Colossus

Samu Varjonen

10.3.2005

Sisällys

- Taustoja
- Lorenz
- Automatisoinnista
- Colossus
- Colossus ja tietokone
- Uudelleen rakennus
- Yhteenveto

Taustoja

- Toinen maailmansota, Bletchley Park
- Murrettiin saksalaisten salattuja viestejä
- Bletchley Park salattuna vuoteen 1974
- Osa työstä salaisena vuoteen 1995
- Julkaistuja dokumentteja ei montaakaan
- Churchill komensi kaiken tuhottavaksi
- Osa työntekijöistä säilytti joitakin osia dokumentaatiosta vastoin määräyksiä

Taustoja

- 1974 paljastui Colossus
- Ohjelmoitava digitaalinen logiikkalaskin
- Pääasiassa Lorenz-salakirjoitusta murtamaan suunniteltu
- Saksan armeijan ylimmän johdon viestiliikenne
- Sanotaan lyhentäneen sotaa
- Nimi kolossaalisesta koosta
- Mk I 1500 elektroniputkea Mk II 2500 elektroniputkea
- Noin kymmenen rakennettiin
- Mahdollisesti kaksi toimintakuntoisena vuoteen 1960 asti

Lorenz

- Saksan armeijan ylin johto pyysi Lorenz-yhtiöltä tehokasta salauskonetta
- Lorenz SZ40 ja SZ42
- Perustui Vernamin additiiviseen metodiin
- Vernam -> RC4 -> SSL ja WEP
- Merkkien koodaus Baudot koodilla
- Viisi bittiä / merkki, 1 on reikä nauhassa

Lorenz

- Vernamin mukaan avaimien pitäisi olla täysin sattumanvaraisia, tällöin saataisiin murtovarma järjestelmä
- Kaksi nauhaa, avain ja salattava teksti
- Ajetaan synkronisesti koneen läpi
- Sotatilanne vaikeutti avainnauhojen levitystä
- Koneeseen suunniteltiin rataspakka, joka generoi pseudosatunnaisen avaimen
- Käyttäjillä tieto oikeista rattaiden aloituskohdista

Murtaminen

- Lorenz-viestejä haltuun 1940
- John Tiltman kiinnostui ja totesi Vernam-salauksen osuuden
- Havainto: kaksi eri viestiä samoilla asetuksilla auttaisi purkamaan viestit
- Bletchley Parkissa osasto nimeltä Testery, jossa tutkittiin kaapattuja viestejä
- Ei mainittavaa edistymistä ennen elokuun loppua 1941

Murtaminen

- Saksalainen kaukokirjoitinoperaattori teki virheen
- Lähetti 4000 merkkiä pitkän viestin ja sai vastaukseksi pyynnön lähettää uudestaan
- Molemmat päät asettivat samat asetukset uudestaan, vaikka se oli kiellettyä
- Lisäksi viestin lähettäjä modifioi alkuperäistä viestiä

Murtaminen

- Jos viesti olisi ollut sama ei olisi mitään vahinkoa tapahtunut
- Viesti erosi pituudeltaan ja rakenteeltaan
- spruchnummer -> spruchnr
- Viittasi siihen, että kaksi erilaista viestiä lähetetty samoin asetuksin
- Viesti voitiin aukaista, mutta siihen käytettiin aikaa 4-6 viikkoa
- Viestin sisältö menettänyt merkityksensä

Murtaminen

- Bill Tutte jatkoi Tiltmanin työtä
- Havaittiin koodissa sarjoja, joiden avulla salaavan koneen looginen rakenne saatiin selville
- Kaikki tämä tapahtui ennen kuin kukaan murtamisen parissa työskennellyt oli nähnyt aitoa Lorenz-konetta
- Vasta sodan jälkeen heille tarjoutui mahdollisuus nähdä kone, jonka tuottaman koodin he olivat murtaneet

Automatisointi

- Max Newman oli ensimmäinen, joka ehdotti automatisointia
- Dollis Hillissä ruvettiin suunnittelemaan konetta tätä tarkoitusta varten
- Vain osa työstä automatisoitiin
- Syntyi Heath Robinson, joka nimettiin sota-ajan pilapiirtäjän mukaan
- Ongelmana hitaus, joka johtui kahden nauhan synkronoinnista
- Todisti kuitenkin automatisoinnin olevan mahdollista

