Hyväksymispäivä Arvosana

Arvostelija

Colossus

Samu Varjonen

Helsinki 10.3.2005

Helsingin Yliopisto

Tietojenkäsittelytieteen laitos

Tekijä – Författare - Author
Samu Varjonen

Työn nimi – Arbetets titel - Titel
Colossus

Oppiaine- Läroämne – Subject
Tietojenkäsittelytiede

Työn laji – Arbetets art – Level	Aika – Datum – Month and year	Sivumäärä –Sidoantal–Number of pages
	10.3.2005	12

Tiivistelmä – Referat – Abstract

Toisen maailmansodan aikana Bletchley Parkissa lähellä Lontoota murrettiin saksalaisten salakirjoittamia viestejä. Tätä työtä pidettiin niin tärkeänä, että Bletchley Parkin olemassaolo salattiin vuoteen 1974 asti. Ehkä suurimpana salaisuutena vuonna 1974 paljastui Colossuksen olemassaolo. Colossus oli ohjelmoitava digitaalinen logiikkalaskin, jota käytettiin pääasiassa saksalaisten käyttämän Lorenz-salakirjoituksen murtamiseen. Colossus oli työkalu, jonka sanotaan lyhentäneen sotaa, koska sen avulla saatiin selville Hitlerin aikeet juuri ennen liittoutuneiden maihinnousua Normandiaan. Colossus sai nimensä suoraan koneen kolossaalisesta koosta. Ensimmäisessä Colossus Mk I versiossa kone koostui 1500 elektroniputkesta, mutta seuraava Colossus Mk II versio koostui 2500 elektroniputkesta. Colossuksia rakennettiin julkaistujen tietojen mukaan noin kymmenen, joista yksi tai kaksi pidettiin käytössä vuosien 1958 ja 1960 välille, jonka jälkeen ne ilmeisesti tuhottiin. Voimme vain arvailla kuinka Colossus olisi voinut muuttaa nykypäivän käsitystä tietojenkäsittelystä ja tietokoneista. Colossuksella voidaan todeta olleen toisen asteen vaikutuksia tietokoneiden kehitykselle, vaikka sen olemassaolo salattiinkin. Työntekijät, jotka olivat osallisia Colossuksien suunnittelussa ja rakentamisessa Bletchley Parkissa ja Dollis Hillissä, saivat merkittävän kokemuksen elektronisten tietokoneiden rakentamisen saralla. Osa työntekijöistä siirtyi sodan jälkeen suoraan seuraavien tietokoneiden rakentamiseen ja koska heillä oli kokemusta asiasta pystyivät he aloittamaan suunnittelun ja rakentamisen paljon korkeammalta tasolta kuin heidän siviili vastakohtansa. Näin ollen he pystyivät tuomaan elektroniikan tuntemuksellaan siviilipuolen kehitystyöhön uusia ajatuksia.

ACM Computing Classification System (CCS):
A.0 General
K.2 History of computing
E.3 Data encryption

Avainsanat – Nyckelord – Keywords
Colossus, Enigma, Fish, Flowers, Good, Lorenz, Newman, Tunny, Tutte

Säilytyspaikka – Förvaringsställe – Where deposited

Muita tietoja – Övriga upgifter – Additional information
Tietojenkäsittelytieteen historia –seminaarin alustus.

Sisältö

1 Johdanto

Toisen maailmansodan aikana Bletchley Parkissa lähellä Lontoota murrettiin saksalaisten salakirjoittamia viestejä. Tätä työtä pidettiin niin tärkeänä, että Bletchley Parkin olemassaolo salattiin vuoteen 1974 asti. Suurin osa siellä tehdyistä keksinnöistä oli salaisena vielä vuoteen 1995. Vuoden 1974 jälkeen julkaisi Iso-Britannia hiljalleen dokumentteja Bletchley Parkissa tehdystä työstä. Dokumenttien määrä ei ole suuri, koska toisen maailmansodan jälkeen valtaosa dokumenteista ja laitteistoista tuhottiin Winston Churchillin komennosta. Siinä määrättiin koneet purettavan uudelleen käytettäviin osiin ja loput nyrkkiä pienemmiksi paloiksi. Kuitenkin osa dokumenteista säilyi, koska työntekijät säilyttivät niitä itsellään vastoin määräyksiä. Suurin osa tämän työn tekemiseen käytetyistä artikkeleista on Colossuksen tekijöiden kirjoittamia tai heidän haastatteluidensa pohjalta kirjoitettuja.

