208 skulle alltså kunna skrivas som "2 hundratal och 8"

Sättet att skriva tal följde det talade språket. Det använde nio siffertecken, kompletterade med tecken för tiotal, hundratal och vidare tiopotenser.
Det bör alltså beskrivas som ett decimalt system, eftersom det är baserat på att tio enheter grupperas till en större enhet. Däremot var det inte ett positions system, eftersom de nio tecknen för ental alltid hade en och samma innebörd; för att skriva exempelvis två tiotal skulle även symbolen för tio/tiotal skrivas ut invid symbolen för två.

Osäkerheten i kronologin är stor, något som kan bero på att den tyranniske Qinkejsaren år 213 f.Kr. lät bränna många böcker. En av de böcker som troligtvis brann år 231 f.Kr i Huangdis stora bokbål var "Nio kapitel", det viktigaste matematiska verk som finns dokumenterat från den här perioden i Kina. Ett känt verk: Chou Pei Suan Ching - som behandlar främst area- och volymräkning, ränteberäkningar, kvadrat o kubikrötter, linjära ekvationer, linjära ekvationssystem, andragradsekvationer, astronomisk matematik, rätvinkliga trianglar, religion och magi.
Där kan man finna den magiska kvadraten.
Där är summan av siffrorna i diagonaler, kolumner eller rader lika med 15.

4	9	2
3	5	7
8	1	6



I denna bok finns 246 problem och hur man ska lösa dem samt numeriska svar. Då var $\pi = 3$. Senare under 200 talet e.Kr. skriver Liu Hui att $\pi = 3.14$ genom att beräkna en polygon med

96 sidor. Genom att göra beräkningar med en polygon med 3072 sidor kommer han fram till att π=3.14159. Tsu Chung-Chih (430-501) gav π ett värde 22/7 och kallade det för ”inexakt”

Kina utvecklade ett decimalt talsystem med tillhörande räkneregler. Kineserna upptäckte talens väsentligaste egenskaper 2000 år innan européerna.
Tanken till producerat material var åsikten att räkning inte är slavgöra utan begåvade människor som kan lösa stora problem.

Vid beräkningar användes ett positions system, där symbolerna för tiopotenser utelämnades och talen markerades genom att så kallade räknestavar, tunna stavar i bambu, drygt decimetern långa, som lades ut för att markera tal från ett till nio, och abakusen till sin hjälp. När man tittar hur de använde stavarna för att räkna så kan man tänka sig hur deras skrivtecken har vuxit fram.

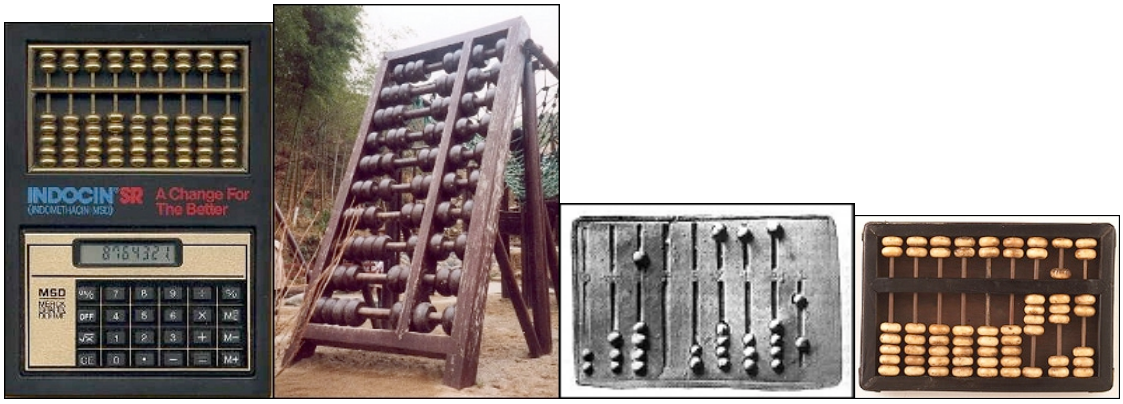
Siffror från 1-9

Tiotalsiffror

Tekniken är väsentligen ett positionssystem med basen 10, dock med den modifikationen att man har två olika slags "siffror", stående och liggande. Istället för en nolla använde man en tom plats.

Exempelvis ska talet 1066 skrivas (med två olika "sexor"):

Ett problem handlar om en följd av tal, där vart och ett är nio gånger större än det föregående. Det är 9 dammvallar där var och en har 9 träd, varje träd har 9 grenar, varje gren har 9 fågelbon, varje bo har 9 fåglar, varje fågel har 9 ungar, varje unge har 9 fjädrar och varje fjäder har 9 färger. Antalet av vart och ett ska beräknas; man får t.ex. 43 046 721 färger. Problemet är den kinesiska motsvarigheten till det egyptiska problemet där vi har 7 hus med vardera 7 katter osv.
Talet nio tycks ha spelat samma "magiska" roll i Kina som talet 7 ibland gjort i Egyptisk kultur och senare även i Europa.



Abakus - ett räknehjälpmedel som används som miniräknare. Termen *abakus* användes av romarna för att beteckna ett bord eller en bricka med marker för kalkylering. Även greker och, före dem, egyptier och troligen babylonier, har använt abakus på samma sätt, men det är först från romersk tid som vi har material bevarat. En skillnad mellan att räkna på abakus och att skriva ner uträkningarna är att själva räkningarna inte bevaras på abakusen. Det som finns kvar efter genomförda beräkningar är slutresultatet. Hur man i praktiken utfört beräkningarna med abakus under antiken finns inte dokumenterat. Den som är skicklig på att använda abakusen kan göra beräkningar snabbare än miniräknare.

Kinesisk rest tiorem uppstod ursprungligen genom uträkningen av kalendern.
Det är i Sun Zis bok "Sun Zi Suanjing", Suns aritmetiska manual, som skrevs omkring 300 f. Kr. som vi för första gången stöter på CRT då problem 26 upptas i boken; "*Vi har ett antal saker, men vi vet inte exakt hur många. Om vi räknar dom tre och tre får vi två över. Om vi räknar dom fem och fem får vi tre över. Om vi räknar dom sju och sju får vi två över. Hur många saker är det?*".
Lösningen lyder: *Om vi räknar tre och tre och har resten 2, lägg ut 140. Om vi räknar fem och fem och har resten 3, lägg ut 63. Om vi räknar sju och sju och har resten 2, lägg ut 30. Addera dessa tal och vi får 233. Dra 210 från detta för att få svaret. Om vi räknar tre och tre och har resten 1, lägg ut 70. Om vi räknar fem och fem och har resten 1, lägg ut 21. Om vi räknar sju och sju och har resten 1, lägg ut 15. Om [ett tal] överstiger 106, så får man svaret genom att subtrahera 105.*
Svaret är alltså 140+63+30-2*105 =23

I boken gavs lösningen på Sun Zis problem endast med numeriska exempel och det är därför inte möjligt att veta om Sun Zi hade utvecklat en generell metod gällande CRT. Qin Jiushao (1202-1261) kom dock på en generell metod för att lösa CRT-problem som Gauss (1777-1855) sedan utvecklade genom att använda sig av primtal. CRT användes i det gamla Kina bland annat för att kunna räkna ut antalet soldater utan att fiender kunde få reda på antalet och även vid byggandet av den kinesiska muren.

1.4 Ett teorem med flera bevis

Modulo (≡) är rest som fås från ett tal x om vi delar med ett annat tal y. Till exempel 14 ≡ 2 (mod 3), det vill säga: fjorton är kongruent med två modulo tre, då 14 delat med 3 ger 4 hela och 2 i rest.

Motiveringen till lösningsförslaget av problemet ovan är enligt följande:

Om vi antar att antalet föremål är *x,* så skulle vi kunna formulera villkoren:
$x = 3n_1 + 2$
$x = 5n_2 + 3$
$x = 7n_3 + 2$
där ett särskilt villkor utgörs av kravet att talen nl, n2 och *n3* måste vara heltal.

Att ett tal, *x,* ger resten *r* vid division med talet *n* kan uttryckas:
$x = r$ mod. n

Så förutsättningarna i problemet skulle kunna formuleras:
$x = 2$ mod. 3
$x = 3$ mod. 5
$x = 2$ mod. 7

I andra delen av lösningen står *"lägg ut* 70". Detta är en multipel av 7*5 som är vald så att det stämmer med villkoret *"om vi räknar tre och tre och har resten* l", alltså att 70 mod. 3 = 1.
Samtidigt är 70 en multipel av 5 och 7, dvs. talet 70 ger resten 0 vid division med 5 eller 7.
På samma sätt väljs talet 21 som en lämplig multipel av 3*7, så att 21 = 1 mod. 5.
Och talet 15 är valt som en lämplig multipel av 3*5, så att 15 = 1 mod. 7.
Dessa tre tal multipliceras sedan med 2, 3 respektive 2.

Då får vi:
140 = 2 mod. 3
63 = 3 mod. 5
30 = 2 mod. 7

Om man nu adderar dessa tre tal, 140 + 63 + 30 = 233, så får vi ett tal som löser uppgiften.
Om vi exempelvis dividerar med talet 5, så får vi resten 3 från en av de tre termerna (nämligen 63) medan de övriga två termerna (alltså 140 och 30) bara bidrar med resten 0.
Outsagt i problemet ligger att man söker det minsta talet, som uppfyller villkoren.
Då kan vi subtrahera ett tal från det första lösningsförslaget, om det inte förändrar resterna.
Ett sådant tal måste vara en multipel av både 3,5 och 7. Den *minsta gemensamma multipeln* av talen tre, fem och sju är 105 och innehåller precis faktorerna 3, 5 och 7. Alltså subtraheras en lämplig multipel av den minsta gemensamma multipeln 105, i detta fall 2*105, och vi får svaret 23.

Teorem:
Antag att $m_1, m_2, ..., m_r$ är parvisa relativa positiva primtal, och låt $a_1, a_2, ..., a_r$ vara tal.
Systemet av kongruenser, $x = a_i \pmod{m_i}$ for $1 <= i <= r$, har en unik lösning
modulo $M = m_1 \times m_2 \times ... \times m_r$, som ges av:

$$x = a_1M_1y_1 + a_2M_2y_2 + ... + a_rM_ry_r \pmod{M},$$

där $M_i = M/m_i$ och $y_i = (M_i)^{-1} \pmod{m_i}$ för $1 <= i <= r$.

