Världens första kryptomaskin

Den första mekaniska apparaten för att underlätta och säkerställa chifferarbetet gjordes - såvitt känt är - i Sverige. Den presenterades år 1786 i ett brev till Gustav III från den i uppfinnarsammanhang okände friherren och före detta officeren Fredrik Gripenstierna. En bevarad räkning visar att denna chiffer-maskin kostade 130 riksdaler specie att tillverka.

Själva maskinen är försvunnen och likaså ritningarna till den. Att den överhuvudtaget existerat visste man i vår tid inte förrän en forskare i svensk underrättelsehistoria på 1970-talet fann spåren i Riksarkivet. Där påträffades ett omslag med beteckningen "Förslag till Chiffre-Machine", vari fanns handlingar som beskrev "inventionen".

Upptäckaren av dokumentet heter Sven Wäsström. Sedan Sven Wäsström under större delen av sitt yrkesverksamma liv sysslat med kryptofrågor vid Försvarets radioanstalt har han efter sin pensionering ägnat sig åt historisk - i synnerhet underrättelsehistorisk forskning.

I nedanstående framställning står Sven Wäsström för skildringen av det historiska sammanhanget medan Bengt Beckman står för den kryptologiska beskrivningen av maskinen. Det underlag Crypto AG i Zug i Schweitz använde sig av i slutet av 1970-talet för att tillverka två Gripenstierna-maskiner tillkom i sammarbete mellan dessa båda.

I den skrivelse till Gustav III, i vilken Gripenstierna mycket underdånigt presenterar sin invention, säger han: ".... af mig uppfunnen - i stöd af de grunder jag i min ungdom inhämtat af min morfader, framlidne komerserådet och kommendören Christopher Polhem...".

Christopher Polhem , den svenska teknikens nationalhelgon, var en mångsidig begåvning, känd bl.a. som uppfinnare av polhemslåset, malmuppfodringsverk, vävstolar, stickmaskiner och pendelur. Genom resor och korrespondans hade Polhem kontakt med tidens stora inom kryptologi och besläktade områden, såsom Wilkins, Wallis och Leibniz. I likhet med dessa hade han också ett stort intresse för språkliga konstruktioner och olika former av konstgjorda språk. Polhem skulterade ett "tekniskt alfabet", som finns att beskåda på Tekniska museet.

Han hade också studerat Kircher, en jesuit och månglärd professor, som 1633 publicerade en skrift benämnd Abacus Numeralis. I denna beskrivs den kryptologiska ide som 1786 års maskin bygger på.

Troligen under sommaren 1786 presenterar Fredrik Gripenstierna sin uppfinning för konungen. Handlingen är odaterad men försedd med en stämpelavgift. I skrivelsen finns ingen antydan om att Gustav III orienterats om uppfinningen tidigare. Tillfälle till detta hade annars funnits genom att Gripenstierna deltog i riksdagen på våren 1786 och alltså ganska nyligen sammanträffat med konungen.

Även i för dåtiden devota ordalag erbjuder han sin uppfinning som han entusiastiskt beskriver:

- varje klartecken hade 1539-2000 olika representationer i kryptotexten, - apparaten kunde förses med ett mekaniskt lås vilket förhindrade obehörig insyn i de kryptotekniska funktioner den dolde, - klartext kunde ställas in på den ena sidan av den på ett bord uppställda maskinen, varvid kryptotexten automatiskt framträdde på den andra sidan. Den där placerade medhjälparen kommer inte i kontakt med klartexten utan kan avskriva kryptotexten och vidarebefodra den sålunda färdigställda depeschen. Ankommande kryptodepescher behandlas analogt i ett motsatt förfarande.

Tanken att förhindra obehörig insyn återfinns i den polhemska vintappningsapparat, vars ide är att husbonden ska kunna tappa vinet direkt från den låsta vinkällaren utan inblandning av obehörigt tjänstefolk.