Ehkä suurimpana salaisuutena vuonna 1974 paljastui Colossuksen olemassaolo. Colossus oli ohjelmoitava digitaalinen logiikkalaskin, jota käytettiin pääasiassa saksalaisten käyttämän Lorenz-salakirjoituksen murtamiseen. Lorenz-salakirjoitusta käytettiin Saksan armeijan korkeimman johdon välisessä viestiliikenteessä. Colossus oli työkalu jonka sanotaan lyhentäneen sotaa, koska sen avulla saatiin selville Hitlerin aikeet juuri ennen liittoutuneiden maihinnousua Normandiaan.

Colossus sai nimensä suoraan koneen kolossaalisesta koosta. Ensimmäisessä Colossus Mk I versiossa kone koostui 1500 elektroniputkesta, mutta seuraava Colossus Mk II versio koostui 2500 elektroniputkesta[1]. Colossuksia rakennettiin julkaistujen tietojen mukaan noin kymmenen, joista yksi tai kaksi pidettiin käytössä vuosien 1958 ja 1960 välille, jonka jälkeen ne ilmeisesti tuhottiin.

Colossuksella ei salassapidon vuoksi ole suoraa vaikutusta tietokoneiden kehitykseen. Kuitenkin sillä todistettiin, että paljon elektroniputkia sisältävät koneet voivat toimia luotettavasti. Tätä tietoa tekijät käyttivät hyödykseen tulevissa projekteissaan, vaikka eivät voineet kertoa miten tähän tulokseen olivat tulleet. Esimerkiksi kun Alan Turing

[1] Elektroniputkien määrä Mark II:ssa vaihtelee lähteestä riippuen 2400 - 2500:taan

antoi ehdotuksensa ACE-tietokoneesta [Dav2003, s. 188-191], tiesi hän vastustuksesta huolimatta ehdotuksen olevan toteutettavissa, koska oli nähnyt samankaltaisen paljon isomman koneen jo toiminnassa Bletchley Parkissa.

Tässä esseessä tarkastellaan ensin hieman Lorenz-salakirjoitusta ja sen murtamista, josta päästään sen murtajiin ja ajatukseen murtamisen automatisoinnista. Automatisoinnin tuloksena syntyy Colossus, jonka rakennetta ja toimintaa käsitellään seuraavaksi. Lopuksi käsitellään lyhyesti Tony Salen käynnistämää projektia, jonka tuloksena Bletchley Parkin museossa on tänäkin päivänä toimiva Colossus.

2 Lorenz-salakirjoitus

Saksan armeijan ylin johto pyysi Lorenz-yhtiötä tuottamaan mahdollisimman tehokkaan koneen salaamaan kaukokirjoitinliikennettään (teleprinter traffic). Lorenz-yhtiö suunnitteli salauskoneen nimeltä Lorenz SZ40 ja myöhemmän version SZ42. Salauskone perustui Gilbert Vernamin vuonna 1918 keksimään additiiviseen metodiin [Wri1998 s. 270-273]. Vernamin metodissa alkuperäiseen tekstiin lisätään merkki merkiltä sekoittavaa materiaalia eli avainhahmoja. Tällöin tuloksena on salattu teksti. Merkkien yhteenlasku suoritetaan bittitasolla modulo 2 lisäyksenä, jolloin salattuun tekstiin lisättynä salaava avainhahmo poistaa salauksensa. Vernamin metodi käyttää aakkosien koodaamiseen kansainvälistä Baudot-koodia. Tässä koodissa aakkoset koodataan viiden bitin ryhmiin, joissa yksi tarkoittaa reikää nauhassa (kuva 1).

A 11000	**B** 10011	**C** 01110	**D** 10010
E 10000	**F** 10110	**G** 01011	**H** 00101
I 01100	**J** 11010	**K** 11110	**L** 01001
M 00111	**N** 00110	**O** 00011	**P** 01101
Q 11101	**R** 01010	**S** 10100	**T** 00001
U 11100	**V** 01111	**W** 11001	**X** 10111
Y 10101	**Z** 10001		

Kuva 1. ***Baudot -koodi***

Esimerkiksi jos salattava teksti on ”JA” ja avainhahmo on ”MT” niin salaus- ja purkuoperaatio tapahtuvat seuraavasti. J- ja M-kirjaimen Baudot-koodin bitit lisätään toisiinsa ja tuloksena saadaan Q-kirjain. Seuraavaksi lisätään A- ja T-kirjain toisiinsa, jolloin tuloksena on W-kirjain. Salattu teksti on siten QW. Salattu teksti muuttuu käytetyn avaimen mukaan. Salatun tekstin purkamiseksi sama avainhahmo lisätään salattuun tekstiin jolloin tuloksena on alkuperäinen teksti (kuva 2).

```
a)
J 11010  A 11000 (salattava)
+        +
M 00111  T 00001 (avainhahmo)
=        =
Q 11101  W 11001 (salattu)


b)
Q 11101  W 11001 (salattu)
+        +
M 00111  T 00001 (avainhahmo)
=        =
J 11010  A 11000
```

