Alan Turing- život a dílo

Radek Tesař

Vysoké učení technické Brno

3. února 2014

Počátky

Alan Mathison Turing, OBE narozen 23. června 1912, zemřel 7. června 1954 byl významný britský matematik, logik, kryptoanalytik a zakladatel moderní informatiky.

- Rodiče Julius Mathison a Ethel Sara.
- žili do synova narození indickém Madrásu.
- Otec se vrátil z Anglie zpět do Indie a matka o rok a půl později.
- Alana vychovávaly do 14 let chůvy a příbuzní.

Počátky

Alan Mathison Turing, OBE narozen 23. června 1912, zemřel 7. června 1954 byl významný britský matematik, logik, kryptoanalytik a zakladatel moderní informatiky.

- Rodiče Julius Mathison a Ethel Sara.
- žili do synova narození indickém Madrásu.
- Otec se vrátil z Anglie zpět do Indie a matka o rok a půl později.
- Alana vychovávaly do 14 let chůvy a příbuzní.

Počátky

Alan Mathison Turing, OBE narozen 23. června 1912, zemřel 7. června 1954 byl významný britský matematik, logik, kryptoanalytik a zakladatel moderní informatiky.

- Rodiče Julius Mathison a Ethel Sara.
- žili do synova narození indickém Madrásu.
- Otec se vrátil z Anglie zpět do Indie a matka o rok a půl později.
- Alana vychovávaly do 14 let chůvy a příbuzní.

Střední škola

- 1926-31 střední škola Sherbone v Dorsetu- cesta na kole.
- Zájem o přírodní vědy, bavily ho šachy.
- Přátelství s Christopherem Morcomem.
- 1930 umírá Morcom na TBC poté co je přijat na univerzitu.
- 1931 je Turing přijat na King´s College.

Střední škola

- 1926-31 střední škola Sherbone v Dorsetu- cesta na kole.
- Zájem o přírodní vědy, bavily ho šachy.
- Přátelství s Christopherem Morcomem.
- 1930 umírá Morcom na TBC poté co je přijat na univerzitu.
- 1931 je Turing přijat na King´s College.

Střední škola

- 1926-31 střední škola Sherbone v Dorsetu- cesta na kole.
- Zájem o přírodní vědy, bavily ho šachy.
- Přátelství s Christopherem Morcomem.
- 1930 umírá Morcom na TBC poté co je přijat na univerzitu.
- 1931 je Turing přijat na King´s College.

King´s College

Zde působili Bernard Russell, Alfred North Whitehead a Ludwig Wittgenstein.

- 1931-34 studium matematiky. Nenápadný, ale pilný student. Kvantová mechanika, pravděpodobnost, logika.
- 1935 člen univerzitní koleje (fellow) na základě disertace o centrální limitní větě.
- 1936 článek „On Computable Numbers, with an Application to the Entscheidungsproblem“.
- Zavádí pojem Turingova stroje, dokazuje že problém zastavení Turingova stroje není rozhodnutelný. Potvrdil tak věty o neúplnosti, které definoval 1931 Gödel.
- Church-Turingova teze: toto zjištění lze aplikovat na Hilbertem formulovaný problém rozhodnutelnosti.

King´s College

Zde působili Bernard Russell, Alfred North Whitehead a Ludwig Wittgenstein.

- 1931-34 studium matematiky. Nenápadný, ale pilný student. Kvantová mechanika, pravděpodobnost, logika.
- 1935 člen univerzitní koleje (fellow) na základě disertace o centrální limitní větě.
- 1936 článek „On Computable Numbers, with an Application to the Entscheidungsproblem“.
- Zavádí pojem Turingova stroje, dokazuje že problém zastavení Turingova stroje není rozhodnutelný. Potvrdil tak věty o neúplnosti, které definoval 1931 Gödel.
- Church-Turingova teze: toto zjištění lze aplikovat na Hilbertem formulovaný problém rozhodnutelnosti.

King´s College

Zde působili Bernard Russell, Alfred North Whitehead a Ludwig Wittgenstein.

- 1931-34 studium matematiky. Nenápadný, ale pilný student. Kvantová mechanika, pravděpodobnost, logika.
- 1935 člen univerzitní koleje (fellow) na základě disertace o centrální limitní větě.
- 1936 článek „On Computable Numbers, with an Application to the Entscheidungsproblem“.
- Zavádí pojem Turingova stroje, dokazuje že problém zastavení Turingova stroje není rozhodnutelný. Potvrdil tak věty o neúplnosti, které definoval 1931 Gödel.
- Church-Turingova teze: toto zjištění lze aplikovat na Hilbertem formulovaný problém rozhodnutelnosti.

