Szyfr Lorenza i jego złamanie (2)

*Bartosz KLIN**

* Uniwersytet Oksfordzki

Szyfr Lorenza był używany przez armię niemiecką podczas II wojny światowej do przesyłania najważniejszych informacji i rozkazów. W pierwszej części artykułu, która ukazała się w poprzednim numerze *Delty*, przedstawiliśmy alfabet telegraficzny używany podczas II wojny światowej do przesyłania komunikatów i ogólną metodę szyfrowania tekstów zapisanych tym alfabetem. W drugiej części opiszemy, jak dokładnie działała maszyna szyfrująca Lorenz SZ40/42 i jak aliantom udało się złamać jej szyfr.

Głównym zadaniem maszyny Lorenza jest generowanie pseudolosowego ciągu znaków w alfabecie telegraficznym. Wygenerowany ciąg jest kluczem szyfrującym, który dodawany jest znak po znaku do oryginalnego komunikatu. Każdy znak w alfabecie telegraficznym składa się z pięciu bitów (○ i ●), dlatego też maszyna generuje równolegle pięć pseudolosowych ciągów bitów.

Centralnym elementem maszyny jest 12 kół zębatych, które w Bletchley Park nazwano literami greckiego alfabetu: pięć kół χ, dwa koła μ i pięć kół ψ. Każde koło ma inną liczbę zębów:

χ_1	χ_2	χ_3	χ_4	χ_5	μ_1	μ_2	ψ_1	ψ_2	ψ_3	ψ_4	ψ_5
41	31	29	26	23	37	61	43	47	51	53	59

Wszystkie te liczby są względnie pierwsze. Dzięki temu synchronicznie obracające się koła nie powracają do początkowego ustawienia przez bardzo długi czas.

Na każdym zębie każdego koła znajduje się igła, która może być wysunięta (●) lub schowana (○). Przy generowaniu kolejnych znaków klucza koła obracają się o jeden ząb zgodnie z poniższymi zasadami:

– koła $\chi_1, \ldots, \chi_5$ i μ_1 obracają się za każdym razem,
– koło μ_2 obraca się tylko, jeśli igła na aktualnie widocznym zębie koła μ_1 jest wysunięta ($\mu_1 = \bullet$),
– koła $\psi_1, \ldots, \psi_5$ obracają się tylko, jeśli igła na aktualnie widocznym zębie koła μ_2 jest wysunięta ($\mu_2 = \bullet$).

W każdym kolejnym generowanym znaku i-ty bit powstaje jako suma $\chi_i + \psi_i$ aktualnych wskazań kół χ_i i ψ_i.

Wygenerowany w ten sposób klucz zależy od:

– ustawienia igieł na kołach; ustawienia te początkowo zmieniano co kwartał lub co miesiąc, a od 1944 roku – codziennie,
– początkowego ustawienia kół.

Początkowe ustawienie kół operator-nadawca wybiera każdorazowo przed wysłaniem komunikatu. Następnie przesyła to ustawienie jawnym tekstem jako 12-literowy *indykator*, po czym przystępuje do szyfrowania właściwej wiadomości. Przypisanie liter alfabetu zębom na poszczególnych kołach zmieniano co miesiąc.

HQIBPEXEZMUG

Tak działała maszyna Lorenza. Oczywiście w czerwcu 1941 roku, kiedy Niemcy uruchomili te maszyny po raz pierwszy, alianci nie mieli o tym wszystkim pojęcia. Wiedzieli jedynie z nasłuchu radiowego, że oto pojawił się nowy szyfr oparty na alfabecie telegraficznym. Szybko doszli do wniosku, że mają do czynienia z jakąś odmianą szyfru Vernama, rozpoznali szczególną rolę pierwszych 12 znaków jako indykatora początkowego ustawienia maszyny i nauczyli się korzystać z pojawiających się czasem głębi. (Powtarzanie ustawień początkowych było w niemieckim regulaminie zakazane, ale operatorzy nie zawsze tego regulaminu przestrzegali). Początkowo nie wiedziano jednak nic o konstrukcji maszyny i głównie zapisywano wszystkie podsłuchane komunikaty w nadziei, że w przyszłości będzie można je odszyfrować.