Kuva 2. ***Vernamin salauksen toiminta***

Vernamin ehdotuksen mukaan avainhahmojen täytyisi olla täysin sattumanvaraisia ja ennalta nauhoille rei’itettyjä. Sattumanvaraisuudella saataisiin aikaan murtovarma järjestelmä. Käytössä on täten kaksi nauhaa joista toisella on avainhahmo ja toisella on salattava teksti. Niin salauksen kuin purkamisenkin aikana näiden nauhojen täytyy kulkea koneen läpi tahdissa toisiinsa nähden. Sotatilanteen huomioon ottaen todettiin, että on liian hankala tuottaa ja levittää satunnaiset avainhahmonauhat kaikille niitä tarvitseville. Tämä johti siihen, että Lorenz-yhtiö päätti tehdä koneeseen Enigma-koneen [Wri1998 s. 260-263] mekanismia muistuttavan rataspakan, joka generoi pseudosatunnaisia avainhahmoja, tällöin salausta haluavilla vastapuolilla täytyi olla tiedossa vain rattaiden oikea aloitusasento. Tämä ominaisuus Lorenz-salauksessa auttoi murtamaan sen.

Ensimmäisiä Lorenz-salauksella salattuja viestejä saatiin haltuun vuoden 1940 alkupuolella. Tällöin John Tiltman kiinnostui niistä ja antoi niille koodinimen Fish. Englantilaiset antoivat Lorenz-koneelle koodinimeksi Tunny. Tiltman havaitsi tutkittuaan viestejä, että niihin on käytetty Vernam-salausta. Tämän jälkeen hän ymmärsi, että jos viestien lähettäjät tekevät virheen ja lähettävät kaksi viestiä samoilla asetuksilla, pystytään niistä laskemaan merkit, jotka kuvaavat alkuperäisten merkkien summaa[2] [Tut1998].

Bletchley Parkiin oli perustettu osasto jota kutsuttiin nimellä Testery ja siellä tutkittiin kaapattuja viestejä, mutta mainittavaa edistystä ei ollut tapahtunut ennen kuin 30. elokuuta vuonna 1941. Tällöin saksalainen kaukokirjoitinoperaattori teki virheen. Hän lähetti 4000 merkkiä pitkän viestin ja odotti vastausta, saaden viestin ”En saanut viestiä, lähetä viesti uudelleen”. Tällöin molemmat palauttivat koneensa samoihin asetuksiin kuin ensimmäistä viestiä lähetettäessä, joka oli kiellettyä. Viestien ollessa samoja olisi viestien salattu muoto ollut täysin sama, mutta operaattori lähettikin viestistä lyhennetyn version. Viesti alkoi sanalla spruchnummer (viestinumero) ja toisessa viestissä viesti alkoi sanalla spruchnr, jossa nr on lyhenne sanasta nummer. Viestin alkaessa samoin, mutta heti seitsemännen merkin jälkeen muuttuessa tulivat murtajat siihen tulokseen, että viesti oli koodattu samoilla asetuksilla, mutta sisältö oli erilainen. Päätelmää tuki myös toisen viestin pituus, joka oli 500 merkkiä vähemmän kuin ensimmäinen. Tämän jälkeen he saivat varmuuden saksalaisten käyttämästä metodista ja pystyivät selvittämään avaimen ja aukaisemaan viestin. Tähän työhön meni kuitenkin neljästä kuuteen viikkoa, jolloin puretulla viestillä ei ollut enää sisällöllistä merkitystä. John Tiltmanin työtä jatkoi juuri työnsä Bletchley Parkissa aloittanut Bill Tutte, joka aloitti kaukokirjoittimen kaikkien viiden kanavan bittihahmojen tallentamisen käsityönä. Tutte löysi tallentamistaan bittihahmoista toistuvia 41 merkin sarjoja[3]. Näiden sarjojen avulla saatiin selville salausavaimen rakenne ja lopulta salaavan koneen looginen rakenne. Tämä tapahtui ennen kuin kukaan purkamisen parissa työskennelleistä ihmisistä oli nähnyt Lorenz-

[2] Lähteessä tarkempi matemaattinen selvitys siitä kuinka Lorenz -salaus pystytään purkamaan
[3] Sarjojen pituus liittyy Lorenz -koneessa käytettyjen rattaiden kokoon

konetta. Vasta sodan jälkeen heille tarjoutui mahdollisuus tutustua aitoon Lorenz-koneeseen.