King´s College

Zde působili Bernard Russell, Alfred North Whitehead a Ludwig Wittgenstein.

- 1931-34 studium matematiky. Nenápadný, ale pilný student. Kvantová mechanika, pravděpodobnost, logika.
- 1935 člen univerzitní koleje (fellow) na základě disertace o centrální limitní větě.
- 1936 článek „On Computable Numbers, with an Application to the Entscheidungsproblem“.
- Zavádí pojem Turingova stroje, dokazuje že problém zastavení Turingova stroje není rozhodnutelný. Potvrdil tak věty o neúplnosti, které definoval 1931 Gödel.
- Church-Turingova teze: toto zjištění lze aplikovat na Hilbertem formulovaný problém rozhodnutelnosti.

King´s College

Zde působili Bernard Russell, Alfred North Whitehead a Ludwig Wittgenstein.

- 1931-34 studium matematiky. Nenápadný, ale pilný student. Kvantová mechanika, pravděpodobnost, logika.
- 1935 člen univerzitní koleje (fellow) na základě disertace o centrální limitní větě.
- 1936 článek „On Computable Numbers, with an Application to the Entscheidungsproblem“.
- Zavádí pojem Turingova stroje, dokazuje že problém zastavení Turingova stroje není rozhodnutelný. Potvrdil tak věty o neúplnosti, které definoval 1931 Gödel.
- Church-Turingova teze: toto zjištění lze aplikovat na Hilbertem formulovaný problém rozhodnutelnosti.

Univerzita Princetown

Byl členem výzkumného týmu matematických logiků vedených Alonzem Churchem.

- Pracoval zde na Riemannově hypotéze a funkci Zeta.
- Setkal se zde s John von Neumannem a také G. H. Hardym, který byl také gay.
- 1938 dokončil svoji práci o logice a obhájil zde doktorát.
- Vzhledem k jeho novým výzkumům na poli teorie grup mu po obhajobě John von Neumann nabídl místo.

Univerzita Princetown

Byl členem výzkumného týmu matematických logiků vedených Alonzem Churchem.

- Pracoval zde na Riemannově hypotéze a funkci Zeta.
- Setkal se zde s John von Neumannem a také G. H. Hardym, který byl také gay.
- 1938 dokončil svoji práci o logice a obhájil zde doktorát.
- Vzhledem k jeho novým výzkumům na poli teorie grup mu po obhajobě John von Neumann nabídl místo.

Univerzita Princetown

Byl členem výzkumného týmu matematických logiků vedených Alonzem Churchem.

- Pracoval zde na Riemannově hypotéze a funkci Zeta.
- Setkal se zde s John von Neumannem a také G. H. Hardym, který byl také gay.
- 1938 dokončil svoji práci o logice a obhájil zde doktorát.
- Vzhledem k jeho novým výzkumům na poli teorie grup mu po obhajobě John von Neumann nabídl místo.

Stroj na výpočet funkce Zeta

- Zajímalo ho rozmístění prvočísel v číselné řadě, což souviselo s jeho zájmem o kryptografii.
- Měl pochybnosti o platnosti Riemannovy hypotézy.
- Před druhou světovou válkou byla nedůvěra v platnost Riemannovy hypotézy celkem běžná.
- Pracoval na stroji, který měl počítat nulové body funkce Zeta v rozsahu $0 < Im(s) < 6000$. Je jich 5598.
- Na tento stroj obdržel grant 40 liber od Královské společnosti.

V době Mnichovské dohody začal pracovat pro vládu na problému dešifrování německé komunikace.

Stroj na výpočet funkce Zeta

- Zajímalo ho rozmístění prvočísel v číselné řadě, což souviselo s jeho zájmem o kryptografii.
- Měl pochybnosti o platnosti Riemannovy hypotézy.
- Před druhou světovou válkou byla nedůvěra v platnost Riemannovy hypotézy celkem běžná.
- Pracoval na stroji, který měl počítat nulové body funkce Zeta v rozsahu $0 < Im(s) < 6000$. Je jich 5598.
- Na tento stroj obdržel grant 40 liber od Královské společnosti.

V době Mnichovské dohody začal pracovat pro vládu na problému dešifrování německé komunikace.