Automatisointi

- Newman tapasi Tommy Flowersin, joka oli postin elektroniikkainsinööri
- Hän työskenteli automaattisten puhelinkeskusten parissa
- Hän ehdotti että avainnauha luotaisiin koneen muistiin, jolloin ei tarvittaisi kuin yksi nauha
- Ehdotus vaati suuren määrän elektroniputkia

Automatisointi

- Elektroniputkia pidettiin epävarmoina
- Flowersin aiemmat tutkimukset kuitenkin kertoivat koneen olevan mahdollinen
- Konetta ei vain saisi sammuttaa sen jälkeen kun se on käynnistetty
- Suurin epäluotettavuus juuri alun lämpenemisen yhteydessä
- Lisäksi suurin elektroniputkien valmistaja sattui olemaan saksalainen
- Lopulta suunnittelu kuitenkin alkoi ja tuloksena syntyi Colossus

Colossus

- Vaati huoneen verran tilaa
- 2,3 metriä korkea ja 5,5 metriä leveä
- Syvyyttä todennäköisesti noin 3 metriä
- Aseteltu kahdeksi 5,5 metriä leveiksi telineiksi
- Telineissä thyratron-rengasmuistit, AND- ja OR-portteja, kytkimet aloituskohtia varten, laskurit ja virransyöttö
- Omassa telineessään vieressä nauhanlukija ja toisessa sähkökirjoituskone tulostamista varten

Colossus

- Toiminnassa kaksi päävaihetta
- 1. vaihe luki tiedot nauhalta, joita verrattiin muistissa olevaan materiaaliin
- Boolean laskujen tulokset tallennettiin laskureihin
- 2. vaihe tapahtui aloitus- ja lopetusmerkkien kohdalla
- Lopetusmerkin kohdalla siirrettiin tulokset tulostettavaksi
- Aloitusmerkin kohdalla kone alustettiin seuraavaa ajoa varten

Colossus

- Optinen lukija koostui kuudesta rinnakkaisesta valokennosta, maskista ja linsseistä
- Maski ohjasi valoa kennoille ja linssit tarkensivat sitä
- Maski vähensi myös häiriöitä bittien välillä
- Lukijalla tuotettu sähkövirta siirrettiin vakiinnuttajiin ja delta-piireihin
- Nämä tasoittivat jännitteet standarditasoihin
- Tietty jännite vastasi bittiä 1 ja toinen bittiä 0

Colossus

- Tiedot siirrettiin siirtorekisteriin (shift register)
- Rekisterissä voitiin pitää viittä peräkkäistä merkkiä
- Rekisteriä käytettiin hyväksi myös joissakin algoritmeissä, joissa vertailtiin vierekkäisiä merkkejä
- Boolean-funktioita varten koneessa oli AND- ja OR-portteja jotka voitiin kytkeä mihin järjestykseen haluttiin
- Kytkentä tapahtui kaapeleiden avulla

Colossus

- Tulokset laskuista siirrettiin laskureihin
- Laskurit perustuivat Wynn-Williams laskureihin
- Lisäksi laskureita, jotka kykenivät huomioimaan korruptoituneen tiedon
- Laskureista tieto siirtyi releiden kautta tulostettavaksi sähkökirjoituskoneelle
- Ainakin ensimmäinen sähkökirjoituskone oli lainassa IBM:ltä

Colossus

- Thyratron-rengasmuistit
- Monimutkaisin osa
- Thyratronit ovat kaasulla täytettyjä putkia
- Tallentavat yhden bitin kerrallaan
- Siirtorekisterit toteutettu myös thyratroneilla
- Renkaan pituutta voitiin säätää hyppykaapeilla
- Renkaan pituuden täytyi vastata käytettyjen rattaiden hammaslukua

Colossus

- Colossuksessa oli kellopulssikone, jota ohjattiin nauhalla olevilla ylimääräisillä rei’illä
- Kellopulssit ohjasivat koneen osien yhteistoimintaa
- Koneen toiminta pystyttiin hidastamaan askel kerrallaan suoritukseen testausta varten