Bevis: Lägg märke till att $\gcd(M_i, m_i) = 1$ för $1 <= i <= r$. Därför existerar alla y_i (och kan bestämmas lätt från den förlängda Euclidean Algorithm). Notera att eftersom $M_iy_i = 1 \pmod{m_i}$, har vi $a_iM_iy_i = a_i \pmod{m_i}$ för $1 <= i <= r$. Å andra sidan, $a_iM_iy_i = 0 \pmod{m_j}$ om j inte är i (eftersom $m_j \mid M_i$ i det här fallet). Alltså ser vi att $x = a_i \pmod{m_i}$ för $1 <= i <= r$.

Om det fanns två lösningar, t ex x_0, och x_1, så skulle vi få $x_0 - x_1 = 0 \pmod{m_i}$ för alla i, så att $x_0 - x_1 = 0 \pmod{M}$, dvs de är samma modulo M.

Exempel

Hitta den minsta multiplikationen av 10 som har resten 2 när det delas med 3, och resten 3 när det delas med 7.

Vi söker ett tal som satisfierar kongruenserna, $x = 2 \bmod 3$, $x = 3 \bmod 7$, $x = 0 \bmod 2$ och $x = 0 \bmod 5$. Eftersom 2, 3, 5 och 7 alla är relativa primtal i par, talar Chinese Remainder Theorem om för oss att det finns en unik lösning modulo 210 (= 2x3x5x7).
Vi beräknar M_i och y_i enligt följande:
$M_2 = 210/2 = 105$; $y_2 = (105)^{-1} \pmod 2 = 1$
$M_3 = 210/3 = 70$; $y_3 = (70)^{-1} \pmod 3 = 1$
$M_5 = 210/5 = 42$; $y_5 = (42)^{-1} \pmod 5 = 3$ och
$M_7 = 210/7 = 30$; $y_7 = (30)^{-1} \pmod 7 = 4$.

Detta innebär att $x = 0(M_2y_2) + 2(M_3y_3) + 0(M_5y_5) + 3(M_7y_7) = 0 + 2(70)(1) + 0 + 3(30)(4) = 140 + 360 = 500 \bmod 210 =$ **80**.

Teorem

Två simultana kongruenser $n = n1 \pmod{m1}$ och $n = n2 \pmod{m2}$ är endast möjliga att lösa när $n1 = n2 \pmod{\gcd(m1,m2)}$. Lösningen är unik modulo lcm(m1,m2).
När m1 och m2 är relativa primtal är deras gcd 1. Genom konvention gäller $a = b \pmod 1$ för vilket a och b som helst.

”Vi har ett antal saker, men vi vet inte exakt hur många.
Om vi räknar dom tre och tre får vi två över.
Om vi räknar dom fem och fem får vi tre över.
Om vi räknar dom sju och sju får vi två över.
Hur många saker är det?”

Lösning:

p1: $x = 2 \pmod 3$
p2: $x = 3 \pmod 5$
p3: $x = 2 \pmod 7$

Från p1 får vi $x = 3t + 2$, för vissa tal t. Genom att byta ut detta mot p2 får vi $3t = 1 \pmod 5$. Genom att hitta 1/3 i divisionstabellen modulo 5, reduceras detta till en enklare ekvation

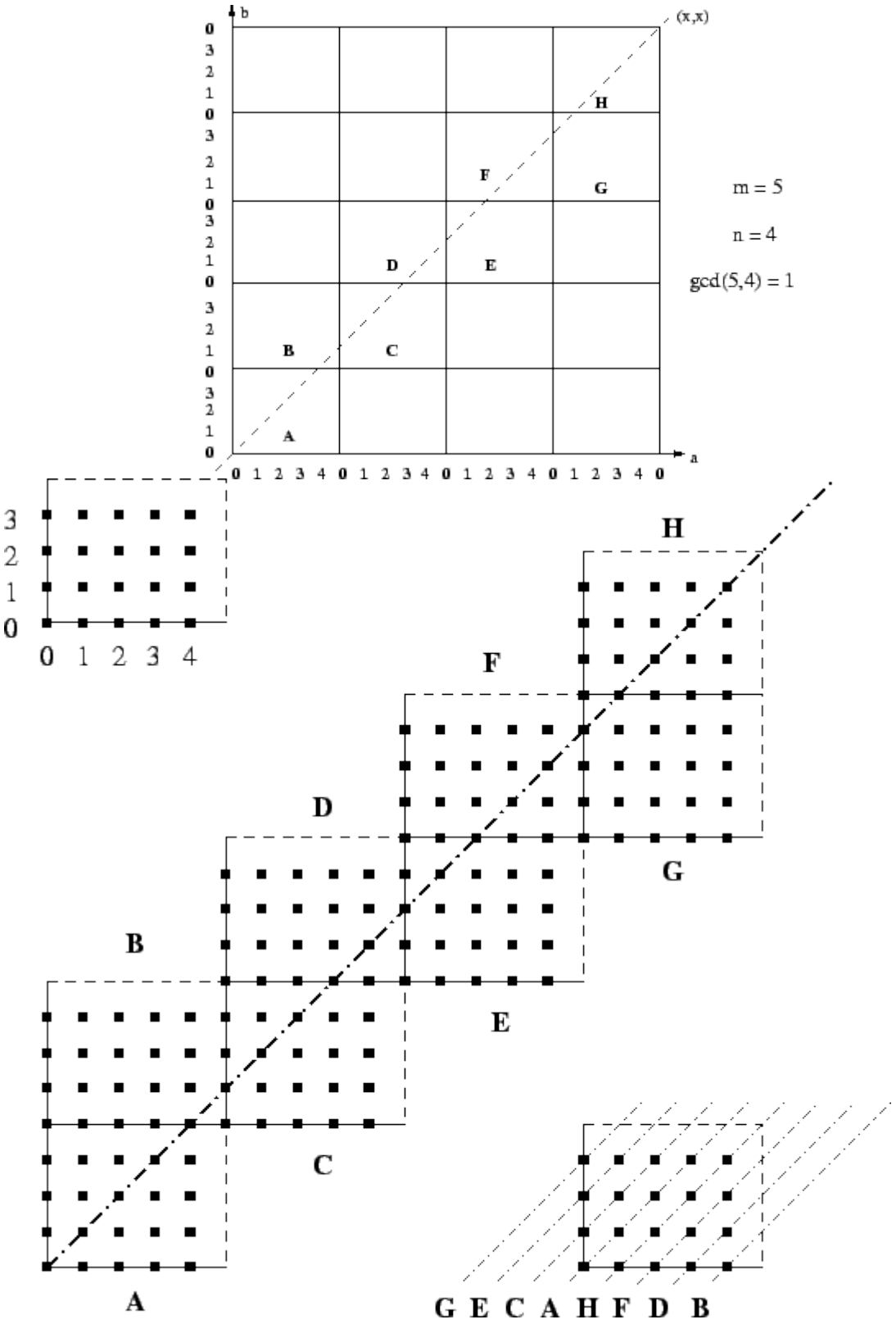
p4: $t = 2 \pmod 5$

som i sin tur är ekvivalent med $t = 5s + 2$ för ett tal s. Substituera detta till $x = 3t + 2$ gör att vi får $x = 15s + 8$.
Detta blir nu p3: $15s + 8 = 2 \pmod 7$. Kastar vi bort 7 får vi $s = 1 \pmod 7$. Härifrån blir $s = 7u + 1$ och till sist $x = 105\,u + 23$.

Notera att 105 = lcm(3,5,7). Alltså har vi lösningarna 23, 128, 233, ...

Här kan vi se att Chinese Remainder Theorem kan räknas ut genom att titta på bilden under.
$m = \mathbf{5}$, $n = \mathbf{4}$ och $x = \mathbf{x}$

$$\underset{\substack{m,n\in\mathbb{N}^* \\ \gcd(m,n)=1}}{\forall} \quad \underset{\substack{a\in\mathbb{Z}_m \\ b\in\mathbb{Z}_n}}{\forall} \quad \underset{0\leqslant x<mn}{\exists} \quad \Big(x \equiv a \pmod m \quad \wedge \quad x \equiv b \pmod n\Big) \;!$$



2. Tillämpning av CRT inom Computing, Coding och Cryptography

Här kommer jag att mer djupgående gå igenom tre områden inom vilka Chinese Remainder Theorem kan vara användbart.

2.1 Computing

Antag att m_1, m_2, …, m_n är parvisa relativa primtal större än eller lika med 2 och låt m vara deras produkt. Med CRT kan vi bevisa att tal a med $0 \leq a < m$ kan vara unikt representerad av n-tuple bestående av dens rest vid division med m_i, i = 1, 2, …, n. Alltså, vi kan unikt representera a med (a **mod** m_1, a **mod** m_2, …, a **mod** m_n).

Med CRT kan alla tal som är mindre än 99 * 98 * 97 * 95 = 89,403,930 representeras unikt med deras rest när vi dividerar med dessa fyra moduler. Till exempel, vi representerar 123,684 som (33,8,9,89), därför att 123,684 **mod** 99 = 33, 123,684 **mod** 98 = 8, 123,684 **mod** 97 = 9, 123,684 **mod** 95 = 89. På liknande sätt kan vi representera 413,456 som (32,92,42,16).

För att hitta summan av 123,684 och 413,456 jobbar vi med dessa 4-tuplar istället.
Vi adderar de 4-tuplerna komponentvis och reducerar varje komponent med hänsyn till den passande modulen. Detta innebär (33,8,9,89) + (32,92,42,16)
= (65 **mod** 99, 100 **mod** 98, 51 **mod** 97, 105 **mod** 95)
= (65, 2, 51, 10).

För att hitta summan, dvs det tal som representeras av (65, 2, 51, 10), behöver vi lösa det här systemet

$x \equiv 65 \pmod{99}$
$x \equiv 2 \pmod{98}$
$x \equiv 51 \pmod{97}$
$x \equiv 10 \pmod{95}$

Det kan bevisas att 537,140 är den unika icke-negativa lösningen till detta system som är mindre än 89,403,930. Följaktligen är 537,140 summan. Notera att det är bara tal mindre än 100 som krävs för att räkna ut summan.

Vi tar ett aritmetiskt uttryck;

$$F(x,y) = 100xy + x^2 + y^2$$

Antag att vi vill räkna ut F (x,y) för talet som är $0 \leq x \leq 10$ och $0 \leq y \leq 10$.

Vi har; $0 \leq F(x,y) \leq 10200$

För att räkna ut m behöver vi parvisa relativa primtal med produkten större än eller lika med 10201.
Då väljer vi
$m_1 = 3$,
$m_2 = 4$,
$m_3 = 7$,
$m_4 = 11$,
$m_5 = 13$.
Då är $m = 12012$.