Stroj na výpočet funkce Zeta

- Zajímalo ho rozmístění prvočísel v číselné řadě, což souviselo s jeho zájmem o kryptografii.
- Měl pochybnosti o platnosti Riemannovy hypotézy.
- Před druhou světovou válkou byla nedůvěra v platnost Riemannovy hypotézy celkem běžná.
- Pracoval na stroji, který měl počítat nulové body funkce Zeta v rozsahu $0 < Im(s) < 6000$. Je jich 5598.
- Na tento stroj obdržel grant 40 liber od Královské společnosti.

V době Mnichovské dohody začal pracovat pro vládu na problému dešifrování německé komunikace.

Stroj na výpočet funkce Zeta

- Zajímalo ho rozmístění prvočísel v číselné řadě, což souviselo s jeho zájmem o kryptografii.
- Měl pochybnosti o platnosti Riemannovy hypotézy.
- Před druhou světovou válkou byla nedůvěra v platnost Riemannovy hypotézy celkem běžná.
- Pracoval na stroji, který měl počítat nulové body funkce Zeta v rozsahu $0 < Im(s) < 6000$. Je jich 5598.
- Na tento stroj obdržel grant 40 liber od Královské společnosti.

V době Mnichovské dohody začal pracovat pro vládu na problému dešifrování německé komunikace.

Grant od Královské společnosti

3. A. M. Turing.....£40.

King's College,
Cambridge.
24 *March* 1939.

"1. It is proposed to make calculations of the Riemann zeta-function on the critical line for $1{,}450 < t < 6{,}000$ with a view to discovering whether all the zeros of the function in this range of t lie on the critical line. An investigation for $0 < t < 1{,}464$ has already been made by Titchmarsh. The most laborious part of such calculations consists in the evaluation of certain trigonometrical sums

$$\sum_{r=1}^{m} \frac{1}{\sqrt{r}} \cos(t \log r - \vartheta) \qquad m = \left[\sqrt{\frac{t}{2\pi}}\right]$$

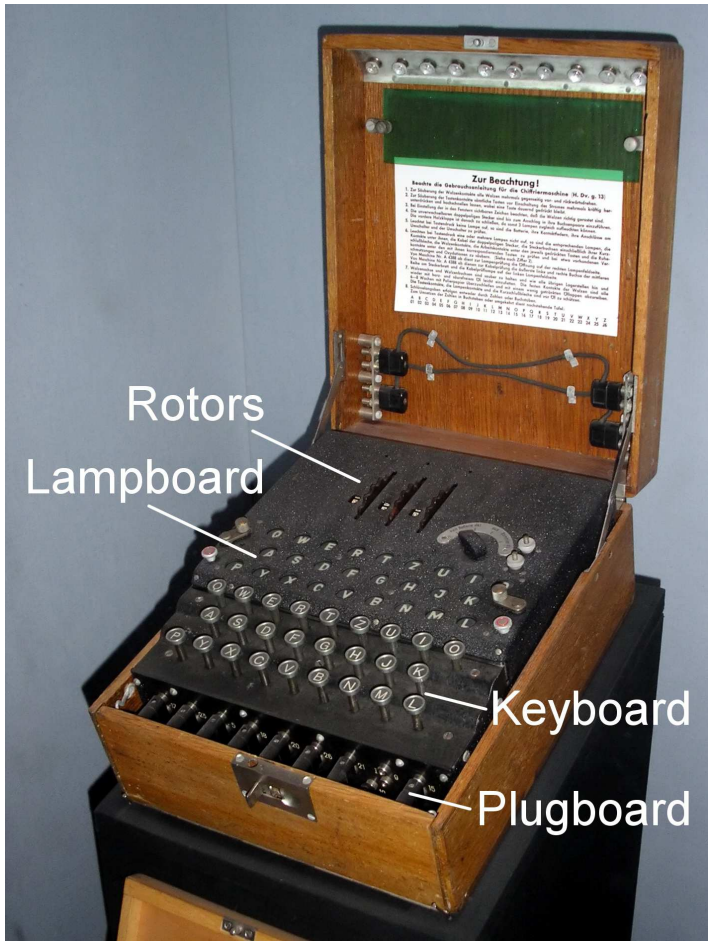
Vynález Enigmy

- Arthur Scherbius získal 1918 patent na šifrovací přístroj Enigma.
- 1925 až 1945 prodal německé armádě přes 30 000 kusů.
- Základem je 26 tlačítková klávesnice jako na psacím stroji, sada 26 žárovek prosvětlující písmena rozmístěné stejně jako zmíněná klávesnice, propojovací deska, tři rotory a reflektor.