3 Murtamisen automatisointi

Max Newman saapui uutena työntekijänä Bletchley Parkiin. Newman oli ensimmäinen, joka esitti ehdotuksen purkamisen automatisoinnista tai ainakin osittaisesta automatisoinnista [Sin1999, s. 327-328]. Tämän ehdotuksen pohjalta työryhmä Dollis Hillissä rupesi suunnittelemaan konetta, joka toteutti Tutten metodin rattaiden aloituskohtien etsimiseksi. Tämä kone tunnetaan nimellä Heath Robinson. Kone käytti kahta reikänauhaa, joista toisessa oli kaapattu viesti ja toisessa koodinmurtajien käsin selvittämät rattaiden hahmot[4]. Näitä kahta nauhaa pyöritettiin koneessa synkronisesti toisiinsa nähden tuhat merkkiä sekunnissa. Jokaisen kierroksen jälkeen toista nauhaa siirrettiin yhdellä merkillä eteenpäin, kunnes koko ratashahmonauha oli käyty läpi. Jokaisella kierroksella laskettiin korrelaatioita bittihahmoista. Siinä ajossa, jossa korrelaatio oli suurin, oli suurin todennäköisyys että rattaiden aloituskohdat olivat löytyneet. Heath Robinson oli kuitenkin hankala kone käyttää ja rakentaa. Suurimman ongelman aiheutti kahden nauhan synkronointi, josta syystä kone oli melko hidas. Kone toimi kuitenkin tarpeeksi hyvin todistaakseen, että Newmanin ajatus automatisoinnista oli oikeassa.

Newman tapasi Dollis Hillissä Tommy Flowers nimisen postin elektroniikkainsinöörin, joka toimi automaattisten puhelinkeskusten parissa. Tapaamisen tarkoituksena oli keksiä kuinka Heath Robinson konetta voitaisiin nopeuttaa. Flowers ehdotti, että ratashahmonauha luotaisiin rengasmuisteihin, jolloin ei tarvittaisi kuin yksi nauha, joka sisältäisi vain kaapatun viestin. Hänen ehdotuksensa vaati kuitenkin suuren määrän elektroniputkia, joista siihen aikaan ei ollut tarvittavassa mittakaavassa paljoakaan tietoa ja niitä pidettiin epäluotettavina suurissa määrin käytettynä. Flowers kuitenkin tiesi puhelinkeskusten parissa tekemänsä tutkimuksen takia, että jos suuresta määrästä elektroniputkia koostuvaa

[4] Rattaiden hahmoilla tarkoitetaan sitä millaisia rattaat ovat, miten ne liikkuvat toisiinsa nähden ja millaisen muutoksen ne tekevät viestiin

konetta ei sammuteta, niin kone toimii luotettavasti. Elektroniputket ovat epäluotettavimmillaan koneen käynnistämisen aikaisessa lämpenemisessä. Tällöin elektroniputkelta ulos tuleva jännite voi olla niin kaukana perustasostaan, ettei siitä voida varmasti sanoa, onko bitti 1 vai 0. Kukaan ei kuitenkaan tuntunut uskovan Flowersia ja lisäksi tuohon aikaan yksi suurimmista tarvittavien elektroniputkien valmistajista sattui olemaan saksalainen. Tämä aiheutti ongelmia tarvikkeiden saannin kannalta. Monien mutkien kautta päätös saatiin tehtyä ja Colossuksen suunnittelu alkoi.

4 Colossus

Jokainen Colossuksista vaati huoneen verran tilaa. Kone koostui telineistä, jotka olivat 2,3 metriä korkeita ja vaihtelevan levyisiä. Telineet oli koottu kahdeksi 5,5 metriä leveiksi elementeiksi, jotka oli aseteltu siten, että huoltohenkilöstö pääsi telineiden väliin. Telineissä oli thyratron-rengasmuistit, AND- ja OR-portteja, kytkimet rattaiden aloituskohdille, laskurit ja virransyöttö. Lisäksi telineiden vieressä oli nauhalukija. Colossuksen perusperiaate oli laskea koko viestin läpi montako kertaa, jokin monimutkainen boolean-funktio tekstin ja rattaiden aloituskohtien välillä oli tosi tai epätosi. Tekstin loppuun päästessä tulokset siirrettiin releisiin, jotta voitiin aloittaa uutta laskentakierrosta. Aikanaan tulokset siirtyivät releistä sähkökirjoituskoneen kautta paperille. Tätä ominaisuutta pidetään alkumuotona puskuroinnille.

Colossuksen toiminnassa oli kaksi päävaihetta. Ensimmäistä kontrolloi optinen nauhanlukeminen, jossa haettiin nauhalta ennalta määrättyjä aloitus- ja lopetuskohtia. Optinen tieto luettiin nauhalta ja verrattiin thyratron-rengasmuisteissa olevaan ratastietoon. Boolean laskujen tulokset tallennettiin laskureihin. Toinen vaihe tapahtui nauhan aloitus- ja lopetusmerkin kohdalla. Lopetusmerkin kohdalla kone siirsi tulokset eteenpäin, tyhjensi muistinsa seuraavaa kierrosta varten ja merkitsi seuraavaksi koetettavan rattaiden aloituskohdan. Aloitusmerkin kohdalla kone alusti thyratron-rengasmuisteihinsa seuraavaksi koetettavan ratastiedon.