För att räkna ut F (10,9) behöver vi först

$F_1(x,y) = (x+y)^2 - xy, \quad (x,y) \in \mathbf{Z}/(3) * \mathbf{Z}/(3),$
$F_2(x,y) = x2 + y^2, \quad (x,y) \in \mathbf{Z}/(4) * \mathbf{Z}/(4),$
$F_3(x,y) = (x+y)^2, \quad (x,y) \in \mathbf{Z}/(7) * \mathbf{Z}/(7),$
$F_4(x,y) = (x+y)^2 - xy, \quad (x,y) \in \mathbf{Z}/(11) * \mathbf{Z}/(11),$
$F_5(x,y) = (x-y)^2 - 2xy, \quad (x,y) \in \mathbf{Z}/(13) * \mathbf{Z}/(13)$

och

$ø_1(10,9) = (1,0), \quad ø_2(10,9) = (2,1),$
$ø_3(10,9) = (3,2), \quad ø_4(10,9) = (-1,-2), \quad ø_5(10,9) = (-3,-4).$

Sen räknar vi;
$F_1(1,0) = 1, \quad F_2(2,1) = 1, \quad F_3(3,2) = 4, \quad F_4(-1,-2) = 7, \quad F_5(-3,-4) = -10.$

Slutligen får vi

$F(10,9) \equiv 1 \pmod 3.$
$\equiv 1 \pmod 4.$
$\equiv 4 \pmod 7.$
$\equiv 7 \pmod{11}.$
$\equiv -10 \pmod{13}$
$= 9181$

2.2 Coding

Coding teori har viktiga appliceringar inom kommunikation och datorsystem, där data-error ofta förekommer. Grundtanken för error-sökning och -rättning är att addera ett överskott av data som sänds genom en störande kanal eller spara den i datorn. Remaindertekniker baserade på CRT är användbara när man konstruerar error-rättningskoder.
Det är intressant att notera att alla koderna och avkoderna så väl som parameteranalysen av de generaliserade överskottskoderna kan utföras med CRT och CRA.

Error-rättningskoder är indelade i två klasser, block och invecklade koder. För block-koder har kodnings- (resp avkodnings-) verktygen inget internt minne, medan de invecklade koderna har det.
Om A={0,1}
Vektorerna C={00000,11111}
Vi har (5,2,5) är koden över A.
Sträckan mellan de två kodorden är 5.
Vi kan kryptera meddelandet genom att byta platser för en 0 (resp.1) i meddelande med 00000 (resp.11111).
Om vi tänker oss att meddelandet är
(100011)
då krypteringen är,
(11111000000000000000011111111111)

2.3 Cryptography

Kungar, drottningar och generaler röjer värdefulla hemligheter för rivaliserande länder och avslöjar viktiga upplysningar för fientliga trupper. Det var inför hotet att fienden skulle uppsnappa meddelandena som man utvecklade koder och chiffer, metoder som döljer budskapet så att bara den rätte mottagaren kan läsa det. Kodernas historia genom tiderna är en berättelse om den månghundraåriga striden mellan kodmakare och kodknäckare. Den ständigt pågående striden mellan kodmakare och kodknäckare har gett inspiration till en rad märkliga vetenskapliga framsteg.
Kodmakarna har ständigt sökt konstruera allt säkrare koder för att trygga förbindelserna, medan kodknäckarna ständigt uppfinner nya kraftfulla metoder för att angripa dem. De har genom sitt arbete påskyndat den tekniska utvecklingen, där våra moderna datorer utgör det mest slående exemplet. Numera studsar våra telefonsamtal mellan satelliterna och e-postbreven passerar olika typer av datorer. Dessa två slag av kommunikation kan lätt uppsnappas, vilket hotar att störa vårt privata liv.
Därför är kryptering det enda sättet att skydda den personliga integriteten och garantera framgång för den digitala marknadsplatsen
Kryptografins betydelse har visserligen ökat i det civila, men vi bör också notera att kryptografin inom det militära är minst lika viktig som förr. Det har sagts att första världskriget var ett kemisternas krig. Då användes senapsgas och klorgas för första gången. Andra världskriget skulle ha varit ett fysikernas krig, eftersom det var då som atombomben sprängdes. I analogi därmed har det hävdats att ett tredje världskrig skulle bli ett matematikernas krig, eftersom de behärskar det nya, avgörande vapen som heter information. Det är ju matematikerna som ligger bakom utvecklingen av de koder som för närvarande används för att skydda militära hemligheter. Det är också matematikerna som befinner sig i frontlinjen i kampen för att knäcka koderna.

Ett hemligt meddelande räddade grekerna från att besegras av Xerxes, Konungarnas konung, persernas diktatoriske ledare. Den långvariga fejden mellan Grekland och Persien nådde sin kulmen strax efter det att Xerxes hade börjat uppföra en stad vid Persepolis.
Den skulle bli ny huvudstad i hans kungarike. År 480 f Kr mobiliserade Xerxes en styrka for att sätta igång en överraskningsattack och tillkännagav att ”vi skall utvidga Persiens gränser”. En grekisk man vid namn Demaratos hade bevittnat den militära mobiliseringen. Han hade fördrivits från sitt land och bodde nu i den persiska staden Susa. Han kände dock en viss lojalitet mot Grekland och beslöt att sända ett varnande budskap till spartanerna om överraskningsattacken. Det gällde att få iväg budskapet utan att de persiska vakterna kunde beslagta det. Eftersom risken för upptäckt var stor, fanns det bara ett sätt för honom att lyckas med att överlämna budskapet. Han skrapade av vaxet på två skrivtavlor och ristade in i träet därunder vad Xerxes tänkte göra. Sedan täckte han åter över budskapet med vax. På så sätt kunde skrivtavlorna, som tycktes vara helt tomma, smidigt föras förbi vakterna längs vägen. Då budskapet nådde sin bestämmelseort upptäcktes inte hemligheten förrän Gorgo, maka till Leonides, frågade gudarna till råds och sade till de andra att om de skrapade bort vaxet skulle de finna en inskrift på träet under. Budskapet avslöjades och lästes upp och fördes sedan vidare till övriga greker. För att få sina instruktioner framförda på ett säkert sätt vid annat tillfälle lät han raka huvudet på sin budbärare, skrev budskapet på huvudsvålen och väntade sedan tills håret hade vuxit ut igen. Budbäraren slapp att bli ofredad på vägen.

Att dölja själva existensen av budskapet går under namnet steganografi, vilket kommer av grekiskans steganos (στεγανός) som betyder 'dold, över täckt', och graflin (γραφειν) som betyder 'skriva'. Under de två tusen år som gått sedan Herodotos tid har

man använt olika former av steganografi över allt i världen. I det gamla Kina skrev man till exempel budskap på tunt silke, som man sedan knycklade ihop till en liten boll och täckte med vax. Sedan svalde budbäraren den lilla bollen.

Den italienske vetenskapsmannen Giovanni Porta beskriver på 1400-taletett sätt att dölja budskapet i ett hårdkokt ägg genom att tillverka bläck av ett uns alun och ett skålpund vinäger och sedan skriva med detta bläck på skalet. Lösningen tränger igenom det porösa skalet och lämnar ett budskap inuti på den stelnade äggvitans yta som kan läsas först när man har skalat ägget. Till steganografi hör också bruket att skriva med osynligt bläck. Redan under det första århundradet e Kr beskriver Plinius den äldre hur man kan använda 'mjölk' från plantan *tithymalus* som osynligt bläck. Det blir genomskinligt när det torkat, men mörknar och blir brunt om man värmer upp det försiktigt. Många organiska vätskor uppför sig på liknande sätt, och det tjugonde århundradets spioner har inte varit främmande för att improvisera när de stått utan sitt vanliga osynliga standardbläck; de har använt sin egen urin. Men en nitisk vakt kan ha som rutin att kroppsvisitera varje person som går över gränsen; han kan skrapa vaxet från tavlan, upphetta det blanka papperet, skala det hårdkokta ägget, raka slavens huvud och så vidare. Det kommer oundvikligen att uppstå tillfällen då budskapet blir avslöjat.

Därför utvecklades parallellt med steganografi det vi kallar för Kryptografi, vilket kommer av det grekiska ordet kryptos (κρυπτός) med betydelsen gömd. Kryptografins syfte är inte att dölja själva meddelandet, utan snarare att dölja dess innebörd. Vill man göra ett budskap obegripligt för fienden kan man förvränga det enligt en uppsättning regler som sändaren och den avsedde mottagaren på förhand kommit överens om. Alltså kan mottagande part tillämpa förvrängningsreglerna baklänges och göra budskapet förståeligt. Fördelen med kryptografi är, att även om fienden fångar upp ett krypterat budskap kan han inte läsa det. Kryptografi och steganografi må vara skilda discipliner, men det är fullt möjligt att samtidigt dölja ett budskap för att uppnå maximal säkerhet

Kryptografin kan i sin tur indelas i två grenar, transposition och substitution.
Vid transposition placerar man helt enkelt om bokstäverna till något som i praktiken utgör ett anagram.. Ett ord om tre bokstäver kan till exempel stuvas om på sexolika sätt (kam, kma, akm, amk, mka, mak). Det blir omöjligt att återgå till det ursprungliga meddelandet om man inte exakt känner till förvrängningsprocessen. ”Betrakta till exempel denna korta mening.” Den innehåller bara 35 bokstäver, och ändå finns det 10 814 200 000 000 000 000 000 000 000 000 olika sätt att placera dem. Om en person kunde kontrollera ett placeringssätt i sekunden och alla människor i hela världen arbetade dygnet runt, skulle det ändå ta mer än universums hela livstid ett tusen gånger om att kontrollera alla placeringssätten.
Ska transpositionen vara effektiv måste omplaceringen av bokstäverna följa ett system som är på förhand överenskommet mellan sändare och mottagare, och som de håller hemligt för fienden. Ett exempel: scouter kan ibland skicka meddelanden med hjälp aven transposition som de kallar ”brädgården” Det innebär att man skriver ut budskapet så att varannan bokstav hamnar på en undre rad och varannan på en övre. Den undre radens bokstäver hakas sedan på den övre. På så vis far man ett krypterat budskap:

DIN HEMLIGHET ÄR DIN FÅNGE; LÅT DEN FARA, OCH DU BLIR SJÄLV DESS FÅNGE

↓

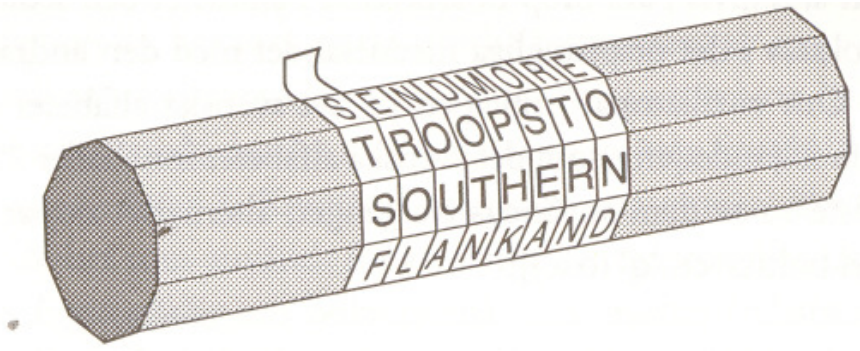
D N E L G E Ä D N Å G L T E F R O H U L R J L D S F N E

I H M I H T R I F N E Å D N A A C D B I S Ä V E S Å G

↓

DNELGEÄDNÅGLTEFROHULRJLDSFNEIHMIHTRIFNEÅDNAACDBISÄVESÅG

Det finns åtskilliga andra former av systematisk transposition, som det treradiga "brädgårdschiffret".