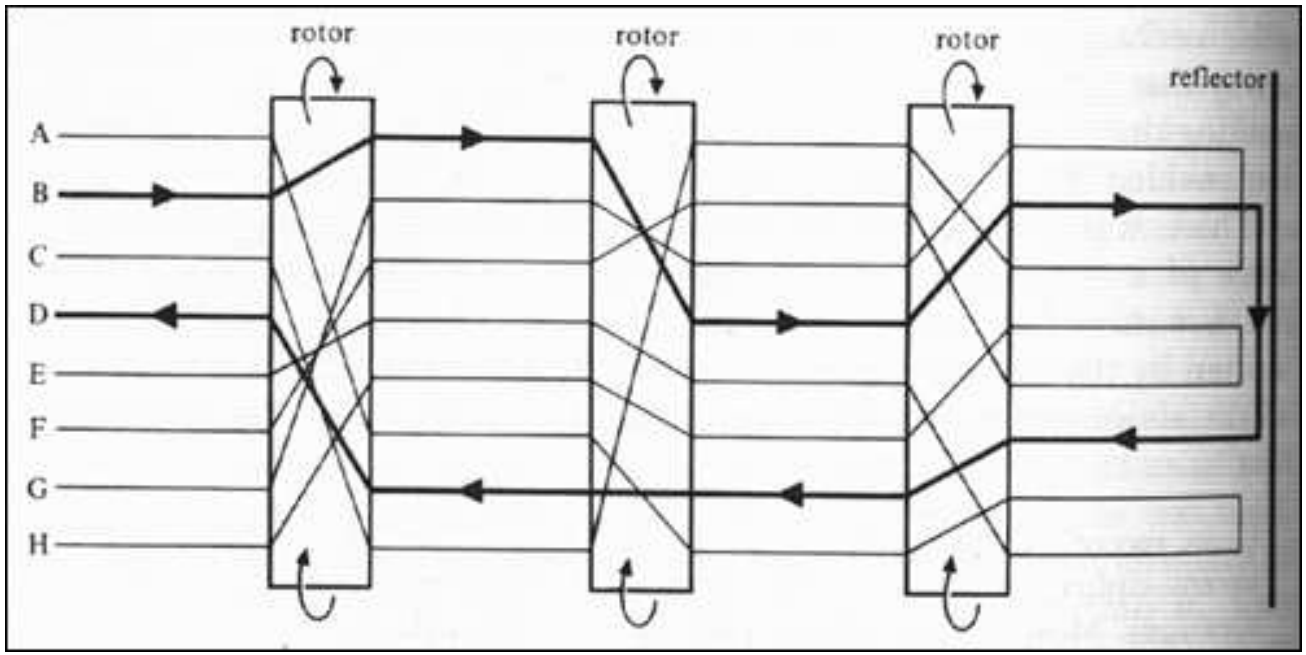
Vynález Enigmy

- Arthur Scherbius získal 1918 patent na šifrovací přístroj Enigma.
- 1925 až 1945 prodal německé armádě přes 30 000 kusů.
- Základem je 26 tlačítková klávesnice jako na psacím stroji, sada 26 žárovek prosvětlující písmena rozmístěné stejně jako zmíněná klávesnice, propojovací deska, tři rotory a reflektor.

Vynález Enigmy II



Vynález Enigmy III



- Získáme 26 x 26 x 26 = 17576 odlišných nastavení.
- Propojovací deska prohazovala dvě písmena, celkem 6 dvojic písmen. Získáme 100 391 791 500 kombinací.
- Celkově se zvýší počet možností na více než 10^{16}.

Šifrování I

Pro šifrování je tedy nutno nastavit rotory do výchozí pozice (podle kódové knihy), kterých je celkem 17576. Tím určíme jak bude enigma šifrovat zprávu.

- Operátor nastaví Enigmu, na klávesnici napíše první písmeno zprávy, podívá se které písmeno se rozsvítilo, zapíše první znak šifrového textu.
- Takto napíše celou zprávu a následně ji odvysílá.
- Příjemce nastaví Enigmu podle stejné kódové knihy, zadá písmeno šifrového textu a zapíše si které písmeno se mu rozsvítilo.
- Díky reflektoru je celá operace inverzní.
- To má ještě jednu vlastnost, které bylo využito při kryptoanalýze: nikdy se nemůže nějaké písmeno substituovat sebou samým.