Optinen lukija koostui pienistä valokennoista, joita oli kuusi rinnakkain. Lukijassa oli myös linssejä, joilla tarkennettiin kennoille tulevaa valoa ja maski, jolla muokattiin valoa matkalla kennoon ja estettiin häiriö toisille kennoille tarkoitetusta valosta. Lukijan lukema tieto siirrettiin vakiinnuttajaan (staticisors) ja delta-piireille, jotka tasoittivat jännitteet standarditasoihin, jotta laskenta voisi tapahtua. Tämän jälkeen tietoa siirrettiin eteenpäin siirtorekisteriin (Shift Register), jossa pystyttiin pitämään viisi peräkkäistä merkkiä. Tätä rekisteriä käytettiin muun muassa joissakin algoritmeissa, joissa vertailtiin korrelaatioita rinnakkaisten merkkien välillä. Boolean laskentaa varten koneessa oli AND- ja OR-portteja, jotka voitiin kytkeä mihin tahansa järjestykseen siirtelemällä piuhoja pistokkeesta toiseen. Tulokset näistä laskuista kerrottiin laskureille, jotka perustuivat Wynn-Williamsin suunnittelemiin laskureihin. Colossuksessa oli myös toisenlaisia laskureita, joiden avulla pystyttiin olemaan välittämättä korruptoituneesta tiedosta, esimerkiksi silloin kun viestiä kaapattaessa signaali on huojunut eikä saatu tasavahvuista signaalia talteen. Tällöin heikon signaalin kohdassa oleva tieto saattaa olla laskennan kannalta harhaanjohtavaa. Tämän jälkeen tulokset siirrettiin releiden kautta tulostettavaksi IBM:n sähkökirjoituskoneelle, joista ensimmäinen oli lainakone [Coo1983].

Colossuksen monimutkaisin osa oli thyratron-rengasmuistit. Tyhratronit ovat kaasulla täytettyjä putkia, jotka antavat jännite purkauksen saatuaan, elektronien virrata tiettyyn suuntaan, jolloin siinä on bitti 1. Thyratroni on siis yhden bitin tallentava osa. Esimerkiksi siirtorekisterit on rakennettu thyratroneilla, jolloin thyratronin tilan muuttuessa kertoo se tilansa seuraavalle ja ottaa itse uuden tilan. Thyratron-muistirenkaiden pituutta voitiin säätää siirtämällä ohituskaapelia renkaassa haluttuun kohtaan. Tämä sen vuoksi, että Lorenz-salauksen purussa oli tärkeätä se, että rattaiden tiedot olivat oikean mittaisia, eli rattaan hammasluku oli sama thyratron-muistirenkaan kanssa [Coo1983].

Colossuksessa oli kellopulssikoneisto, jolla pystyttiin hallitsemaan koneen toimintaa ja ohjaamaan sen eri osien käyttöä suhteessa muihin osiin. Lisäksi kellopulssikoneistolla pystyttiin hidastamaan koneen toimintaa askel kerrallaan suoritettavaksi, esimerkiksi testausta varten. Colossusta ohjelmoitiin kaapeleilla ja

kytkimillä, joilla pystyttiin muuttamaan korrelaatioihin käytettyjä laskentakaavoja. Laskentakaavojen tulokset pystyttiin antamaan seuraaville loogisille porteille tai ne pystyttiin lähettämään halutulle laskurille. Manuaalisen ohjelmointityön kuten muunkin koneen käytön hoitivat WREN:it (Women's Royal Naval Service, WRNS). Heille ohjeet antoivat matemaatikot, joista muodostui nopeasti jonkin asteisia ohjelmoijia. Ohjeet olivat yleensä pikaisesti kirjoitettuja pieniä paperilappusia, jotka sisälsivät vain koetettavaksi halutun päätöspuun. Tulokset annettiin takaisin matemaatikoille, jotka sitten kertoivat miten edetään ja minkälainen ohjelma ajetaan seuraavaksi [Cha1983].