När läderrems an lindas av sändarens scytale (trästaven), tycks den bära en rad meningslösa bokstäver: S, T, S, F, ... Inte förrän mottagaren virar remsan omkring sin egen scytale (med samma diameter) framstår budskapet som begripligt.

Substitution är en metod som rekommenderas består i att slumpvis para ihop bokstäverna i alfabetet och sedan ersätta varje bokstav i det ursprungliga meddelandet med den andra parbokstaven.

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

Då skulle avsändaren, istället för att skriva "möt mig vid midnatt" skriva
"cqz cgi agx cgxsvzz" I transpositionschiffret behåller varje bokstav sin identitet men ändrar position. I substitutionschiffret däremot ändrar varje bokstav identitet men bibehåller sin position.
Julius Caesar använde substitutionschiffret. Han ersatte varje bokstav i det romerska alfabetet med den bokstav som fanns tre positioner längre ner, d.v.s. ”a” ersattes med ”d”, ”c” ersattes med ”f ”och när man kom till slutet fortsatte man i alfabetets början. Lite senare använde Augustus samma teknik men flyttade bara en position.
Dessa chiffer är exempel på (monoalfabetiska) substitutionschiffer. I monoalfabetisk substitution kan man generera 26! olika substitueringar, d.v.s. 403 291 461 126 605 635 584 000 000. Men en sådan här substitution är lätt att knäcka om man använder kryptanalytiska tekniker som började utvecklas av araberna.

De uppfann kryptoanalysen, den vetenskap som handlar om att återställa ett budskap utan kännedom om nyckeln. Medan kryptografen utvecklar nya hemliga skriftmetoder, är det kryptoanalytikerns uppgift att hitta svagheterna i dem för att kunna forcera hemliga meddelanden.
De arabiska kryptoanalytikerna lyckades hitta en metod att knäcka det monoalfabetiska substitutionskryptot, som hade varit osårbart i åtskilliga hundra år.
Ett sätt att lösa ett krypterat budskap är att leta upp en klartext på samma språk. Vi räknar ut hur många gånger varje bokstav uppträder. Vi kallar den vanligast förekommande bokstaven för den "första", den näst vanligaste för den "andra" o s v. tills vi är färdiga med alla de olika bokstäverna i klartextprovet Därefter betraktar vi den chiffertext vi vill lösa och klassificerar även dess symboler.
Vi letar upp den vanligaste symbolen och ändrar dess utseende till den "första" bokstaven i klartextprovet; den näst vanligaste symbolen ändrar utseende till den "andra" bokstaven osv.

Tabell över relativa frekvenser för det svenska språkets bokstäver,

Bokstav	%	Bokstav	%	Bokstav	%
a	9,3	k	3,2	u	1,8
b	1,3	l	5,2	v	2,4
c	1,3	m	3,5	w	0,03
d	4,5	n	8,8	x	0,1
e	9,9	o	4,1	y	0,6
f	2,0	p	1,7	z	0,02
g	3,3	q	0,007	å	1,6
h	2,1	r	8,3	ä	2,1
i	5,5	s	6,3	ö	1,5
j	0,7	t	8,7		

I svenskan är 'e' den vanligaste bokstaven, följd av' a', 'n' och 't', och så vidare; se. Sedan undersöker vi kryptotexten i fråga och arbetar fram frekvensen för varje bokstav. Om den vanligaste bokstaven i kryptotexten är, låt oss säga Ä verkar det troligt att den ersätter bokstaven 'e'. Om vidare den näst vanligaste bokstaven är 'P', är den förmodligen en ersättning för' a', o s v.

Vi antar att vi har uppsnappat följande kodade budskap. Det gäller att dekryptera det. Vi vet att texten står på svenska och att den har förvrängts enligt ett enkelt substitutionskrypto, men vi har ingen aning om nyckeln. Det är opraktiskt att pröva alla tänkbara nycklar, och därför måste vi tillämpa kryptoanalys.

RSP EKPÅ IGÄNHDÄH KJÖHÄIJ: ”ÄAE, IGSNSHÄWÄVS, LDOESP KPVSHÖÄH NDIJCHDÄ! VK NÄH RSV VDPÄ EKPPDÅÄ CAN LYOLÄ-OVÄ CHV OXJDJ RDÅ TZOGÄ NYPVSOISH ICR EKPÅÄH CAN TCOE D ÄPVHÄ OYPVSH NÄH KBBOSLÄJ TZHH CAN PK, CAN RXPÅÄ ÄL VSR NÄH LÄHDJ RUAESJ IYOOIÄRRÄ CAN JYPELYHVÄ. ÅSPCR ÄJJ OUIIPÄ JDOO VDÅ D JKISP CAN SP PYJJSH NÄH GÄÅ ÖODLDJ SP NSOJ ÄPPÄP RYPPDIEÄ CAN YH PK NSOJ KBBTUOOV ÄL OUAEÄP ÄL ÄJJ OSLÄ. ÄOOÄN LÄHS OCLÄV TZH ÄJJ NÄP NÄH IEYPEJ VDÅ, RDP LSIDHI LYOIDÅPÄVS VCJJSH, IX RXPÅÄ KJIZEJÄ ÅXLCH. ”

KH SBDOCÅSP JDOO JKISP CAN SP PÄJJ

Frekvens analys av det krypterade meddelandet.

bokstav	frekvens	%	bokstav	frekvens	%
A	11	2,6	P	36	8,5
B	5	1,2	Q	0	0,0
C	17	4,0	R	13	3,1
D	22	5,2	S	29	6,9
E	13	3,1	T	5	1,2
F	0	0,0	U	4	0,9
G	4	0,9	V	18	4,3
H	29	6,9	W	1	0,2
I	19	4,5	X	5	1,2
J	31	7,4	Y	11	2,6
K	14	3,3	Z	4	0,9
L	16	3,8	Å	13	3,1
M	0	0,0	Ä	49	11,6
N	21	5,0	Ö	3	0,7
O	28	6,6			

Efter några försök kommer man fram till den riktiga texten med de riktiga bokstäverna

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

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

Men kung Sjahriar utbrast: ”Ack, Sjeherazade, vilken underbar historia! Du har med dina kunniga och välvalda ord låtit mig följa händelser som kungar och folk i andra länder har upplevat förr och nu, och många av dem har varit mycket sällsamma och tänkvärda. Genom att lyssna till dig i tusen och en nätter har jag blivit en helt annan människa och är nu helt uppfylld av lyckan av att leva. Allah vare lovad för att han har skänkt dig, min vesirs välsignade dotter, så många utsökta gåvor.”

Ur epilogen till Tusen och en natt

Man skulle kunna använda två eller ännu fler olika krypto alfabet och växla mellan dem under krypteringens gång för att förvirra den tänkte kryptoanalytikern.

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 1

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

Kryptoalfabet 2

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

Vigeneres chiffer.
Styrkan i Vigenere kryptot ligger i att man använder inte bara ett, utan tjugonio olika chifferalfabet för att kryptera en text. Första steget i krypteringen innebär att man ritar upp en så kallad Vigenere tabell ett klartextalfabet följt av 29 kryptoalfabet, där vart och ett ligger förskjutet ett steg i förhållande till det föregående.

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
1	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	A
2	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	A	B
3	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
4	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	D
5	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	D	E
6	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	D	E	F
7	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	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	Å	Ä	Ö	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
26	Å	Ä	Ö	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
27	Ä	Ö	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
28	Ö	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
29	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

Alltså återger första raden ett kryptoalfabet med en Caesarrullning, en förskjutning om ett steg, vilket betyder att det kan användas som ett Caesarkrypto där varje bokstav i klartexten ersätts med den bokstav som står ett steg åt höger i alfabetet. Om man använder alfabet nummer två krypteras bokstaven c som E, men använder man alfabet nummer tolv krypteras *c* som O. Istället för att skicka att du vill använda alfabet nummer 2 och sedan nummer 12 så skickar du ett nyckel ord och i det här fallet så är det ”CM”. ”C” för rad nummer 2 för den

börjar med ”C” och rad 12 börjar med ”M”. Nyckel ordet kan vara så lång man vill. Är den lika lång som själva meddelandet så är det svårare att dekrypteras.
De traditionella substitutioner krypton, som fanns redan före Vigeneres chiffer, har kallats monoalfabetiska, eftersom man bara använder ett alfabet per meddelande. Vigeneres krypto hör däremot till en grupp chiffer som kallas polyalfabetiska eftersom det utnyttjar flera olika kryptoalfabet per meddelande. Men efter som hans krypto är mycket komplicerat och kräver extra ansträngning för att tillämpas. Avskräckte det många från att ta det i bruk.

Det fanns medel svåra chiffer, bland annat det homofoniska substitutionskryptot.
På grekiska heter 'samma' homos, och 'ljud' heter fone. Det går ut på att ersätta varje bokstav med flera olika tecken som ska ha samma ljud som själva bokstaven och låta antalet tecken vara proportionerligt mot bokstavsfrekvensen. Bokstaven ”a” svarar för drygt 9 % av alla bokstäver i skriven svenska, och därför skulle vi avdela åtta tecken till att ersätta den. Varje gång ”a” uppträder i klartexten väljer vi ett av tecknen som ersättning. Då krypteringen är slutförd utgör varje sådant tecken ungefär 1% av den krypterade texten. En så sällsynt bokstav som z skulle bara få sig tilldelat ett tecken.

I exemplet nedan råkar de substituerande kryptobokstäverna vara tvåsiffriga tal, och för varje bokstav i klartextalfabetet finns mellan ett och tolv substitut, beroende på hur ofta den förekommer.

Ett exempel på homofoniskt substitutionskrypto.