Šifrování I

Pro šifrování je tedy nutno nastavit rotory do výchozí pozice (podle kódové knihy), kterých je celkem 17576. Tím určíme jak bude enigma šifrovat zprávu.

- Operátor nastaví Enigmu, na klávesnici napíše první písmeno zprávy, podívá se které písmeno se rozsvítilo, zapíše první znak šifrového textu.
- Takto napíše celou zprávu a následně ji odvysílá.
- Příjemce nastaví Enigmu podle stejné kódové knihy, zadá písmeno šifrového textu a zapíše si které písmeno se mu rozsvítilo.
- Díky reflektoru je celá operace inverzní.
- To má ještě jednu vlastnost, které bylo využito při kryptoanalýze: nikdy se nemůže nějaké písmeno substituovat sebou samým.

Šifrování I

Pro šifrování je tedy nutno nastavit rotory do výchozí pozice (podle kódové knihy), kterých je celkem 17576. Tím určíme jak bude enigma šifrovat zprávu.

- Operátor nastaví Enigmu, na klávesnici napíše první písmeno zprávy, podívá se které písmeno se rozsvítilo, zapíše první znak šifrového textu.
- Takto napíše celou zprávu a následně ji odvysílá.
- Příjemce nastaví Enigmu podle stejné kódové knihy, zadá písmeno šifrového textu a zapíše si které písmeno se mu rozsvítilo.
- Díky reflektoru je celá operace inverzní.
- To má ještě jednu vlastnost, které bylo využito při kryptoanalýze: nikdy se nemůže nějaké písmeno substituovat sebou samým.

Šifrování II

- Při kryptoanalýze náhodně nastavíme rotory, zapíšeme část šifrového textu a zkontrolujeme, dává-li nám smysluplný text. Pokud ne, proces opakujeme.
- Takto v nejhorším případě musíme vyzkoušet 17576 kombinací, což je při paralelizaci reálné.
- Proto udělali výměnné rotory. Lze je tedy prohazovat (první místo třetího, atd). To dává 6 x 17576 kombinací.
- Později měli vojáci k dispozici sadu 5 rotorů, takže mohli použít libovolné 3 z pěti rotorů.
- Pro zvýšení kombinací byla použita propojovací deska.

Scherbius byl přesvědčen, že je Enigma nezdolatelná. Německé memorandum to shrnulo: „Při posuzování bezpečnosti šifrovacího systému vycházíme z předpokladu, že nepřítel má přístroj k dispozici.“

Šifrování II

- Při kryptoanalýze náhodně nastavíme rotory, zapíšeme část šifrového textu a zkontrolujeme, dává-li nám smysluplný text. Pokud ne, proces opakujeme.
- Takto v nejhorším případě musíme vyzkoušet 17576 kombinací, což je při paralelizaci reálné.
- Proto udělali výměnné rotory. Lze je tedy prohazovat (první místo třetího, atd). To dává 6 x 17576 kombinací.
- Později měli vojáci k dispozici sadu 5 rotorů, takže mohli použít libovolné 3 z pěti rotorů.
- Pro zvýšení kombinací byla použita propojovací deska.

Scherbius byl přesvědčen, že je Enigma nezdolatelná. Německé memorandum to shrnulo: „Při posuzování bezpečnosti šifrovacího systému vycházíme z předpokladu, že nepřítel má přístroj k dispozici.“

Šifrování II

- Při kryptoanalýze náhodně nastavíme rotory, zapíšeme část šifrového textu a zkontrolujeme, dává-li nám smysluplný text. Pokud ne, proces opakujeme.
- Takto v nejhorším případě musíme vyzkoušet 17576 kombinací, což je při paralelizaci reálné.
- Proto udělali výměnné rotory. Lze je tedy prohazovat (první místo třetího, atd). To dává 6 x 17576 kombinací.
- Později měli vojáci k dispozici sadu 5 rotorů, takže mohli použít libovolné 3 z pěti rotorů.
- Pro zvýšení kombinací byla použita propojovací deska.