Dla przykładu zaszyfrujmy komunikat `DELTA_`. W alfabecie telegraficznym wygląda on tak:

$T =$

●	●	○	○	●	○
○	○	●	○	●	○
○	○	○	○	○	●
●	○	○	○	○	○
○	○	●	●	○	○
D	E	L	T	A	_

Aby go zakodować, musimy dodać do niego klucz szyfrujący. Do jego stworzenia użyjemy maszyny Lorenza. Powiedzmy, że zęby maszyny po kolejnych obrotach wyglądają następująco (strzałki oznaczają obrót danego koła):

χ	●	→	○	→	●	→	○	→	●	→	●
	○	→	○	→	●	→	●	→	●	→	○
	○	→	●	→	○	→	●	→	○	→	●
	●	→	○	→	○	→	○	→	●	→	●
	●	→	○	→	●	→	○	→	○	→	●
μ	○	→	●	→	○	→	●	→	○	→	○
	○		○	→	●		●	→	○		○
ψ	●		●		●	→	○	→	○		○
	○		○		○	→	○	→	●		●
	●		●		●	→	●	→	○		○
	●		●		●	→	○	→	○		○
	○		○		○	→	○	→	●		●

Dodając do siebie kolejne wskazania kół χ i ψ, dostajemy klucz szyfrujący.

$\chi + \psi =$

○	●	○	○	●	●
○	○	●	●	○	●
●	○	●	○	○	●
○	●	●	○	●	●
●	○	●	○	●	○
H	D	V	→	B	K

Aby zakodować oryginalny komunikat, dodajemy do niego znak po znaku klucz szyfrujący: $S = T + (\chi + \psi)$, uzyskując następujący szyfrogram:

$S =$

●	○	○	○	○	●
○	○	○	●	●	●
●	○	●	○	○	○
●	●	●	○	●	●
●	○	○	●	●	○
X	↵	N	L	G	J

Rozkodowanie tekstu polega na ponownym dodaniu klucza szyfrującego.

O tym, czym jest głębia, pisaliśmy w poprzedniej części artykułu. W skrócie: jeżeli otrzymamy dwie wiadomości zakodowane tym samym kluczem szyfrującym, to dodając do siebie zakodowane teksty, otrzymamy sumę oryginalnych wiadomości. Jeżeli teraz zgadniemy fragment jednej wiadomości, to dostaniemy fragment drugiej, który po rozszerzeniu da nam znowu fragment pierwszej itd.

Rozwiązanie zadania F 1074.
Całkowita moc produkowana w Słońcu $P_S = 4\pi R^2 l_S \approx 3{,}8 \cdot 10^{26}$ W, co odpowiada stosunkowi mocy do masy: $P_S/M_S \approx 1{,}9 \cdot 10^{-4}$ W/kg. Utrzymanie stałej temperatury ciała wymaga ciągłej produkcji energii w procesach przemiany materii, nawet gdy spoczywamy. Dla oszacowania tej energii przyjmijmy, że ciało człowieka promieniuje jak ciało doskonale czarne. Przy takim założeniu promieniowana moc jest proporcjonalna do powierzchni ciała, S_c, i wynosi $P_c = \sigma S_c T_c^4$. Potrzebna jest jeszcze powierzchnia ciała człowieka o masie $m_c = 75$ kg. Średnia gęstość ciała jest w przybliżeniu równa gęstości wody ρ_w, a więc jego objętość $V_c \approx m/\rho_w$. Powierzchnia ciała jest na pewno większa od powierzchni, S, kuli o objętości V:

$$S_c \geqslant 4\pi \left(\frac{3V}{4\pi}\right)^{2/3} = 4\pi \left(\frac{3m_c}{4\pi\rho_w}\right)^{2/3}.$$