Gripenstierna erbjuder sig föranstalta om tillverkning av en sådan maskin samt beskriver den inre hemliga kryptofunktionen, vilken ej framgår av den ritning som Gripenstierna inledningsvis säger sig bilägga men som tyvärr saknas i arkivhandlingarna.. (Sannolikt lämnades den till tillverkaren av prototypen). Gripenstierna avslutar sitt brev med följande:

"Men så framt Eders Kongl Maijt i nåder icke finner för godt att Inventionen antaga, så utbeder jag mig dock,

såsom vedermäle af Kongl Nåd, att få till något främmande Hof upplåta denna af mig uppfunde Chiffre-Clav."

Men Gustav III blev intresserad i så måtto att han lät Gripenstierna ombesörja tillverkandet av en prototyp. Den 26 augusti 1786 utställde och kvitterade så firma Charles Apelquist en räkning på Fredrik Gripenstierna för tillverkandet av en mekanisk chiffermaskin. Tillverknngskostnaden, som får betraktas som synnerligen hög, utgjorde 130 Riksdaler specie. Samma dag sände Gripenstiera räkningen vidare till expeditionssekreterare Frank (svensk handläggare av utrikespolitiska ärender) med en hemställan att få ersättning för utlägget och en försäkran att han erhållit maskinen. Det kan nämnas att firman Charles Apelquist i andra sammanhang inte var tadelfri, utan bl.a. var anklagad för att förfalska sedlar.

I en odaterad skrivelse, förmodligen skriven samtidigt med ovannämnda, anmäler Gripenstierna till Gustav III att maskinen är färdig.

" Stormägtigste Allernådigste Konung! Efter Allernådigste Befallning har jag nu förfärdigat en Chiffre-Clav, och som jag högeligen önskar, att den måtte vinna Eders Konglige Majestäts Nådigaste Approbation; så utbeder jag mig den Nåde, att inför Eders Konglig Majestät, få den samma i underdånighet uppvisa. Med underdånigste Zele och Soumission, har jag nåden, att intill dödsstunden framhärda, Stormägtigste Allernådigste Konung, Eders Konglig Majestäts, Allerunderdånigste Tropligtigste Tienare och undersåte Fridric Gripenstierna "

Och en månad senare får Gripenstierna tillfälle att demonstrera sin uppfinning för konungen. Den beskrivning eller, för att använda en modernare term, den manual, som Gripenstierna utlovat i sin första skrivelse föreligger nu i elegant präntad form. Den bär titeln: "Beskrifning som utvisar, huruledes den af undertecknad inrättade Chiffre-Machinen kan nyttias till Chiffrering och Dechiffrering". Akten är dagtecknad Drottningholm den 23 september 1786. Samtidigt omnämnes en bilagd tabell, "som till Chiffre-Machinens bruk inrättad är", men som tyvärr saknas. Dessutom föreligger i aktsamlingen några chifferexempel, varav möjligen något överlämnats vid tidigare tillfälle.

Säkerligen skedde demonstrationen i anslutning till ovannämnda datum. Därefter är allt tyst om Gripenstiernas invention. Trots reltivt ambitiösa efterforskningar har några spår ej erhållits, vare sig av maskinen som sådan eller av dess användning i den diplomatiska korrespondensen. Säkerligen kom den aldrig till användning och tillverkades bara i ett enda exemplar.

Polhems dotter var gift med Carl Gripenstierna, kammarherre hos änkedrottning Hedvig Eleonora och innehavare av Kersö Herrgård på Ekerö. Efter sin hustrus död 1735 flyttade Polhem ut till sin dotter på Ekerö och stannade där till 1744 då han vid 74 års ålder flyttade till Stockholm. Dottersonen Fredrik var då 16 år. De hågkomster Gripenstierna kunde ha kvar från denna tid var alltså 44 år gamla. Till saken hör att gården brann år 1755 och dokumenten som rörde maskinen kan ha blivit lågornas rov.

Gripenstierna tillbringade i 17-18 årsåldern en kortare tid vid Uppsala universitet, varefter han sökte sig in på den militära banan, vilken kröntes med en befattning som fortifikationofficer vid Sveaborg 1748. Han avslutade sin militära bana som kunglig livdrabant vid 24 års ålder. Han upphöjdes 1755 tillsammans med brodern till friherre - möjligen för att soulagera släkten i en ekonomisk tvist med Kronan och han tillbringade återstoden av sitt liv som godsägare samtidigt som han innehade den föga arbetskrävande befattning som hovjägmästare. Han dog 1804.