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
09	48	13	01	14	10	06	23	32	15	04	26	22	18	00	38	94	29	11	17	08	34	60	28	21	02			
12	81	41	03	16	31	25	39	70			37	27	58	05	95		35	19	20	61		89		52				
33		62	45	24			50	73			51		59	07			40	36	30	63								
47			79	44			56	83			84		66	54			42	76	43									
53				46			65	88					71	72			77	86	49									
67				55			68	93					91	90			80	96	69									
78				57										99					75									
92				64															85									
				74															97									
				82																								
				87																								
				98																								

”ett exempel” skulle skrivas ”141720-14281622382426”.

Under 1700-talet började kryptoanalysen bli något aven industri, där regeringarnas krypto analytiker arbetade i lag för att knäcka även det mest invecklade monoalfabetiska chiffer. Det mest berömda, disciplinerade och effektiva av dem alla var Geheime Kabinetts-Kanzlei i Wien.
Förutom den allt effektivare kryptoanalysen fanns ytterligare en faktor som drev fram säkrarekrypteringsmetoder, nämligen utvecklingen av telegrafen under mitten av 1700-talet och behovet av att skydda telegrammen från att bli uppsnappade och forcerade.

Ett anonymt brev i en skotsk tidskrift beskriver hur man kunde vidarebefordra meddelanden över långa avstånd genom att förbinda sändare och mottagare med tjugosexledningar, en för varje bokstav i det engelska alfabetet.
Sändaren kunde då bokstavera meddelandet genom att skicka elektriska impulser genom ledningarna. För att bokstavera "hejsan" skulle sändaren först skicka en signal via 'h' ledningen, sedan via 'e' ledningen, och så vidare. Mottagaren skulle på något sätt uppfatta den elektriska strömmen i varje ledning och kunna tolka budskapet.
Samuel Morse konstruerade den första telegraflinjen, Morse använde en elektromagnet för att förstärka signalen så att den vid ankomsten hos mottagaren var kraftig nog att göra en rad långa eller korta avtryck på ett papper. Han tog också fram det numera välkända morsealfabetet, en kod för översättning av alfabetets bokstäver till olika kombinationer av streck och punkter.

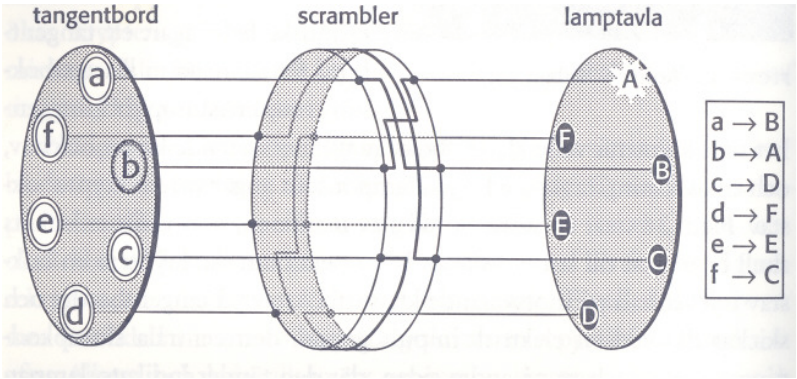
Symbol	Code	Symbol	Code
A	·–	W	·––
B	–···	X	–··–
C	–·–·	Y	–·––
D	–··	Z	––··
E	·	1	·––––
F	··–·	2	··–––
G	––·	3	···––
H	····	4	····–
I	··	5	·····
J	·–––	6	–····
K	–·–	7	––···
L	·–··	8	–––··
M	––	9	––––·
N	–·	10	–––––
O	–––	full stop	·–·–·–
P	·––·	comma	––··––
Q	––·–	question mark	··––··
R	·–·	colon	–––···
S	···	semicolon	–·–·–·
T	–	hyphen	–····–
U	··–	slash	–··–·
V	···–	quotation mark	·–··–·

Utvecklingen av krypteringsmaskinerna från krypteringsskivor till Enigma.
Den första krypteringsmaskinen är chiffer skivan, som uppfanns på 1400-talet av den italienske arkitekten Leon Alberti, en av upphovsmännen till det polyalfabetiska chiffret. Han tog två runda kopparskivor, den ena något större än den andra, och ristade in alfabetet runt kanten på dem båda. Så placerade han den mindre skivan ovanpå den större och fäste ihop dem med en nål i mitten som axel. De två skivorna kan vridas futt, så att de två alfabetena kan

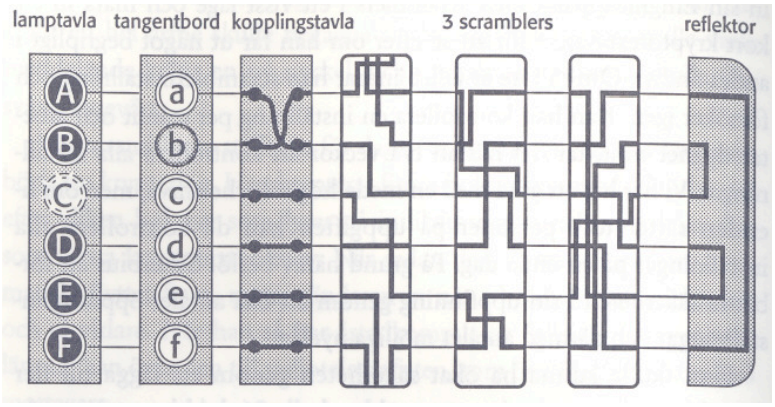
inta olika lägen i förhållande till varandra, vilket betyder att de kan användas för att kryptera ett budskap med enkel Caesarrullning.

Vill man kryptera ett meddelande med en caesarisk förskjutning om ett steg placerar man det inre 'N´ mot det yttre 'B' - den inre skivan blir klartextalfabet och den yttre tjänstgör som kryptoalfabet. Varje bokstav i klartextmeddelandet letas upp på innerskivan och motsvarande bokstav på ytterskivan skrivs ner och utgör kryptotexten.
Om man i stället vill skicka ett meddelande med en caesarisk förskjutning om fem steg, vrider man skivan så att det inre 'N´ står vid det yttre 'F' och använder sedan skivan på samma sätt med den nya inställningen. Som maskin betraktad är chifferskivan ytterst elementär, men den förenklar trots allt krypteringen, och den stod sig i fem hundra år.

Slumpkodaren, eller scramblern, är en tjock gummiskiva full av elledningar, som utgör maskinens viktigaste beståndsdel. Från tangentbordet löper ledningarna in i slumpkodaren på sex olika ställen och snor runt därinne för att sedan dyka upp vid sex olika punkter på baksidan.
Det är detta inre ledningsnät som avgör hur klartextbokstäverna kommer att krypteras. Om man skriver bokstaven a tänds lampan för bokstaven B, vilket betyder att a krypteras som B; . om man skriver bokstaven b tänds lampan för bokstaven A, vilket betyder att b krypteras som A; och c krypteras som D; och d krypteras som F; och e krypteras som B; och f krypteras som C.
Ordet caft skulle krypteras som DBCE. Detta är själva grundstrukturen för hur slumpkodaren anger ett kryptoalfabet, och man kan alltså med maskinens hjälp ta fram ett enkelt monoalfabetiskt substitutionskrypto.

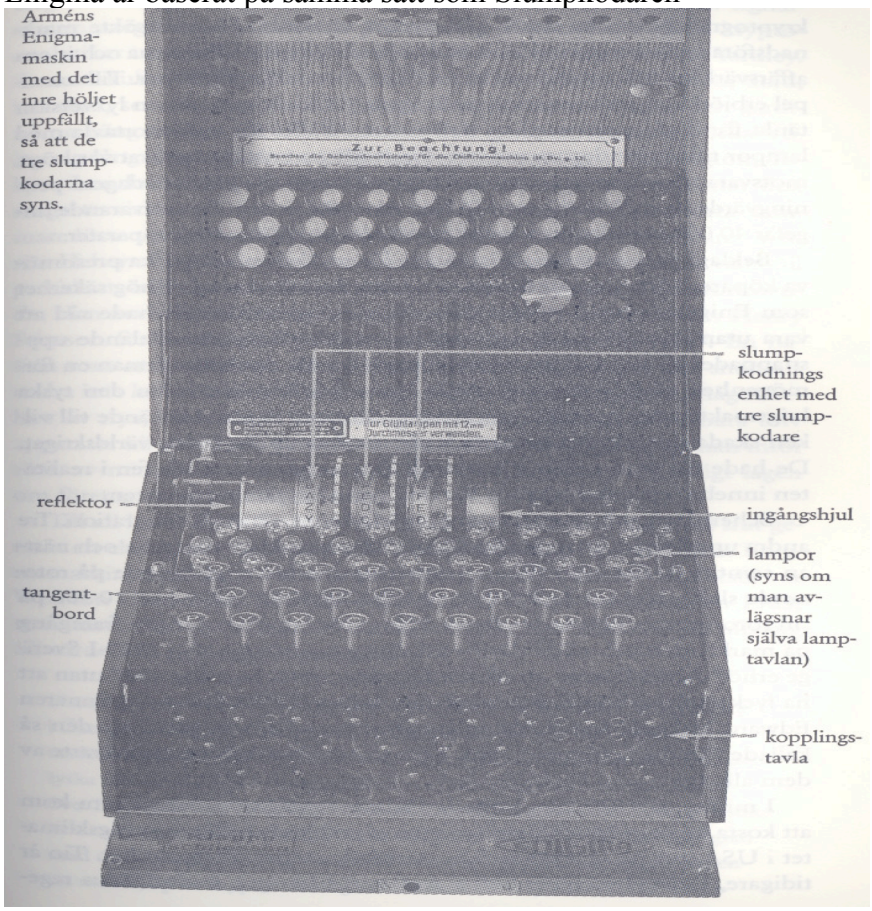


Man kan bygga mer avancerade Slumpkodaren som kan se ut så här.
Kopplingstavlan är placerad mellan tangentbordet och den första scramblern.
Genom att ansluta lösa kablar på olika sätt kan man låta bokstäverna byta plats parvis. I detta fall byter *b* plats med *a.* Då krypteras *b* genom att strömmen följer den väg som förut användes får att kryptera *a.* I den riktiga Enigma med 26 bokstäver hade operatören minst sex kablar och kunde alltså låta minst sex bokstavspar byta plats.