Colossuksien rakentaminen ja suunnittelu tapahtui paljolti rinnakkain. Ensimmäisessä rakennetussa Colossuksessa oli 1500 elektroniputkea. Tämä kone oli kuitenkin oletettua hitaampi. Ennen kuin Mark I oli valmistunut, jatkettiin suunnittelua seuraavaa versiota varten. Toisessa versiossa elektroniputkien määrä oli kasvatettu 1500:sta 2500:taan. Elektroniputkien määrän kasvu johtui rakenteen muuttamisesta. Mark II:ssa hyödynnettiin enemmän rinnakkaisuutta ja lyhytaikaista muistia. Tällöin koneen todellinen nopeus oli 25000 merkkiä sekunnissa, vaikka koneen perusnopeus (5000 merkkiä / s) ei noussut. Nopeuden kasvu johtui siitä, että Mark II:lla pystyttiin ajamaan viiden peräkkäisen merkin vertailu samanaikaisesti. Nauhan syöttönopeuden kasvattamista kokeiltiin kokeilumielessä ja todettiin, että 5000 merkkiä sekunnissa on turvallinen käyttönopeus. Tämä päätös johtui kokeilujen aikana sattuneesta tapahtumasta. Tällöin kone pyöri noin 9700 merkkiä sekunnissa nopeudella ja nauha katkesi useasta eri kohdasta. Koska nauhan nopeus koneessa oli noin 100 kilometriä tunnissa, niin voi kuvitella millainen kaaos huoneessa oli kun nauhan palasia lenteli huoneessa 100 kilometrin tunti nopeudella [Flo1983]. Suunnittelutyön jatkuminen rakentamisen aikana, johti siihen, että jokainen Colossus oli jollakin tavalla toisistaan poikkeava. Colossuksiin oli tehty aikaisempien jo rakennettujen koneiden pohjalta havaittuja parannuksia.

5 Colossus ja tietokone

Colossuksien ominaisuuksien vertailu nykyaikaiseen tietokoneeseen on hankalaa, koska niistä ei ole jäänyt jäljelle paljoakaan tietoa. Vaikka Colossus on pystytty rakentamaan uudelleen, jouduttiin rakentamisvaiheessa sitoutumaan viranomaisten vaatimuksiin että uudelleen rakennetun Colossuksen käyttäminen ja tekniset tiedot olisivat vieläkin vain virallisen luvan saaneiden henkilöiden etuoikeus. Erinäisistä lähteistä voidaan silti kertoa seuraavat ominaisuudet, joita voidaan verrata nykyaikaisiin tietokoneisiin. Osa ominaisuuksista koskee lähinnä Mark II versiota [Ran1982, s. 349-352; Ran1976].

- Elektroninen muisti, jonka sisältöä voidaan muuttaa komentojonoin
- Ehdollinen haarautumislogiikka (Conditional branching logic)
- Loogiset funktiot voitiin ennalta asettaa kytkimin ja kaapelein
- Binääriaritmetiikka
- Täysin automaattinen toiminta
- Vaihteleva ohjelmointi kytkimillä tarpeen mukaan
- Laski monimutkaisia boolean-funktioita, joissa saattoi olla 100 symbolia

Näiden kohtien perusteella voidaan sanoa, että Colossus oli ainakin tietyn tarkoituksen ohjelmoitava elektroninen digitaalitietokone. Vaikka kone ohjelmoitiinkin ulkoisesti kytkimillä ja kaapeleilla, oli se jonkinasteinen SPC-kone (stored program computer). Riippumatta siitä, että kone oli tarkoitettu tiettyyn tarkoitukseen, oli se suhteellisen joustava. Ainakin yhdessä lähteessä mainitaan Colossuksen kyenneen laskemaan päätöspuita, jotka ovat samankaltaisia kuin shakissa [Ran1976 s. 33], mutta missään lähteistä ei sanottu tarkemmin olisiko Colossus kyennyt pelaamaan shakkia. Toisessa lähteessä puhuttiin, että shakkia pelaavat koneet olisivat olleet yleisesti Bletchley Parkin työntekijöiden vapaa-ajan harrastus, joten kiinnostusta asiaan ainakin olisi ollut [Hod2000, s. 299].

Colossuksien käyttö ei rajoittunut vain Lorenz-salauksen purkamiseen, vaan sillä tehtiin kaikenlaista muutakin. Tästä muusta toiminnasta on vain arvailuja, koska tarkempaa tietoa asiasta ei ole julkaistu. Tiedetään kuitenkin, että Mark II versio yllätti joustavuudessaan, jopa suunnittelijansa. Colossuksien toiminnassa ja rakenteessa on huomattavissa se, että suunnittelijoilla oli käytettävissään Alan Turing ja hänen ajatuksensa universaalista automaatista (universal automaton). Tätä ja hänen julkaisuaan laskettavista numeroista (Computable Numbers) pidettiin suurena vaikutuksen lähteenä koneen suunnittelussa. Muutoin Turingin osallisuudesta ja vaikutuksesta Colossuksen suunnittelussa ollaan haastateltavasta tai kirjoittajasta riippuen hyvinkin eri mieltä. Toiset ovat mieltävät Turingin korvaamattomaksi ja toiset sivuuttavat hänet hitaana ajattelijana. Lähteiden mukaan Turing työskenteli pääasiassa Enigma-koodin purkamisessa [Cop2004, Lee1995[5], Mic2001]. Colossukset kokivat loppunsa vuonna 1945, jolloin ne purettiin uudelleen käytettäviksi osiksi ja loput hävitettiin Winston Churchillin komennosta nyrkkiä pienemmiksi palasiksi. Yksi tai kaksi koneista kuitenkin pidettiin salaisessa paikassa toimintakuntoisena ainakin vuosien 1958 ja 1960 välille, jonka jälkeen se ilmeisesti tuhottiin. Uudelleen rakentamisen kannalta on kiittäminen insinöörien piittaamattomuutta säännöistä, kun he säästivät joitakin koneen osien piirustuksia itsellään, eivätkä polttaneen niitä Bletchley Parkin kellarin uunissa niin kuin käskyssä oli määrätty.