Colossus

- Colossusta ohjelmoitiin kaapeleilla ja kytkimillä
- Laskentakaavojen tulokset pystyttiin siirtämään kaapeleilla omille laskureilleen
- Tulokset voitiin siirtää myös seuraaville logiikka-porteille jos laskentaa haluttiin jatkaa
- Käytännön ohjelmoinnin suorittivat WREN:it (Women’s Royal Naval Service, WRNS)
- Matemaatikoista muodostui ohjelmoijia
- Antoivat ohjeet WREN:eille
- Ohjeet pieniä paperilappusia, jotka sisälsivät halutun päätöspuun mallin
- Tulokset annettiin takaisin matemaatikoille, jotka päättivät mitä seuraavaksi tehdään

Colossus

- Colossuksien rakentaminen tapahtui osittain rinnakkaisesti
- Jokainen Colossus erosi toisistaan jossain määrin
- Eroavaisuudet olivat pieniä parannuksia edelliseen versioon
- Colossus Mk I oli oletettua hitaampi
- Colossus Mk II:ssa elektroniputkia lisättiin
- Kasvu johtui rinnakkaisuuden lisäämisestä

Colossus

- Mk II:ssa hyödynnettiin rinnakkaisuutta ja lyhytkestoista muistia enemmän
- Mk II:ssa suoritettiin viiden peräkkäisen merkin vertailu samanaikaisesti
- Nopeus kasvoi
  Mk I 5000 merkkiä /s -> Mk II 25000 merkkiä /s
- Nopeuden todettiin olevan turvallinen käyttönopeus
- Koe mielessä Colossusta on ajettu 9700 merkin nopeudella
- Koe päättyi katastrofiin nauhan palasten lennellessä 100 km/h vauhdilla ympäri huonetta

Colossus ja tietokone

- Vertailu hankalaa salailun vuoksi
- Vaikka uudelleen rakennettu, tietojen saanti silti rajoitettua
- Seuraavista kohdista osa koskee lähinnä Mk II versioita

Colossus ja tietokone

- 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 tarpeen mukaan
- Laski monimutkaisia boolean-funktioita, joissa saattoi olla 100 symbolia

Colossus ja tietokone

- Oli tietyn tarkoituksen ohjelmoitava elektroninen digitaalitietokone
- Ohjelmoitiin ulkoisesti, mutta oli jonkinasteinen SPC-kone (Stored Program Computer)
- Vaikka tehty tiettyyn tarkoitukseen oli kuitenkin joustava toiminnassaan
- Yllätti joustavuudessaan tekijänsäkin

Colossus ja tietokone

- Kykeni laskemaan päätöspuita, jotka muistuttivat shakissa tarvittavia
- Bletchley Parkissa yleisenä harrastuksena shakkia pelaavat koneet
- Ei varmaa tietoa osasiko Colossus pelata shakkia
- Käyttö ei rajoittunut ainoastaan Lorenz-salauksen purkamiseen
- Muusta toiminnasta ei kuitenkaan ole mitään tarkempaa tietoa

Colossus ja tietokone

- Koneen rakenteesta ja toiminnasta voidaan havaita Alan Turingin vaikutus
- Universaali automaatti (Universal Automaton)
- Laskettavat numerot (Computable Numbers)
- Turingin osuus kiistanalainen
- Korvaamaton / Hidas ajattelija
- Turing työskenteli pääasiassa Enigman parissa

Colossus ja tietokone

- Colossukset kokivat loppunsa 1945
- Churchil komensi koneet tuhottavaksi ja dokumentoinnin poltettavaksi
- Yksi tai kaksi koneista pidettiin toimintakuntoisina vuoteen 1960 asti, tämän jälkeen koneet on todennäköisesti tuhottu
- Uudelleen rakentamisen kannalta oli tärkeätä insinöörien piittaamattomuus säännöistä
- Tämä pelasti osan dokumentaatiosta

Uudelleen rakentaminen

- Tony Sale aloitti kampanjan Bletchley Parkin pelastamiseksi vuonna 1991
- Hän työskenteli Lontoon tiedemuseossa restauroiden vanhoja englantilaisia tietokoneita
- Halusi rakentaa Colossuksen uudelleen
- Tehtävää pidettiin mahdottomana
- Dokumentaatio, rahoitus ja materiaali ongelmia