Här följer en lista över maskinens olika variabler och antalet möjligheter
som gäller för var och en:
Scramblers: Var och en av de 3 scramblerna kan ställas in på 26 olika sätt. Det finns alltså 26x 26 x 26 olika inställningar. **17576**
Scramblers:3 scramblers (1,2 och 3) kan ha följande inbördes
ordning: 123,132,213,231,312,321 **6**
Kopplingstavla: Antalet sätt att kombinera sex par bokstäver av 26 och därmed låta
dem byta plats, är jättelikt. **100391 791 500**
Det totala antalet möjliga nycklar är lika med produkten av de ovanstående tre talen:
Antalet möjliga nycklar = 17576 x 6 x 100391 791 500
Ca 10 000 000 000 000 000

Enigma är baserat på samma sätt som Slumpkodaren



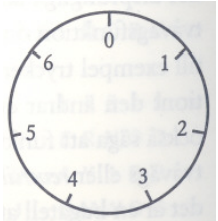
Sedan kryptoanalytikerna alltså bidragit till den moderna datorns födelse, fortsatte de efter kriget med att utveckla och använda datortekniken för att knäcka alla slagskrypton. De kunde utnyttja den programmerbara datorns snabbhet och flexibilitet för att söka igenom alla nyckelmöjligheter tills de slutligen fann den rätta.
Så småningom började emellertid kryptokonstruktörerna att slå tillbaka. De utnyttjade datorkraften för att skapa allt mer intrikata krypton. Kort sagt, efter kriget har datorn kommit att spela en avgörande roll i kampen mellan kodmakare och kodknäckare. Datorkryptering av meddelanden liknar i mångt och mycket de mer traditionella krypteringsformerna. Egentligen finns det bara tre skillnader mellan datorkryptering och den sortens mekaniska kryptering som låg till grund för krypton som Enigma. Den första skillnaden är att den mekaniska krypteringsapparaten begränsas av vad som i praktiken är möjligt att bygga, medan datorn kan imitera en hypotetisk kryptomaskin som är ofantligt komplicerad. En dator kan till exempel programmeras till att utföra hundra slumpkodar arbete, varav vissa snurrar medurs, andra moturs, eller plockas bort efter var tionde bokstav, eller snurrar fler och fler steg åt gången under krypteringen. En dylik mekanisk apparat går inte att bygga, men dess datoriserade motsvarighet kan leverera ett högst tillförlitligt krypto. Den andra skillnaden rör hastigheten. Elektronik är snabbare än mekaniska rotorer. En dator som programmerats att efter likna Enigma kan kryptera ett långt meddelande på ett ögonblick. Även om en dator skulle programmeras för att genomföra en avse värt mer komplicerad kryptering. Den tredje och kanske viktigaste skillnaden är att datorn slumpkodar siffror och inte bokstäver. Datorerna opererar enbart med binära tal, rader av ettor och nollor som kallas *bits*. Därför måste alla meddelanden omvandlas till binära tal innan man kan kryptera dem. För tillfället räcker det med att vi tänker oss ett binärt tal som en viss räcka ettor och nollor som betecknar en viss speciell bokstav, på samma sätt som morsealfabetet kopplar samman varje bokstav med sin särskilda kombination av punkter och streck.
Det finns 128(2) sätt att ordna sju binära siffror inbördes, och därför kan ASCII beteckna upp till 128 olika tecken. Det ger gott om utrymme för beteckningar även för de gemena tecknen (t.ex. 'a' = 1100001), interpunktionstecken (t.ex. 'J' = 0100001) och andra symboler (t.ex. '&' = 0100110). När väl konverteringen är genomförd kan krypteringen ta vid.

A	1000001	N	1001110
B	1000010	O	1001111
C	1000011	P	1010000
D	1000100	Q	1010001
E	1000101	R	1010010
F	1000110	S	1010011
G	1000111	T	1010100
H	1001000	U	1010101
I	1001001	V	1010110
J	1001010	W	1010111
K	1001011	X	1011000
L	1001100	Y	1011001
M	1001101	Z	1011010

För att kryptera *HEJSAN* med hjälp av ett transpositionskrypto i enkel datorversion. Innan vi kan börja måste vi översätta budskapet till ASCII enligt tabellen ovan:
Klartext= HEJSAN= 10010001000101 10010101010011 1000001 1001110
Den kanske enklaste formen av transpositionskrypto vore att låta första och andra siffran byta plats, sedan den tredje och fjärde, och så vidare.

Klartext = 10010001000101100101010100111000001100111 0
Kryptotext = 01100010001010011010101000110100001100110 1
En intressant aspekt av transpositionen på de binära talens nivå är att växlingen sker inuti bokstaven, och vad mera är, delar aven bokstav kan byta plats med delar av grannbokstäverna. Här har till exempel slutnollan i 'H' bytt plats med ingångs ettan i 'E'. Det krypterade meddelandet består alltså av fyrtiotvå binära siffror i en enda lång rad, och det överförs i det formatet till mottagaren. Han kan sedan vända på transpositionen och återskapa den ursprungliga talföljden. Slutligen tolkar han tillbaka de binära siffrorna till bokstäver via ASCII, och budskapet har återkommit: *HEJSAN*.

Vi tänker oss ett land där moralen inom postväsendet är obefintlig: de postanställda läser all oskyddad korrespondens. En vacker dag vill Alice skicka ett personligt meddelande till Bob. Hon väljer att lägga det i en stålbox, som hon stänger och låser med hänglås och nyckel. Hon lämnar lådan med sitt hänglås på posten och behåller nyckeln, men när lådan når Bob kan han inte öppna den, eftersom han inte har någon nyckel till den. Alice kanske funderar på att stoppa nyckeln i en annan låda, låsa denna med hänglås och skicka iväg till Bob, men utan nyckel kan han inte heller öppna låda nummer två, och därför kan han inte få tag i nyckeln som går till den första lådan. Enda sättet att komma runt problemet tycks vara att Alice gör en kopia av sin nyckel och ger den till Bob i förväg när de träffas for att dricka kaffe.
Vi är tillbaka i samma gamla nyckeldistributionsproblem.
Vi föreställer oss följande scenario: Alice vill skicka ett ytterst personligt meddelande till Bob. Hon stoppar precis som förut sitt hemliga meddelande i lådan, låser med hänglås och skickar det till Bob. Men när lådan kommer fram, fäster han ytterligare ett hänglås i den och skickar tillbaka till Alice. När hon far lådan är den låst med två hänglås. Hon avlägsnarsitt eget hänglås, och Bobs lås är ensamt kvar. Sedan skickar hon tillbaka lådan till Bob som nu kan öppna den, eftersom den är låst enbart med hans eget lås.
Det verkar som om frågan om nyckeldistributionen här har lösts, eftersom metoden med dubbel kryptering inte fordrar någon utväxling av nycklar. Det finns dock ett principiellt hinder for den praktiska användningen av ett system där Alice krypterar, Bob krypterar, Alice dekrypterar och Bob dekrypterar. Vi far problem med turordningen. I allmänhet är den inbördes ordningen mellan olika krypteringar och dekrypteringar avgörande, enligt regeln "sist in, först ut".
De flesta matematiska funktioner kan klassificeras som tvåvägsfunktioner, eftersom de är lätta att lösa och lika lätta att kasta om och utföra i andra riktningen. En "dubblering" är till exempel en tvåvägsfunktion. Det är lätt att dubblera ett tal for att erhålla ett nytt tal, men det är lika lätt att avveckla, eller vända på, funktionen och gå från det dubblerade talet till det ursprungliga. Om vi vet att resultatet av dubbleringen är 26, kan vi lätt kasta om, avveckla, funktionen och härleda det ursprungliga talet, nämligen 13. Så vi behöver envägsfunktioner.
Ett mycket fruktbart matematiskt område som behandlar en sorts envägsfunktioner är den del av aritmetiken som rör modulera förmer. Inom den modulera aritmetiken behandlas en ändlig uppsättning tal som bildar en ögla, ungefär som siffrorna på en urtavla. En ring för modul 7, eller mod 7,som innehåller sju siffror från 0 till 6. Om vi beräknar (2 +6) och börjar på 2, flyttar vi 6 steg, vandrar varvet runt och hamnar på 1, vilket inte är det väntade resultatet inom den normala aritmetiken. Alltså kan vi skriva 2 + 6 = 1 (mod 7).



Vi kan till exempel undersöka den matematiska funktionen 3^x. Om x = 2, och vi löser funktionen, ser vi att $3^2 = 3 \times 3 = 9$. Funktionen har alltså förvandlat 2 till 9. Om vi alltså far reda på resultatet av funktionen är det tämligen enkelt att arbeta sig bakåt igen och härleda det ursprungliga talet. Låt oss säga att resultatet är 81. Då vet vi att x är lika med 4, eftersom

$3^4 = 81$. Även om vi räknar fel och gissar att x är lika med 5, kan vi genom att räkna ut att $3^5 = 243$ få reda på att vi valt ett för högt värde av x. Alltså väljer vi att minska x till 4 och får till slut det rätta svaret.
Inom den modulera aritmetiken uppför sig samma funktion inte lika ordentligt. Vi tänker oss att vi fatt reda på att $3^x \pmod 7$ är lika med 1. Vi får inte osökt något värde i tankarna, eftersom vi inte känner särskilt väl till de modulera formernas aritmetik. Vi försöker oss på en gissning att x = 5 och beräknar sedan resultatet av $3^5 \pmod 7$. Svaret visar sig vara 5, vilket är för högt, eftersom vi letar efter svaret 1. På grund av det svar vi fatt kanske vi frestas att minska värdet av x och försöka på nytt. Men då skulle vi faktiskt vara på väg i fel riktning, eftersom det rätta svaret är x = 6.
I vanlig aritmetik ökar värdet av funktionen kontinuerligt, medan det är oförutsägbart inom den modulera aritmetiken.