5 Uudelleen rakentaminen

Vuonna 1991 Tony Sale aloitti kollegoidensa kanssa kampanjan Bletchley Parkin pelastamiseksi, joka oli saanut purkutuomion. Tällöin hän työskenteli Lontoon tiedemuseossa restauroiden ensimmäisiä englantilaisia tietokoneita. Hänellä oli ajatuksena Colossuksen uudelleen rakentaminen. Hänen ideansa kuitenkin joutui vastatuuleen, koska häntä ei uskottu ja tehtävää pidettiin mahdottomana. Vuonna 1993 Sale sai kerättyä kaiken saatavilla olevan materiaalin, joka koostui kahdeksasta valokuvasta sekä joistakin laitteiston osien piirustuksista. Yhdeksän kuukauden ajan

[5] Lähteestä saa mielestäni hyvän käsityksen siitä millaista oli työskennellä Bletchley Parkissa toisen maailman sodan aikana.

hän piirsi valokuvien pohjalta koneen rakennetta ja sai selville, että alkuperäisiä osia olisi vielä saatavilla tarpeeksi koneen rakennukseen. Colossukseen liittyvien salaisuuksien takia Sale piti tärkeänä saada virallisen luvan koneen uudelleen rakentamiseen. Luvan saamisessa ehtona oli, että konetta ei saisi käyttää kuka tahansa. Luvan saatuaan Sale aloitti koneen rakentamisen omilla varoillaan, koska muilla ei ollut luottamusta projektin onnistumisesta. Työtä hidastivat yhä jatkuva salassapito osassa Colossukseen liittyvissä asioissa ja alkuperäisten rakennusmateriaalien saatavuus. Lopulta Sale sai The Museum Trust of Communications & Electronics -järjestöltä Bristolista tarpeelliset tarvikkeet rakentamiseen ja vuonna 1994 olivat koneen kehikot valmiina ja vuonna 1996 koko kone oli toimintakuntoinen. Tämän mahdollisti vuonna 1994 mukaan tullut Kentin Herttua, joka perusti museon Bletchley Parkiin ja otti Colossuksen uudelleen rakentamisen virallisesti suojelukseensa. Projekti sai vuonna 1994 lisäksi jonkin verran yksityistä pääomaa käyttöönsä. Vuonna 1994 Sale sai apua myös Flowersilta, joka oli alun perin suunnittelemassa Colossusta [Sal1995]. Sale piti tätä apua tärkeänä. Hänen mielestään kone piti rakentaa uudelleen vielä silloin, kun edes osa sen alkuperäisistä suunnittelijoista ja rakentajista on edelleen elossa. Vuonna 1995 Arnold Lynch auttoi häntä rakentamaan nauhanlukijan siten kuin se oli alun perin rakennettu. Lynch oli rakentanut alkuperäisen nauhanlukijan vuonna 1942. Vuonna 1996 Kentin Herttua kytki uudelleen rakennettuun Colossukseen virran ja kone toimi aivan niin kuin se oli alun perin toiminutkin. Myös Flowers oli paikalla, kun kone käynnistettiin ensimmäisen kerran. Nykyään Colossuksen kopio on nähtävissä Bletchley Parkin museossa.

Colossuksen uudelleen rakentamisen takana on osittain mielipiteet siitä, että amerikkalaiset ovat liian kauan ylpeilleet ENIAC koneellaan ja asialla, että ENIAC on ensimmäinen tietokone maailmassa. Sale toteaa artikkelissaan [Sal2000], että koneen käynnistämisen jälkeen toiselta rannalta ei ole kuulunut mitään, ainoastaan hämmästyttävä hiljaisuus.