Dla człowieka otrzymujemy oszacowanie stosunku produkowanej mocy do masy:

$$\frac{P_c}{m_c} \approx \left(\frac{36\pi}{m_c\rho_w^2}\right)^{1/3} \sigma T_c^4.$$

Liczbowo: $P_c/m_c \approx 6$ W/kg, a więc wielokrotnie więcej niż stosunek promieniowanej mocy do masy dla Słońca.

Uwagi: Nasze oszacowanie znacznie zaniża wartość powierzchni ciała człowieka: otrzymujemy $S_c \approx 0{,}86\,\mathrm{m}^2$, podczas gdy pomiary prowadzą do średnich wartości $1{,}6\,\mathrm{m}^2$ dla kobiet i $1{,}9\,\mathrm{m}^2$ dla mężczyzn. Z drugiej strony, nasze ciała nie promieniują jak ciała doskonale czarne (zdolność emisyjna skóry jest wprawdzie bliska 1, ale zwykle znaczną część ciała pokrywa odzież) i dodatkowo absorbują promieniowanie termiczne otaczających ciał (np. ścian budynku) oraz wymieniają ciepło z otaczającym powietrzem. Otrzymaną wartość promieniowanej mocy należy więc uznać za zawyżoną.
Na podstawie dziennego zapotrzebowania na energię przyjmowaną w żywności L. Weinstein i J.A. Adams otrzymują wartość $P_c/m_c \approx 1$ W/kg (w książce „Guesstimation" wydanej przez Princeton University Press w 2008 r., skąd pochodzi pomysł zadania).

Przełom nastąpił 30 sierpnia 1941 roku. Tego dnia jeden z niemieckich operatorów popełnił poważny błąd. Wysłał wiadomość o długości około 4000 znaków, a kiedy okazało się, że z powodu problemów technicznych wiadomość nie została odebrana, wysłał ją jeszcze raz, z tym samym indykatorem: `HQIBPEXEZMUG`. Gdyby jeszcze wysłał dokładnie ten sam ciąg znaków, to nie byłoby problemu, ale – poirytowany koniecznością ponownego wpisania długiego tekstu – poczynił w wiadomości pewne drobne skróty. Przykładowo, od razu na samym początku zastąpił słowo *Spruchnummer* (czyli „komunikat numer...") skrótem *Spruchnr*. Kiedy alianci przechwycili obie wiadomości, szybko zorientowali się, że wpadł im w ręce prawdziwy skarb: głębia, w której jeden komunikat jest praktycznie kopią drugiego z niewielkim przesunięciem. W niedługim czasie John Tiltman, jeden z najbardziej doświadczonych specjalistów w Bletchley Park, odczytał cały tekst. Jego treść nie była bardzo cenna wywiadowczo, ale jednocześnie uzyskano coś o wiele cenniejszego: niemal 4000 kolejnych znaków klucza wygenerowanego przez maszynę Lorenza.

Przez kolejne miesiące cały zespół kryptologów próbował odgadnąć zasadę działania maszyny, która mogłaby wygenerować taki ciąg znaków. W październiku dołączył do nich William Tutte, błyskotliwy student matematyki z Cambridge, który krótko wcześniej w innym dziale Bletchley Park rozpracował szyfr włoskiej marynarki wojennej. Rozmaite teorie rozważane przez zespół właśnie upadły, więc nowy pracownik dostał wolną rękę w pracy nad tajemniczym kluczem.