x	1	2	3	4	5	6
3^x	3	9	27	81	243	729
$3^x \pmod 7$	3	2	6	4	5	1

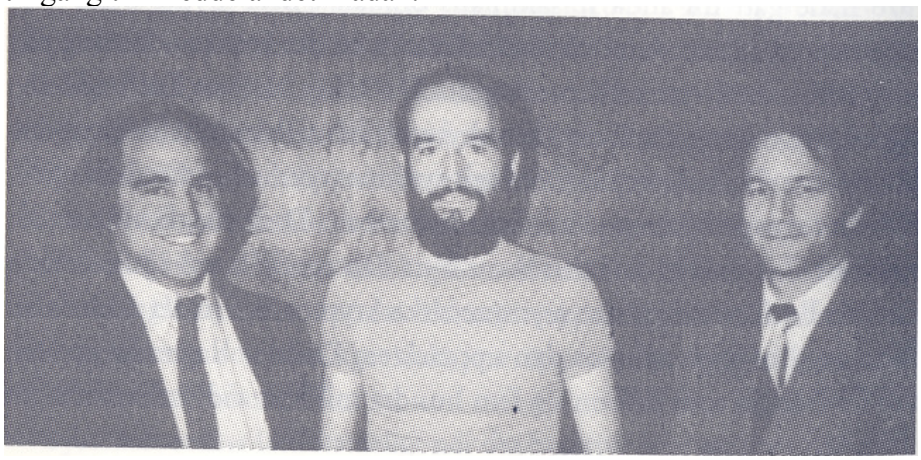
På den modulera aritmetikens område har vi inga ledtrådar till hjälp; det är förhållandevis mycket svårare att göra en omkastning aven funktion. Enda sättet är ofta att beräkna ett stort antal värden av x för funktionen i fråga och ställa upp dem i tabellform, tills man hittar det värde man letar efter. Så länge vi har att göra med någorlunda låga tal kan det möjligen vara en smula långtråkigt att skriva en tabell, men att behandla en funktion som $453^x \pmod{21\,997}$ skulle bli olidligt påfrestande. Det är ett klassisktexempel på en envägsfunktion: jag skulle kunna välja ett värde för x och räkna ut resultatet av funktionen, men om jag lämnade ut resultatet till en annan person, till exempel 5 787, skulle det vara mycket svårt för honom att göra en omkastning av förloppet för att försöka härleda mitt val av värde för x. Det tog bara ett par sekunder för mig att beräkna och få fram 5 787, men för den andre skulle det ta flera timmar att ställa upp tabellen och räkna ut mitt val av x.
Formeln är $y^x \pmod p$.
Till att börja med kommer Alice och Bob överens om värdena för *Y* och *P*. Det går bra med nästan vilket värde som helst, men med vissa begränsningar, däribland att *Y* måste vara mindre än *P*. Värdena är inte hemliga, och Alice kan alltså ringa Bob och föreslå att $Y = 7$ och $P = 11$.
Även om telefonlinjen inte är säker, utan Eve avlyssnarsamtalet, spelar detta ingen roll. Alice och Bob har alltså kommit överens om envägsfunktionen $7^x \pmod{11}$. På det här stadiet i proceduren ska de nu försöka bestämma en hemlig nyckel utan att träffas.
Låt oss undersöka systemet från Eves synpunkt. Om hon avlyssnar linjen får hon reda på följande, ingenting annat: funktionen är $7^x \pmod{11}$, och Alice skickar a = 2 medan Bob skickar b = 4. Vill hon ha reda på nyckeln måste hon antingen göra som Bob, förvandla a till nyckel genom att känna till *B,* eller också göra som Alice, förvandla b till nyckel genom att känna till *A*.
Men Eve känner inte till värdena för *A* och *B*. Det är inte dem Alice och Bob har utväxlat; de är fortfarande hemliga. Eve kan bara hoppas på en sak: rent teoretiskt skulle hon kunna räkna ut *A* ur a, eftersom a var det resultat som följde av att sätta in *A* i funktionen, den som ju Eve faktiskt känner till. Hon kan också räkna ut *B* ur b. Tråkigt nog för Eve är det en envägsfunktion; det är enkelt att förvandla *A* till a, eller *B* till b, men synnerligen besvärligt för Eve att vända på förfarandet särskilt om talen är höga.

Så här skulle Alice och Bob arbetar parallellt

	Alice	Bob
STEG 1	Alice väljer ett tal, t ex 3, och håller det hemligt. Hennes tal benämner vi A.	Bob väljer ett tal, t ex 6, och håller det hemligt. Hans tal benämner vi B.
STEG 2	Alice placerar in talet 3 i envägs funktionen och räknar ut resultatet av $7^A \pmod{11}$: $7^3 \pmod{11} = 343 \pmod{11} = 2$	Bob placerar in talet 6 i envägsfunktionen och räknar ut resultatet av $7^B \pmod{11}$: $7^6 \pmod{11} = 117\,649 \pmod{11} = 4$
STEG 3	Alice kallar resultatet av beräkningen a och skickar sitt resultat, 2, till Bob	Bob kallar resultatet av beräkningen b och skickar sitt resultat, 4, till Alice
BYTET	Vanligen är det känsligaste momentet just när Alice och Bob utväxlar information, eftersom Eve kan tjuvlyssna och utröna alla detaljer. Men det ska visa sig att Eve kan avlyssna samtalet utan att det påverkar systemets säkerhet. Alice och Bob kan mycket väl använda samma telefonlinje som då de kom överens om värdena för Y och P, och Eve får gärna uppsnappa vilka två tal som utväxlas, 2 och 4, ty de utgör ju inte nyckeln! Därför gör det ingenting om Eve känner till dem.	
STEG 4	Med hjälp av Bobs resultat beräknar Alice resultatet av $b^A \pmod{11}$: $4^3 \pmod{11} = 64 \pmod{11} = 9$	Med hjälp av Alices resultat beräknar Bob resultatet av $a^B \pmod{11}$: $2^6 \pmod{11} = 64 \pmod{11} = 9$
NYCKELN	Som genom ett under har Alice och Bob till slut erhållit samma tal, 9. Detta blir nyckeln!	

Alla krypteringsmetoder som hittills beskrivits i boken har varit symmetriska, vilket betyder att utredningsproceduren helt enkelt är spegelvänd mot förvrängningen. Till exempel använde Enigma maskinen en viss nyckelinställning för att kryptera ett budskap, och mottagaren använde en likadan maskin med samma inställning för att dekryptera det. Sändaren och mottagaren vet i sak detsamma, de använder samma nyckel för både kryptering och dekryptering; det vill säga att förhållandet dem emellan är symmetriskt. Men i ett asymmetriskt system är, precis som namnet antyder, krypteringsnyckeln och dekrypteringsnyckeln däremot inte identiska. När Alice använder ett asymmetriskt krypto kan hon med andra ord kryptera sitt budskap om hon känner till krypteringsnyckeln, men hon kan inte dekryptera något meddelande. Vill hon dekryptera måste hon ha tillgång till den särskilda

dekrypteringsnyckeln. Att krypterings- och dekrypteringsnyckeln skiljer sig åt är just poängen i det asymmetriska kryptot. Alice skulle förstås skapa sig ett eget nyckelpar, en för krypteringen och en för dekrypteringen. Om vi utgår från att det asymmetriska kryptot är en sorts datorkryptering, är hennes krypteringsnyckel ett visst tal, och dekrypteringsnyckeln ett annat tal. Hon håller dekrypteringsnyckeln hemlig. Den kallas därför vanligen privat nyckel. Däremot offentlig gör hon krypteringsnyckeln så att alla får tillgång till den. Det är därför man brukar kalla den publik eller öppen eller offentlig nyckel. Om
Bob vill skicka ett meddelande till Alice letar han bara upp hennes publika nyckel. Sedan krypterar han sitt meddelande med hjälp av Alices publika nyckel och skickar det till henne. När hon får det kan hon tolka det med hjälp av sin privata dekrypteringsnyckel. På samma sätt kan
Carl, Emma eller William, om de skulle vilja skicka ett hemligt meddelande till Alice, slå upp hennes krypteringsnyckel, och hela tiden är Alice den enda som har tillgång till den privata nyckeln och kan dekryptera meddelandena. För att återgå till liknelsen med hänglåset skulle vi kunna tänka oss asymmetrisk kryptografi på följande sätt. Vem som helst kan stänga ett hänglås genom att helt enkelt klämma ner bygeln med ett klick, men bara den som har nyckeln kan öppna det igen. Att låsa (kryptera) är lätt, och alla klarar av det, men att låsa upp (dekryptera)är möjligt bara för den som äger nyckeln. Den grundläggande kunskapen om hur man klämmer ner bygeln så att låset stängs talar om ingenting om hur man ska låsa upp det. Vi kan utsträcka liknelsen och tänka oss att Alice konstruerar ett hänglås och en nyckel. Hon behåller nyckeln för sig själv men tillverkar tusentals exemplar av hänglåset och skickar ut dem till postkontor överallt i världen. När Bob vill skicka ett meddelande stoppar han det i en låda, går till postkontoret, ber om ett 'Alicehänglås' och låser lådan med det. Nu kan inte ens han låsa upp lådan, men då Alice far den kan hon öppna den med sin enda, unika nyckel. Hänglåset och låsningsförfarandet motsvarar den öppna krypteringsnyckeln, eftersom alla har tillgång till hänglås och kan låsa in ett meddelande i lådan. Hänglåsnyckeln motsvarar den privata dekrypteringsnyckeln, eftersom Alice är den som äger den, kan öppna låset och få tillgång till meddelandet i lådan.



Ronald Rivest Adi Shamir Leonard Adleman.

Systemet, som fick namnet RSA (Rivest, Shamir, Adleman) blev så småningom det krypto som fått störst betydelse av alla inom modern krypteringsteknik. Kärnan i Rivests asymmetriska krypto är en envägsfunktion som är baserad på moduler funktioner. Med hans envägsfunktion kan man kryptera ett budskap genom att det översätts till ett tal, som placeras i funktionen, och resultatet blir ett annat tal. Detta tal utgör kryptotexten. N är viktig, ty den är en variabel beståndsdel i envägsfunktionen. Det betyder att var och en kan välja sitt eget värde av N och alltså skaffa sig en personlig envägsfunktion. När Alice ska bestämma sitt eget N värde väljer hon ut två primtal, som vi kan kalla p och q, och multiplicerar dem. Alice