Uudelleen rakentaminen

- Dokumentaatiota koostui kahdeksasta valokuvasta ja joistakin laitteiston osien piirustuksista
- 9 kuukautta Sale piirsi Colossuksen rakennetta uusiksi
- Sai rakennusmateriaalit the Museum Trust of Communications & Electronics –järjestöltä
- 1994 mukaan tuli Kentin Herttua, joka perusti Bletchley Parkin museon ja otti projektin suojelukseensa
- Projektin rahoitus oli suurin osin Salen harteilla ja osin joidenkin yksityisten lahjoitusten varassa
- 1995 Arnold Lynch auttoi rakentamaan nauhalukijan, jonka hän alunperinkin oli rakentanut
- Myös Flowers auttoi rakentamisessa

Uudelleen rakentaminen

- Rakentamisen takana osittain ajatukset amerikkalaisten ylpeilystä ENIAC koneellaan
- Sale halusi tehdä koneen uudelleen vielä silloin kun alkuperäiset rakentajat ovat elossa
- Sale totesi koneen käynnistymisen jälkeen, että toiselta rannalta ei ole kuulunut mitään, ainoastaan hämmästyttävä hiljaisuus
- Colossuksen voi nähdä Bletchley Parkin museossa

Yhteenveto

- Koko työ oli pitkään salassa pidetty
- Ohjelmoitava digitaalinen logiikkalaskin
- Colossuksen avulla saatiin selville mitä Saksan armeijan ylin johto suunnitteli
- Kykeni laskemaan monimutkaisia boolean-funktioita ja käytti haarautuvaa logiikkaa
- Colossus käytti hyväkseen rinnakkaisuutta ja lyhytkestoista muistia

Yhteenveto

- Voidaan vain esittää arvailuja miten tietojenkäsittely olisi muuttunut jos kone olisi ollut julkinen
- Toisen asteen vaikutuksia voidaan löytää
- Työntekijät veivät tietämyksensä siviiliprojekteihin, vaikka eivät voineet suoraan sanoa miten tiesivät asioista

Loppu

”*It was a great time in my life – it spoilt me for when I came back to mundane things with ordinary people*”

-Tommy Flowers (1976)

Bletchley Park

Tekijöitä ja vaikuttajia

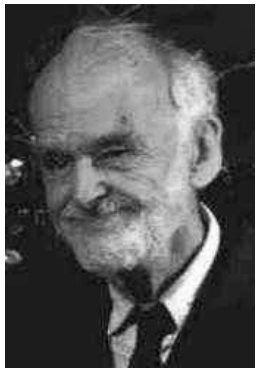
Gilbert Vernam

John Tiltman (oikealla)