Tutte postanowił skupić uwagę na „kanale 1", czyli na pierwszych bitach liter klucza. Zaczął wypisywać te bity w tabelkach o rozmaitej liczbie kolumn w nadziei na rozpoznanie jakiejś regularności. Po wielu próbach i błędach w tabeli o 41 kolumnach zauważył, że pewne wzorce powtarzały się w tych samych kolumnach częściej, niż by to wynikało z rachunku prawdopodobieństwa. Nabrał przekonania, że kanał 1 jest sumą dwóch kanałów, czyli ciągów bitów: kanału χ_1 o okresie 41 i kanału ψ_1, który się „jąkał": długie sekwencje takich samych bitów występowały w nim częściej niż w czysto losowym ciągu. Domyślił się, że istnieją dwa koła zębate: jedno o 41 zębach, które obraca się za każdym razem, i drugie, które czasem stoi w miejscu.

Reszta zespołu podchwyciła ten obiecujący pomysł i wszyscy zaczęli analizować pozostałe kanały klucza. Wkrótce odgadnięto liczbę zębów na wszystkich pięciu kołach χ. Ustalono też, że koła ψ obracają się i zatrzymują synchronicznie. Jako że indykator wiadomości za każdym razem miał 12 znaków, naturalnym było przypuszczenie, że za sterowanie ruchem kół ψ odpowiadają dwa dodatkowe koła, nazwane μ. Po wielu próbach i niepowodzeniach, wspomagając się także innymi znanymi wcześniej głębiami, ustalono liczby zębów na wszystkich tych kołach, a następnie ustawienie igieł. W styczniu 1942 roku, po czterech miesiącach od odczytania głębi `HQIBPEXEZMUG`, maszyna Lorenza była rozpracowana. Szybko skonstruowano jej replikę i zaczęto odczytywać komunikaty zaszyfrowane za jej pomocą.

Atak 1 + 2

Jednak już w październiku 1942 roku pojawił się problem. Niemcy ulepszyli procedurę uzgadniania początkowych ustawień kół w maszynie. Zamiast przesyłanych jawnym tekstem indykatorów wprowadzili książki kodowe. Taka książka zawierała setki ponumerowanych ustawień kół. Operator, wysyłając komunikat, wybierał jedno z ustawień i przesyłał jawnym tekstem tylko jego numer, po czym wykreślał to ustawienie z książki, aby nigdy nie użyć go ponownie. Alianci, rzecz jasna, nie mieli dostępu do tych książek (aż do końca wojny żadna nie wpadła im w ręce). W rezultacie, mimo że kryptologom udawało się odgadywać ustawienia igieł na kołach maszyny, to nie wiedzieli, jak ustawiać te koła, aby odszyfrować poszczególne komunikaty.

Rozwiązanie, zwane „atakiem 1 + 2", znów opracował Tutte. Polegało ono na rozważeniu tak zwanych *delt* kanałów bitów. Dla dowolnego ciągu bitów C

jego delta $\Delta(C)$ powstaje przez dodawanie kolejnych par sąsiednich elementów w C: i-ty bit w $\Delta(C)$ to suma i-tego i $(i+1)$-tego bitu w C. Przykładowo:

$$C = \bullet\bullet\circ\bullet\bullet\bullet\circ\circ\bullet\circ\circ\bullet\circ\circ\bullet\bullet\circ\bullet\bullet\bullet\cdots$$
$$\Delta(C) = \ \circ\bullet\bullet\circ\circ\bullet\circ\bullet\bullet\circ\bullet\bullet\circ\bullet\circ\bullet\bullet\circ\circ\ \cdots$$

Dla dwóch bitów ich suma jest równa •, kiedy się różnią, i ∘, kiedy są takie same. A zatem i-ty bit w ciągu $\Delta(C)$ mówi o tym, czy bity i oraz $i+1$ w C się różnią.