Det är inte mycket i Gripenstiernas kända liv som gör det troligt att han är chiffermaskinens egentlige upphovsman, han hänvisar ju också själv i sitt första brev till Polhem. Det är mycket som talar för att man bör tala om "Polhems chiffermaskin som lanserades av Fredrik Gripenstierna". Men det är möjligt att Gripenstierna lagt ned tankemöda på att utfundera det användningssätt för maskinen som föreskrives.

"Chiffre-Machinen" är till sin grundide inte särskilt komplicerad, men i användarinstruktionen är inlagt flera komplikationer för att stärka kryptosäkerheten. Här skall ges en bild av såväl grundiden som komplikationerna samt några reflexioner om kryptosäkerhet.

Maskinen bestod av 57 hjul uppträdda på en gemensam axel. De var inneslutna i en långsträckt cylinder. På varje hjuls halva periferi var bokstäverna ingraverade i alfabetisk ordning medan den andra halvan upptog tal mellan 0 och 99 i oordning. På vardera långsidan av cylindern fanns en längsgående öppning i vilken man på hjulens bokstavssida kunde ställa in ett klartextavsnitt om maximalt 57 tecken. På motsatta sidan kunde man samtidigt i en liknande öppning avläsa 57 tal som utgjorde kryptotexten.

Apparaten var - som tidigare nämnts - gjord att betjänas av två man; den behörige ämbetsmannen som sätter in klartexten, medan den obehörige - sekreteraren - skriver av kryptotexten. Vid dechiffreringen sätter sekreteraren in kryptotexten men får aldrig se klartexten.

Varje hjul har sin specifika oordning på talen och en bokstavs siffermotsvarighet är alltså beroende av med vilket hjul den är chiffrerad, d.v.s. vilken plats på raden den har. Sedan en rad chiffrerats sätts ett nytt klartextavsnitt in och skrivs av och så forsätter man tills hela texten är chiffrerad. Kryptotexten skulle alltså få perioden 57 om man rakt igenom texten endast använde fullständiga rader. Så var det emellertid inte tänkt.

Att man skulle kunna sluta chiffreringen var som helst på raden är naturligt, men man skulle också - enligt Gripenstierna speciella föreskrifter - variera den plats på raden där man började sin chiffrering. Denna plats skulle anges i början på varje rad i chiffertexten. För ändamålet fanns två möjligheter:

a) att använda Claven K, som bestod av en rad av nio vokaler som var präglade på en mässingsskiva ovanför den längsgående öppningen på maskinens hölje eller

b) att använda Claven C som stod på en rad under den förutnämnda och bestod av det fullständiga alfabetet. Användes Claven K skulle vid radbyta det första ordets första vokal ställas in på det hjul som återfanns direkt under denna vokal på mässingsskivan. Användes Claven C skulle man ställa in förstaordets begynnelsebokstav under motsvarande bokstav i alfabetsraden. I båda fallen skulle man blankställa det hjul som satt närmast till vänster om begynnelsehjulet. På maskinens siffersida fanns på höljet tal som utgjorde kodnummer för de bokstäver man rättade sig efter. Kryptosekreteraren skall, sedan han från vänster till höger skrivit av den chiffrerade raden, ange kodnummer för det hjul som begynner raden och vilken han kan identifiera genom att det närmaste hjulet är blankt även på siffersidan.

Eftersom den som sätter in klartexten gör det från vänster till höger och den, som på motsatta sidan av chifferapparaten nedtecknar chiffertexten, också skriver från vänster till höger, innebär det att chifferraderna i själva depeschen kommer baklänges i förhållande till klartexten. När mottagardekryptören sätter in chifferraderna kommer de ju åter rätt för klartextläsaren.

Man tror gärna Gripenstierna när han skriver: "Ehuruväl att detta alt, kan lättare uppå Chiffre-Machinen demonstrerats, än uppå papper beskrivas".