Bill Tutte

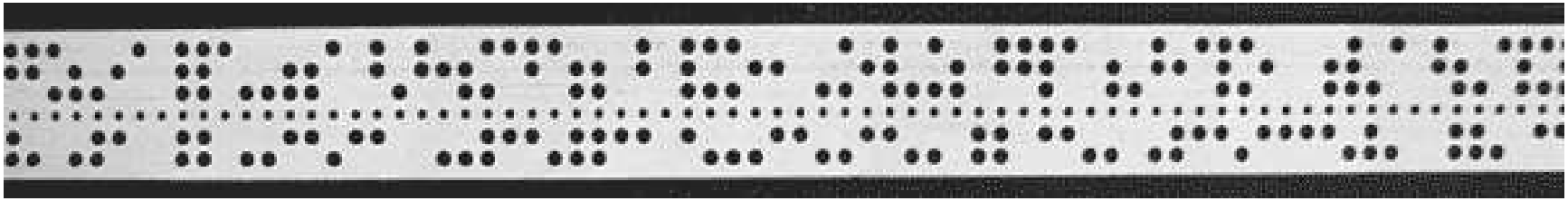
Max Newman

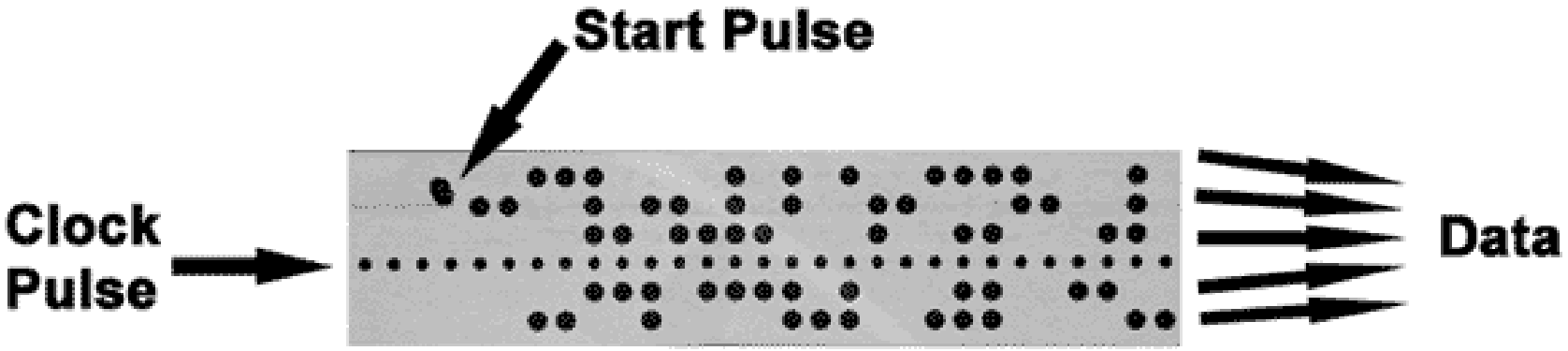
Tommy Flowers



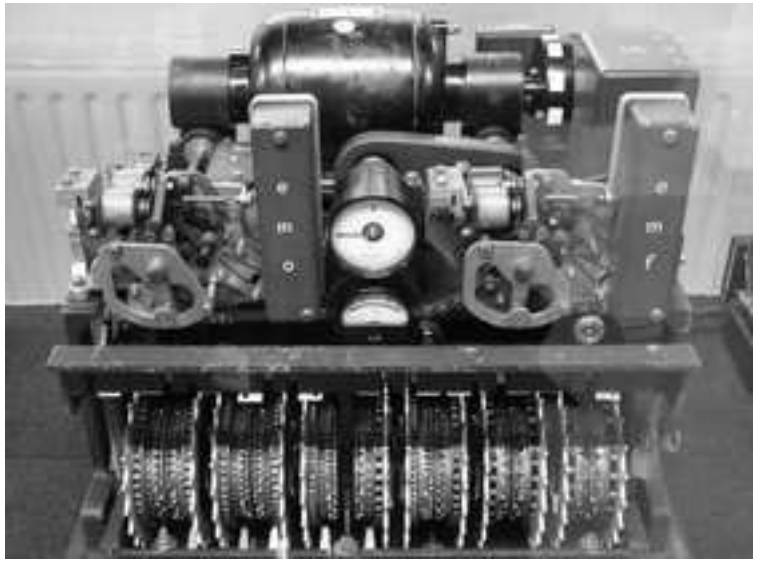
Arnold Lynch

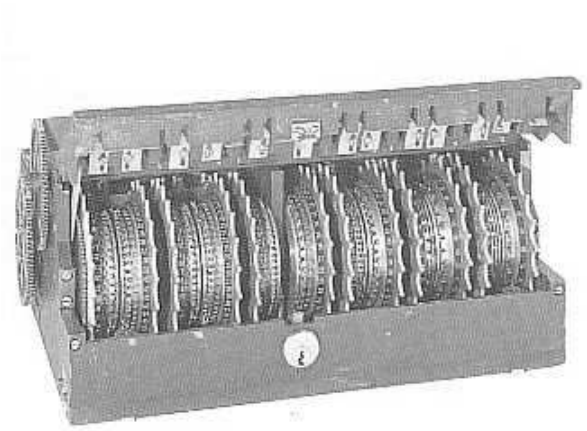
Tony Sale

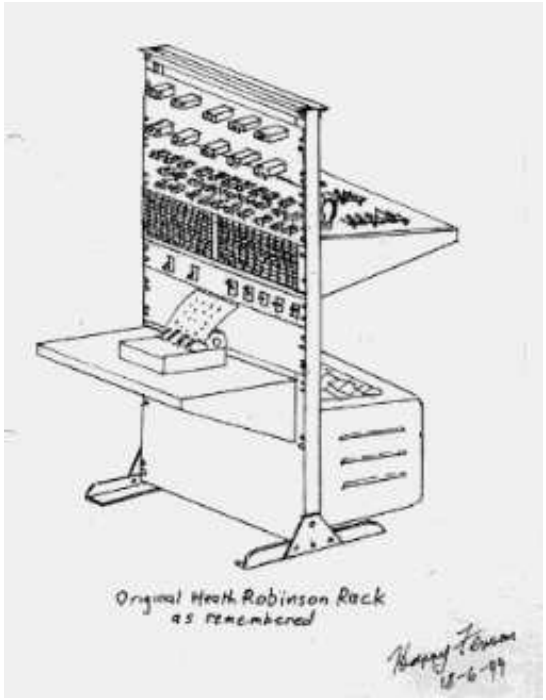




Colossuksessa käytettyjen nauhojen mallit

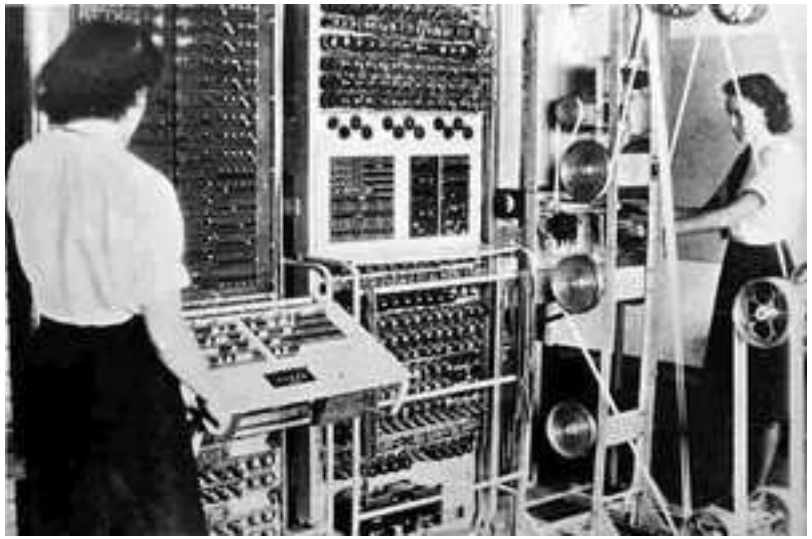


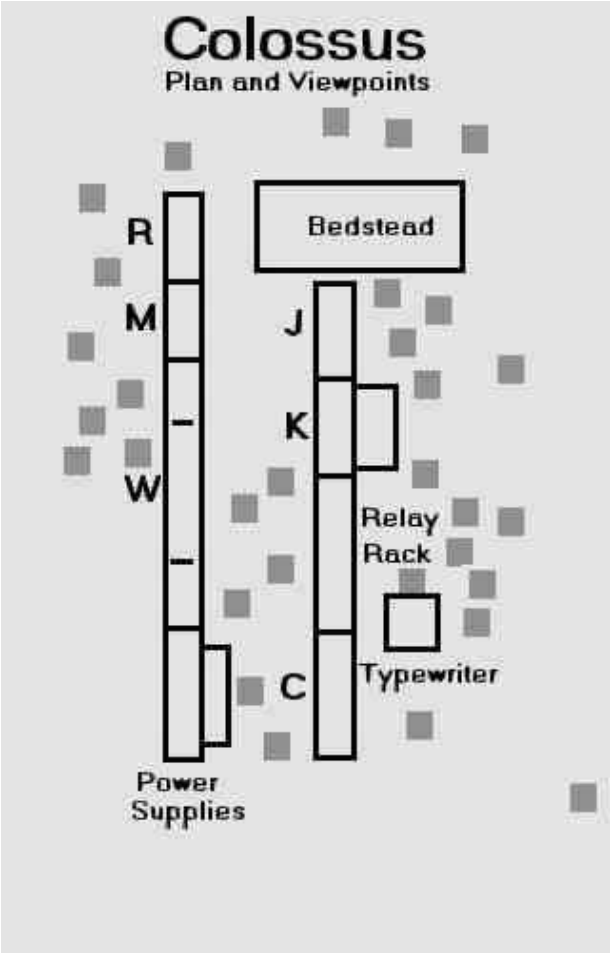




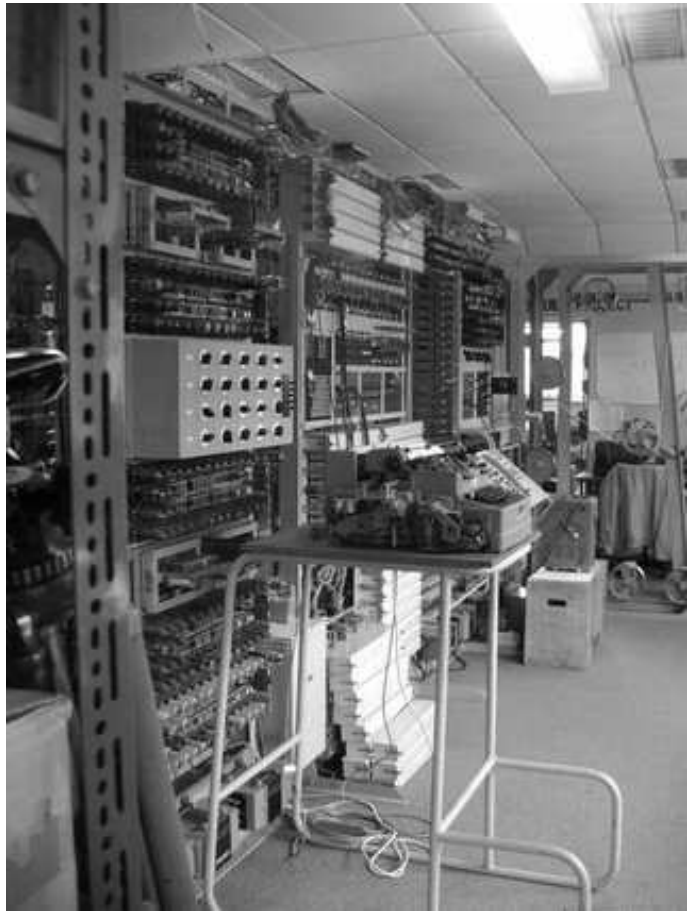