Tutte rozważył delty kanałów ψ. Zauważmy, że skoro podczas generowania kolejnych znaków klucza koła ψ czasem stoją w miejscu, to odpowiadające im kanały stosunkowo często zawierają długie ciągi takich samych bitów. To oznacza, że w deltach tych kanałów bit ∘ występuje częściej niż •. Tutte skupił uwagę na delcie sumy pierwszych dwóch takich kanałów. Okazało się, że jeśli na kołach μ około połowa igieł jest wysunięta (a Niemcy tak właśnie projektowali ustawienia igieł), to w kanale $\Delta(\psi_1+\psi_2)$ bit ∘ występuje średnio na około 70% pozycji.

Rozważmy teraz przeciętny tekst jawny T, zakodowany alfabetem telegraficznym, oraz pierwsze dwa kanały jego bitów. Okazuje się, że w kanale $\Delta(T_1+T_2)$ bit ∘ także występuje stosunkowo często, średnio na około 60% pozycji! To jest szczęśliwa cecha języka niemieckiego i kodowania w alfabecie ITA2, ale także rezultat zwyczajów niemieckich operatorów, którzy np. znaki przestankowe często powtarzali dwukrotnie, co dodaje do kanału delt bit ∘.

Prosty rachunek pokazuje, że w sumie delt

$$\Delta(T_1+T_2)+\Delta(\psi_1+\psi_2)$$

bit ∘ występuje średnio na około 54% pozycji.

Istotnie:
$0{,}7\cdot 0{,}6+(1-0{,}7)\cdot(1-0{,}6)=0{,}54$.

Co z tego wynika? Niech T oznacza tekst jawny, S – odpowiadający mu szyfrogram, a χ i ψ – kanały generowane przez koła maszyny. Jak już wiemy, zachodzi

$$S = T+\chi+\psi.$$

Klucz jest generowany i dodawany do T niezależnie na pięciu kanałach, więc także:

$$S_1+S_2 = T_1+T_2+\chi_1+\chi_2+\psi_1+\psi_2.$$

Nietrudno sprawdzić, że operacja Δ jest rozdzielna względem dodawania kanałów, więc:

$$\Delta(S_1+S_2) = \Delta(T_1+T_2)+\Delta(\chi_1+\chi_2)+\Delta(\psi_1+\psi_2).$$

Z poprzedniej obserwacji możemy zatem wywnioskować, że dla przeciętnego komunikatu kanały $\Delta(S_1+S_2)$ i $\Delta(\chi_1+\chi_2)$ zgadzają się ze sobą na około 54% pozycji.

Kanał S i wszystkie jego składowe znamy – to po prostu podsłuchany szyfrogram. Jeżeli znamy aktualne ustawienia igieł, to kanał χ też znamy. Konkretnie, $\chi_1+\chi_2$ (a także jego delta) to znany nam ciąg bitów o okresie $41\cdot 31 = 1271$. Jedyne, czego nie wiemy, to początkowe ustawienie kół, czyli przesunięcie okresowego kanału χ względem S. Ale statystyczna nierównowaga bitów ∘ i • w deltach występuje tylko, jeśli to przesunięcie dobraliśmy właściwie! W przeciwnym razie $\Delta(S_1+S_2)$ i $\Delta(\chi_1+\chi_2)$ będą się zgadzać na zupełnie przypadkowych pozycjach, średnio na 50% z nich.

Możemy więc spróbować dopasować kanały S i χ na wszystkie 1271 sposobów i sprawdzić, jak często się zgadzają. Jeżeli odsetek zgodnych pozycji istotnie przekracza 50%, to zapewne właśnie odgadliśmy początkowe ustawienie kół χ_1 i χ_2 dla tego konkretnego komunikatu. Następnie możemy postąpić podobnie z pozostałymi kołami χ. Na odpowiadających tym kołom składowych kanałach tekstów jawnych nie ma co prawda aż tak mocnej nierównowagi bitów, ale teraz znamy już ustawienia dwóch kół, więc z pozostałymi idzie łatwiej.