kanske väljer ut åt sig primtalen p = 17 159 och q= 10 247. Hon multiplicerar dem och får fram
N = 17 159 x 10 247 = 175 828 273.
Alicesval av N blir hennes offentliga krypteringsnyckel, som hon låter trycka på sina visitkort, skickar ut på nätet. Om Bob tar lust att kryptera ett brev till Alice letar han upp hennes värde för N (175 828 273) och sätter in det i den allmänna formel som envägsfunktionen utgör. Även den känner alla till. Nu har han en envägsfunktion som är skräddarsydd efter Alices öppna nyckel; man skulle kunna kalla den för Alices envägsfunktion. När han krypterar sitt brev till Alice placerar han det, omvandlat till siffror, i hennes envägsfunktion, noterar resultatet och skickar det till henne. I det här skedet är det krypterade meddelandet säkert, och ingen kan dekryptera det. Eftersom det har krypterats med hjälp aven envägsfunktion, är det per definition mycket besvärligt, för att inte säga omöjligt, att vända funktionen åt motsatt håll och dekryptera brevet. Men då är frågan: hur ska Alice själv kunna dekryptera det? För att kunna läsa sina brev måste hon faktisktvända på sin envägsfunktion. Hon måste sitta inne med en liten extra hemlighet som hjälper henne att tolka brevet.
Till all lycka för Alice utformade Rivest sin envägsfunktion så att den blev reversibel för den som kände till värdena av p och q, de två primtal som man multiplicerar för att få fram N. Alice har talat om för alla människor att hennes värde för N är 175 828 273, men vad hon inte har yppat är värdena för p och q. Hon har alltså den extra kunskap som behövs för att dekryptera de egna meddelandena.
Vi kan betrakta N som den offentliga nyckeln, upplysningen som är tillgänglig för alla, och som behövs för att kryptera budskap till Alice.
Om alla känner till N, den offentliga nyckeln, kan de väl räkna ut p och q, den privata nyckeln, och läsa Alices brev? N är ju faktiskt framtagen ur p och q, en produkt av dem. Men nu förhåller det sig så, att om N är ett tillräckligt högt tal är det i realiteten omöjligt att härleda p och q, och häri ligger själva finessen med det asymmetriska RSA kryptot.
Det asymmetriska kryptosystemet RSA är en form av kryptering med öppen nyckel [kallas ofta helt enkelt public key kryptering]. För att få reda på hur säkert RSA är kan vi lämpligen betrakta systemet ur Eves synvinkel och försöka knäcka ett meddelande från Alice till Bob. För att kryptera sitt budskap letar Alice upp Bobs offentliga nyckel. Som är N=408508091 hon stoppar in det i den allmänna envägsfunktionen och krypterar sitt brev. När det trillar in i Bobs brevlåda kan han köra funktionen baklänges genom att han sitter inne med värdena p och q, hans egen privata nyckel.
Han dekrypterar så sitt budskap. Samtidigt har Eve uppsnappat meddelandet på vägen. Hennes enda chans att kunna dekryptera det är att kasta om envägsfunktionen, vilket bara är möjligt om hon känner till p och q. Bob har behållit dem för sig själv, men Eve vet lika väl som alla andra att hans värde för N är 408508 091. Hon försöker då räkna ut värdena av p och q genom att beräkna vilka primtal man ska multiplicera med varandra för att erhålla 408 508 091, en räkneoperation som kallas faktorisering, uppdelning i faktorer. Sådan faktorisering kan vara mycket tidskrävande. Hur lång tid skulle det ta för Eve att hitta faktorerna till 408 508 091? Det finns ett antal sätt att dela upp N i faktorer. Somliga är visserligen lite smidigare än andra, men i sak måste Eve gå igenom vartenda primtal och kontrollera om N kan divideras med det utan att man far någon rest. Talet 3 är tillexempel ett primtal, men är trots det ingen faktor till 408 508091 eftersom man far en rest vid divisionen. Därför går Eve till nästa primtal, 5. Inte heller det tillhör faktorerna vi söker, så hon går till nästa, och så vidare. Till slut kommer hon till 18 313, det tvåtusende primtalet i ordningen, och det råkar faktiskt vara en av faktorerna. Hittar hon en faktor är det lätt att hitta den andra, vilken visar sig vara 22 307.
Om Eve har en miniräknare eller ett kalkylprogram i datorn och kan kontrollera fyra primtal i minuten, skulle det ta henne fem hundra minuter, drygt åtta timmar, att få fram p och q. Hon

skulle alltså kunna räkna ut Bobs privata nyckel på mindre än en dag och dekryptera ett uppfångat meddelande inom den tidsramen.
Säkerhetsnivån är alltså inte särskilt hög, men om Bob väljer två riktigt höga tal kan han göra den privata nyckeln säkrare. Han kan till exempel välja primtal i klassmed 10^{65} (vilket betyder att ettan följs av 65 nollor). Det skulle resultera i ett värde för N som skulle ligga omkring 10^{65}x 10^{65} =10^{130}. Med datorns hjälp kan man multiplicera de båda primtalen och få fram N på bara några sekunder, men om Eve vill vända på förloppet och räkna ut p och q skulle det ta omåttligt mycket längre tid. Precis hur mycket längre beror på hur snabb Eves dator är. Säkerhetsexperten Simson Garfinkel har beräknat att det skulle ta uppskattningsvis runt femtio år för en 100MHz Intel 8MB Pentium-dator att faktorisera ett så högt tal som 10^{130}
Följaktligen är det nu allmänt accepterat att man för att uppnå verklig säkerhet måste använda ännu högre primtal. För riktigt viktiga bankärenden är det bäst att N är åtminstone 10^{308}, vilket är cirka en miljon miljarder miljard miljarder miljard miljarder miljard miljarder miljard miljarder miljard miljarder miljard miljarder miljard miljarder miljard miljarder miljard miljarder större än 10^{130}. Om etthundra miljoner datorer förenade sina krafter skulle det ta mer än ett tusen år att knäcka ett sådant chiffer. Kort sagt, om värdena av p och q är tillräckligt höga är RSA motståndskraftigt mot alla attacker.
Krypteringsmeddelande är teckensträngar av karaktärer som är översatta till siffror. Dessa siffror krypteras men denna öppna nyckeln till andra siffror och sedan skickas .
Det är endast dekrypteringsnycklarna som hålls hemliga och bara den som är menad att få meddelandet kan dekryptera det.
För att kryptera meddelandet ”STOP” med hjälp av krypteringssystem där $p = 43$, $q = 59$, det betyder att $n = 43 * 59 = 2537$ och med $e = 13$.
gcd(e, (p – 1)(q – 1)) = gcd(13,42 * 58) = 1.

Lösning: Vi översätter bokstäverna i ”STOP” till deras numeriska ekvivalenter och sedan grupperar vi numrena i block om fyra. Vi får då;
1819 1415

Vi krypterar varje block genom att använda funktionen;
$C = M^{13}$ **mod** 2537.
Beräkningar med hjälp av multiplikation visar att 1819^{13} **mod** 2537 = 2081 och 1415^{13} **mod** 2537 = 2182. Det betyder att meddelandet är 2081 2182.
Meddelandet kan snabbt återskapas när dekrypteringsnyckeln *d*, en invertering av e mod (p – 1)(q – 1), är känd.

Vi får det krypterade meddelandet 0981 0461. Meddelandet är krypterat med hjälp av krypteringssystem när $n = 2537$ och $e = 13$ och $d = 937$ är en invertering av 13 **mod** 4259 = 2436. Vi använder 937 som vår dekrypteringsexponent. Följaktligen, för att dekryptera block C beräknar vi $P = C^{937}$ **mod** 2537.
0981^{937} **mod** 2537 = 0704 och 0461^{937} **mod** 2537 = 1115. Det betyder att det ursprungliga meddelandet är 0704 1115. Översätter vi detta block till engelska bokstäver så ser vi att meddelandet är ”HELP”.
Här beskrivas hur RSA-kryptering och dekryptering rent matematisk går till.
Kryptering.
Om Bob ska skicka ett meddelande till Alice.
Alice väljer sina primtal p=17 q=11(de är hennes privata nycklar).
Nu kan hon publicera N ,som är p*q, hon behöver att publicera ett tal till e= 7
(e och (p-1)(q-1)ska vara relaterade primtal)(N och e är hennes publika nycklar).

Man förvandlar budskap till ett tal M. Nu ska vi använda ASCII-koder och betrakta den som ett decimaltal. Talet M krypteras sedan och ger kryptotexten $C = M^e (\text{mod } N)$.
Om Bob vill skicka en kyss till Alice, bokstaven X, och i ASCII betecknas den med 1011000 vilket motsvarar 88 enligt decimalsystemet. M =88.
Formeln blir $C = 88^7 (\text{mod} 187)$.
För att beräkna exponentialfunktioner i moduler aritmetik gör Bob så
$88^7 (\text{mod} 187) = 88^4 (\text{mod} 187) * 88^2 (\text{mod} 187) * 88^1 (\text{mod} 187)$

$88^1 = 88 = 88 (\text{mod} 187)$
$88^2 = 7744 = 77 (\text{mod} 187)$
$88^4 = 59969536 = 132 (\text{mod} 187)$
$88^7 = 88^1 * 88^2 * 88^4 = 88 * 77 * 132 = 894432 = 11 (\text{mod} 187)$

Bob skickar kryptotexten c=11 till Alice.
Dekryptering.
d, dekrypteringsnyckeln, beräknas från p och q.
$e*d = 1 (\text{mod}(p-1)*(q-1))$
$7*d = 1 (\text{mod } 16*10)$
$7*d = 1 (\text{mod } 160)$
d=23.
Formeln för dekryptering är
$M = C^d (\text{mod} 187)$
$M = 11^{23} (\text{mod} 187)$
$M = 11^1 * 11^2 * 11^4 * 11^{16} (\text{mod} 187)$
$M = 11*121*55*154 (\text{mod} 187)$
M = 88= X i ASCII.

3. Analys av material

Böckerna ”Discrete mathematics and its applications”, ” Matematikens historia” och ”Kodboken” vara relativt lätta att förstå men ”Chinese Remainder Theorem” var dock betydligt svårare. I den svårare boken fanns det även skriv- och räkningsfel som förvirrade ytterligare. Boken kräver också mycket erfarenhet för att man helt och fullt ska kunna förstå boken. Jag har använt exempel från alla böckerna för att kunna underlätta förståelse av denna uppsats. Uppgifter från Internet gav ytterligare information inom ämnesområdet.

3.1 Reliabilitet och validitet

Jag anser att böckernas information är tillförlitlig och beskriver det de avser att beskriva. Uppgifter från Internet verkar även de vara tillförlitliga de också då de överensstämmer med böckernas information.

4. Avslutning

Jag har kommit fram till att Chinese Remainder Theorem är ett viktigt teorem som trots att det upptäcktes för länge sedan även är användbar i modern tid.

5.Källförteckning

Rosen, Kenneth H. (1999), *Discrete mathematics and its applications*, 4th ed, McGraw-Hill Book Co, Singapore

C. Ding, D. Pei och A. Salomaa (1996), *Chinese Remainder Theorem*, World Scientific Publishing Co. Pte. Ltd., Singapore

Johansson, Bo Göran (2004), *Matematikens historia*, Studentlitteratur AB, Sverige

Singh, Simon (1999), *Kodboken,* Norstedts Förlag, Stockholm

Internet:

http://www.math.sfu.ca/histmath/China/3rdCenturyBC/STSC.html

http://www.math.mtu.edu/mathlab/COURSES/holt/dnt/chinese.html

http://encyclopedia.laborlawtalk.com/Chiese_remainder_theorem

http://www.chinapage.com/math/crt.html

http://www.mtm.ufsc.br/~andsol/english/mat/china.html

http://www.abacus.ca/abacus-images.php