Yllä Lorenz SZ42 ja sen rataspakka

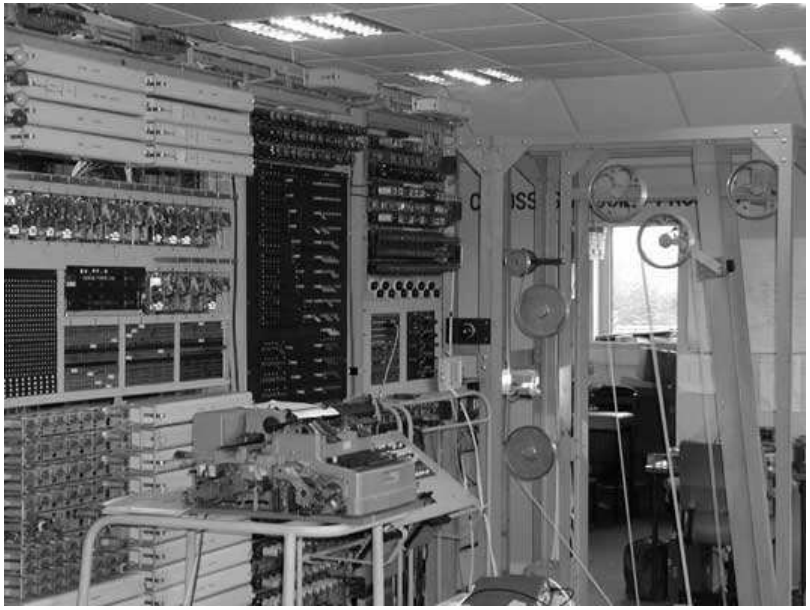
Oikealla Heath Robinson





Colossus ja sen pohjapiirustus





Uudelleen rakennettu Colossus ja sen käynnistäminen

Kuvassa istumassa Tommy Flowers, konetta käynnistämässä Kentin Herttua ja hänen takanaan Tony Sale

Kuvalähteet

http://www.codesandciphers.org.uk

http://www.bletchleypark.org.uk/

http://www-ivs.cs.uni-magdeburg.de/bs/lehre/wise0102/progb/vortraege/kmuecke/lorenz.html

http://www.apprendre-en-ligne.net/crypto/vigenere/masque.html

http://www.math.uwaterloo.ca/CandO_Dept/William_Tutte/tutte_pictures/party2.shtml

http://www.connected-earth.com/Journeys/Transformingsociety/Inpeaceandwar/Enterthecodebreakers/TommyFlowers/tommyflowers(1905-1998).htm

http://www.mariner.org/atlantic/bb01.htm

www.fc.up.pt/mp/jcsantos/spinexpo.html

(15.3.2005)