Gripenstierna säger att maskinen totalt innehåller 1539 förändringar av bokstäver, "af hvilket uppkommer en ovedersägelig Omöjelighen, att någonsin kunna uträkna Bokstäfvernas Valeur uti Chiffre". Talet 1539 innebär 27 bokstäver på vart och ett av de 57 hjulen och lika många motsvarigheter i siffror. Därtill skall tilläggas ett par skiljetecken och en symbol för ordskillnad och en för "blankt". Gripenstierna har ingenstans i de bevarade papperen angivit sitt klartexts-alfabet, men av hans textexempel att döma bör det minst ha omfattat följande: ABCDEFGHIJKLMNOPQRSTUVYZÅÄÖ samt tecken .,- # (för ordskillnad och för # "blankt").

Att det är en ovedersäglig omöjlighet att knäcka det hela det är naturligtvis en överdrift, men helt enkelt skulle det inte vara för den som ville forcera depescher som chiffrerats med Gripenstiernas maskin.

Kryptosystemet kan fackmässigt beskrivas som ett substitutionschiffer med flera oordnade alfabet. Fleralfabetssystem brukar kallas vigenere efter diplomaten Vigenere som år 1586 beskrev sådana system. Skall man precisera kryptotypen även med hänsyn till möjligheten att variera radlängden kan man säga att Gripenstiernas maskin producerade ett krypto av typen "Oordnad vigenere med stammande nyckel".

För att fullständigt klarlägga maskinen skulle en forcör behöva rekonstruera 57 oordnade alfabet om minst 30 tecken i varje - något som kräver att han har tillgång till mer än 100 chiffrerade rader. Innan han tar itu med rekonstruktionen måste han ha alla rader i rätt utgångsläge - i det fallet har han dock god hjälp av den vid varje rad angivna indikatorn. Sist och slutligen måste han för att kunna läsa klartext komma underfund med att varje rad i depeschen är skriven baklänges!

Tar man i beaktande den sparsamma diplomatiska trafik som förekom vid den här tiden kan man utan tvekan säga att maskinen hade en mycket god kryptosäkerhet. Nedan återges första raden i kryptotexten omvänd och med första nyckelhjulets kodnummer angivet (det är bara i första raden som K föregår kodnummer) Påläggstext inpassad:

K36 s t o r m ä g t i g s t e

02 22 63 51 04 07 29 59 90 97 89 14 47

Huruvida Gripenstierna placerat ut talen helt slumpmässigt på hjulen eller om han gjort det enligt något system är inte undersökt, men den som lyckas placera in hela pålägget har ju möjlighet att bilda sig en uppfattning även om den saken. Texten torde dock vara för kort för att man skall kunna komma till några säkra slutsatser.

Bazeries cylinder

Den s.k. Bazeries cylinder, uppfunnen av fransmannen Etienne Bazeries år 1891, påminner något om Gripenstiernas krypto, men Bazeries cylinder är listigare. Den är genialisk i sin enkelhet. 25 hjul, vart och ett omfattande ett ordnat alfabet, är uppträdda på en axel. Kryptören sätter in ett klartextavsnitt och läser på valfri rad på cylindern av en kryptotext. Vid dekryptering sätts kryptotexten in och någonstans på cylindern skall då finnas ett klartextavsnitt på 25 bokstäver.

Man har funnit att den amerikanske statsmannen, sedermera presidenten, Thomas Jefferson, hundra år tidigare hade utvecklat samma ide men att den då ej kommit till användning utan förfallit i glömska. Principen användes av amerikanarna under andra världskriget och instrumentet kallades M-94.

När Sven Wäsström berättade för den gamle kryptomaskintillverkaren Boris Hagelin om Gripenstiernas maskin, blev han intresserad och lät Crypto AG i Zug tillverka två exemplar. Det ena står i firmans entrehall med beteckningen "Gustaf den III Adolfs chiffermaskin". Det andra exemplaret finns som gåva av Sven Wäsström i Försvarets radioanstalts interna museum.

Publicerat 2003-06-05.