6 Yhteenveto

Colossus oli pitkään salassa pidetty ohjelmoitava digitaalinen logiikkalaskin. Sen katsotaan ratkaisevasti lyhentäneen toista maailmansotaa, koska sen avulla liittoutuneet kykenivät saamaan selville, mitä Saksan armeijan ylin johto suunnitteli. Colossus kykeni suorittamaan monimutkaisia boolean-funktioita ja käyttämään haarautuvaa logiikkaa. Koneessa käytettiin hyväksi myös tehtävien rinnakkaisuutta, jolloin koneen nopeutta saatiin kasvatettua, koska kone teki samaan aikaan useita tehtäviä. Colossuksia rakennettiin noin kymmenen. Toisen maailmansodan jälkeenkin Colossus haluttiin pitää salaisuutena ja kaikki materiaali siitä haluttiin tuhota. Yksi tai kaksi koneista kuitenkin säilytettiin toimintakuntoisena ainakin vuoteen 1960 asti, jonka jälkeen ne todennäköisesti tuhottiin.

Voimme vain arvailla kuinka Colossus olisi voinut muuttaa nykypäivän käsitystä tietojenkäsittelystä ja tietokoneista. Colossuksella voidaan todeta olleen toisen asteen vaikutuksia tietokoneiden kehitykselle, vaikka sen olemassaolo salattiinkin. Työntekijät, jotka olivat osallisia Colossuksien suunnittelussa ja rakentamisessa Bletchley Parkissa ja Dollis Hillissä, saivat merkittävän kokemuksen elektronisten tietokoneiden rakentamisen saralla. Osa työntekijöistä siirtyi sodan jälkeen suoraan seuraavien tietokoneiden rakentamiseen ja koska heillä oli kokemusta asiasta pystyivät he aloittamaan suunnittelun ja rakentamisen paljon korkeammalta tasolta kuin heidän siviili vastakohtansa. Näin ollen he pystyivät tuomaan elektroniikan tuntemuksellaan siviilipuolen kehitystyöhön uusia ajatuksia.

Tämän esseen lopettaa hyvin Flowersin kommentti Randelin haastattelussa. Tämä kommentti kuvaa mielestäni hyvin Bletchley Parkin ilmapiiriä. ”*It was a great time in my life – it spoilt me for when I came back to mundane things with ordinary people.*” [Ran1976 ,s.52].

Lähteet

Cha1983 Chandler W. W., *the Installation and Maintenance of Colossus.* Annals of the History of Computing, Volume 5, Number 3, July 1983, s. 260-262

Coo1983 Coombs A.W. M., *the Making of Colossus.* Annals of the History of Computing, Volume 5, Number 3, July 1983, s. 253-259

Cop2004 Copeland J. B., *Colossus: It's origins and originators.* IEEE Annals of the History of computing, October-December 2004, s. 38-45

Dav2003 Davis M., *Tietokoneen esihistoria Leibnizista Turingiin.*, Art House, 2003

Flo1983 Flowers T.H., *the Design of Colossus.* Annals of the History of Computing, Volume 5, Number 3, July 1983, s. 239-252

Hod2000 Hodges A., *Alan Turing arvoitus.*, Terra Cognita, 2000

Lee1995 Lee J. A. N., Holtzman G., *50 years after breaking the codes: Interviews with two of the Bletchley Park Scientists*, IEEE Annals of the History of Computing, Vol 17, No. 1, 1995, s. 32-43

Mic2001 Michie D., *Secrets Of Colossus Revealed*, IEEE Intelligent Systems, November/December 2001, s.82-83

Ran1976 Randell B., *the COLOSSUS*, Technical Report Series, University of Newcastle Upon Tyne, 1976

Ran1982 Randell B., *the Origins of Digital Computers. selected papers.*, Springer-Verlag Berlin, Heidelberg New York, 1982

Sal1995 Sale T., *the Colossus of Bletchley Park.*, IEE Review, March 1995, s. 55-59

Sal2000 Sale T., *Lorenz and Colossus.*, 0-7695-0671-2/00 IEEE, 2000

Sin1999 Singh S., *Koodikirja salakirjoituksen historia muinaisesta egyptistä kvanttikryptografiaan.*, Gummerus, 1999

Tut1998 Tutte W.T. *Fish and I.* University of Waterloo, Canada, in Coding theory and cryptography, Annapolis, *MD, 1998* (Berlin, 2000), s. 9-17 http://www.math.uwaterloo.ca/CandO_Dept/William_Tutte/bletchley.html (27.2.2005)

Wri1998 Wrixon F. B., *Codes and ciphers & other cryptic & clandestine communication. Making & breaking secret messages from hieroglyphs to the internet.*, Black Dog & Leventhal Publishers, 1998

Muuta luettavaa

B. Randell, *The Origins of Digital Computers: Supplementary Bibliography*. Technical Report Series, University of Newcastle Upon Tyne, 1976