Po ustaleniu początkowych ustawień kół χ możemy dodać kanał χ do S – ten proces, realizowany w Bletchley Park przez zbudowane tam repliki maszyn Lorenza, nazywano *deχzacją*. Zdeχzowane szyfrogramy przekazywano kryptologom, którzy odczytywali je (tzn. odgadywali początkowe ustawienia

Rozwiązanie zadania F 1073.
Orbita, po jakiej Ziemia obiega Słońce, jest bardzo bliska orbicie kołowej. Siłą dośrodkową w ruchu orbitalnym jest przyciąganie grawitacyjne Ziemia–Słońce. Na podstawie równości tych sił otrzymujemy:

$$\frac{GM_S}{R^2} = \frac{4\pi^2 R}{t_0^2}.$$

Masa Słońca wynosi więc:

$$M_S = \frac{4\pi^2 R^3}{Gt_0^2}.$$

Liczbowo: $M_S \approx 2\cdot 10^{30}$ kg. Do wyznaczenia gęstości musimy znać promień Słońca. Całkowita moc promieniowana przez Słońce wynosi $P_S = 4\pi R^2 l_S$ i jest równa mocy promieniowanej przez ciało doskonale czarne o temperaturze T_S i promieniu równym promieniowi Słońca R_S: $P_S = 4\pi R_S^2 \sigma T_S^4$. Otrzymujemy:

$$R_S = R\sqrt{\frac{l_S}{\sigma T_S^4}}.$$

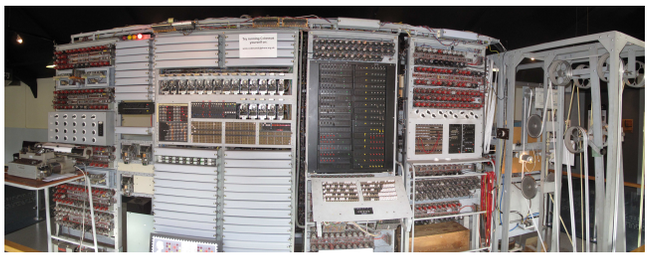
Liczbowo: $R_S \approx 6{,}98\cdot 10^8$ m. Możemy teraz wyznaczyć gęstość Słońca:

$$\rho_S = \frac{3\pi T_S^6}{t_0^2 G}\left(\frac{\sigma}{l_S}\right)^{3/2}.$$

Po podstawieniu danych liczbowych otrzymujemy $\rho_S \approx 1{,}4\cdot 10^3\ \mathrm{kg/m^3}$, to jest niemal półtora raza więcej niż gęstość wody.

Uwaga: Promień Słońca można wyznaczyć na podstawie obserwowanych rozmiarów kątowych Słońca $\sim 32'$, gdy znamy odległość Ziemia–Słońce.

kół ψ i μ) ręcznie. Było to już stosunkowo łatwe zadanie. Zdeχzowany komunikat jest sumą niemieckiego tekstu T i „jąkającego się" kanału ψ, i doświadczony specjalista, znający na pamięć tabliczkę dodawania liter, zwykle radził sobie z tym zadaniem bez trudności.



Rekonstrukcja komputera Colossus. Źródło: Wikipedia

Colossus

Jest tylko jeden problem: deχzacja każdego pojedynczego szyfrogramu wymagała porównania go z kanałem χ na ponad tysiąc sposobów. Nasłuch radiowy dostarczał niekiedy setki długich komunikatów każdego dnia, i robienie tego ręcznie było zupełnie niemożliwe. Było jasne, że należy to zadanie powierzyć maszynie.

Pierwszą wersję takiej maszyny uruchomiono w czerwcu 1943 roku. Potrafiła ona czytać równolegle dwie zapętlone perforowane taśmy telegraficzne – jedną z kanałami χ_1 i χ_2, drugą z przechwyconym szyfrogramem – i zliczać pozycje, na których ich delty zgadzają się ze sobą. Jeśli odsetek tych pozycji istotnie przekraczał 50%, urządzenie zatrzymywało się i dzwonkiem sygnalizowało znalezienie możliwego dopasowania.

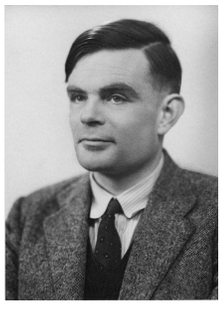
Maszyna była tak skomplikowana, że nazwano ją *Heath Robinson*, na cześć angielskiego rysownika znanego z absurdalnych projektów urządzeń do wykonywania najprostszych czynności. Była też bardzo zawodna, a głównym problemem była dokładna synchronizacja dwóch równolegle przesuwających się taśm. Jeden z jej konstruktorów, Tommy Flowers, postanowił zaprojektować ją od nowa z wykorzystaniem nowoczesnej technologii, nigdy wcześniej nieużywanej do takich celów: lamp elektronowych.

William Tutte (1917–2002)

Maszyna Flowersa, nazwana *Colossus*, była w istocie pierwszym na świecie programowalnym komputerem elektronicznym – powstała na dwa lata przed uruchomieniem sławnego na cały świat amerykańskiego komputera ENIAC. Obliczanie delt i dodawanie kanałów było realizowane przez elektroniczne bramki logiczne zbudowane z lamp. Także kanał χ był generowany przez układ lamp symulujących działanie obracających się kół zębatych, co eliminowało konieczność synchronizacji dwóch czytników taśm. Całe urządzenie składało się z około 1600 lamp oraz licznych wspomagających układów elektromechanicznych i potrafiło przetwarzać do 25 tys. znaków na sekundę. Układy bramek logicznych można było programować, dzięki czemu maszyna nadawała się nie tylko do jednego konkretnego zadania. Istotnie, jeszcze w czasie wojny zastosowano ją m.in. do odgadywania układów igieł na kołach maszyny Lorenza, pomysłową metodą opracowaną przez Alana Turinga.

Tommy Flowers (1905–1998)

Flowers wraz z około 50-osobowym zespołem rozpoczął projektowanie Colossusa jeszcze w lutym 1943 roku, a prototyp uruchomiono w grudniu tegoż roku. Do końca wojny zbudowano dziesięć egzemplarzy maszyny, co pozwoliło Anglikom rutynowo odczytywać komunikaty sztabów niemieckich zaszyfrowane maszyną Lorenza. Uzyskano w ten sposób bezcenne informacje, m.in. dane kluczowe dla powodzenia inwazji na Normandię.



Alan Turing (1912–1954)

Źródło zdjęć:
www.gchq.gov.uk/person/bill-tutte
en.wikipedia.org/wiki/Tommy_Flowers
www.iwm.org.uk/history/how-alan-turing-cracked-the-enigma-code (National Portrait Gallery)

Po zakończeniu wojny cała historia złamania szyfru Lorenza pozostała ściśle tajna. William Tutte zyskał sławę jako matematyk, twórca nowoczesnej teorii grafów, a o tzw. wielomianie Tutte'a studenci informatyki uczą się do dziś. Inni wybitni członkowie zespołu, tacy jak Donald Michie czy Jack Good, a także sam Alan Turing, zajęli się projektowaniem pierwszych komputerów elektronicznych, do czego z pewnością zainspirował ich przykład Colossusa. Sam Tommy Flowers próbował zdobyć finansowanie na budowę komputera, ale potencjalni fundatorzy nie uwierzyli, że jest to możliwe. Flowers oczywiście wiedział, że jest możliwe, bo już taki komputer zbudował, ale nie mógł tego ujawnić.

Istnienie komputera Colossus pozostawało tajemnicą do 1975 roku, a cała sława związana z konstrukcją pierwszego komputera elektronicznego spłynęła na amerykańskich konstruktorów ENIAC-a z 1945 roku. Historię odtworzenia maszyny Lorenza, złamania jej szyfru i zastosowania Colossusa odtajniono dopiero w 2000 roku.