Scherbius byl přesvědčen, že je Enigma nezdolatelná. Německé memorandum to shrnulo: „Při posuzování bezpečnosti šifrovacího systému vycházíme z předpokladu, že nepřítel má přístroj k dispozici.“

Polsko před válkou

- Polské Biuro Szyfrow mělo k dispozici komerční verzi Enigmy. Ta se lišila od vojenské, hlavně v zapojení rotorů, proto nebyla použitelná pro luštění vojenských kódů.
- Francouzi získali návody k použití Enigmy, ze kterých se dalo odvodit zapojení rotorů. To však ke nestačí, je nutno vědět kterou z více než 10^{16} kombinací nastavení přístroje použít.
- Na základě smlouvy mezi Poláky a Francouzi o vojenské spolupráci jim Francouzi předali všechny informace o Enigmě. Součástí informací byl popis jak vypadají kódové knihy.

Polsko před válkou

- Polské Biuro Szyfrow mělo k dispozici komerční verzi Enigmy. Ta se lišila od vojenské, hlavně v zapojení rotorů, proto nebyla použitelná pro luštění vojenských kódů.
- Francouzi získali návody k použití Enigmy, ze kterých se dalo odvodit zapojení rotorů. To však ke nestačí, je nutno vědět kterou z více než 10^{16} kombinací nastavení přístroje použít.
- Na základě smlouvy mezi Poláky a Francouzi o vojenské spolupráci jim Francouzi předali všechny informace o Enigmě. Součástí informací byl popis jak vypadají kódové knihy.

Polsko před válkou

- Polské Biuro Szyfrow mělo k dispozici komerční verzi Enigmy. Ta se lišila od vojenské, hlavně v zapojení rotorů, proto nebyla použitelná pro luštění vojenských kódů.
- Francouzi získali návody k použití Enigmy, ze kterých se dalo odvodit zapojení rotorů. To však ke nestačí, je nutno vědět kterou z více než 10^{16} kombinací nastavení přístroje použít.
- Na základě smlouvy mezi Poláky a Francouzi o vojenské spolupráci jim Francouzi předali všechny informace o Enigmě. Součástí informací byl popis jak vypadají kódové knihy.

Dešifrování II

Němci zavedli opatření pro ztížení kryptoanalýzy- pomocí denního klíče se kódoval pouze klíč zprávy. Ten měl stejné nastavení propojovací desky i pozici rotorů, ale lišil se v nastavení rotorů.

- Odesílatel nastavil Enigmu na denní klíč (např. QCW), zakódoval jím nový klíč zprávy (např. PGH), který zakódoval 2x po sobě aby se vyloučila možnost chyby. Takže prvních šest znaků zprávy bylo PGHPGH, což se zakódovalo jako KIVBJE.
- Zbytek zprávy pak kódoval s nastavením rotorů na PGH.
- Příjemce prvních šest znaků KIVBJE dešifroval pomocí denního klíče (QCW), tím získal otevřený text PGHPGH, nastavil rotory na PGH a pak dešifroval zbytek zprávy.

Dešifrování II

Němci zavedli opatření pro ztížení kryptoanalýzy- pomocí denního klíče se kódoval pouze klíč zprávy. Ten měl stejné nastavení propojovací desky i pozici rotorů, ale lišil se v nastavení rotorů.

- Odesílatel nastavil Enigmu na denní klíč (např. QCW), zakódoval jím nový klíč zprávy (např. PGH), který zakódoval 2x po sobě aby se vyloučila možnost chyby. Takže prvních šest znaků zprávy bylo PGHPGH, což se zakódovalo jako KIVBJE.
- Zbytek zprávy pak kódoval s nastavením rotorů na PGH.
- Příjemce prvních šest znaků KIVBJE dešifroval pomocí denního klíče (QCW), tím získal otevřený text PGHPGH, nastavil rotory na PGH a pak dešifroval zbytek zprávy.

Dešifrování II

Němci zavedli opatření pro ztížení kryptoanalýzy- pomocí denního klíče se kódoval pouze klíč zprávy. Ten měl stejné nastavení propojovací desky i pozici rotorů, ale lišil se v nastavení rotorů.

- Odesílatel nastavil Enigmu na denní klíč (např. QCW), zakódoval jím nový klíč zprávy (např. PGH), který zakódoval 2x po sobě aby se vyloučila možnost chyby. Takže prvních šest znaků zprávy bylo PGHPGH, což se zakódovalo jako KIVBJE.
- Zbytek zprávy pak kódoval s nastavením rotorů na PGH.
- Příjemce prvních šest znaků KIVBJE dešifroval pomocí denního klíče (QCW), tím získal otevřený text PGHPGH, nastavil rotory na PGH a pak dešifroval zbytek zprávy.

Dešifrování II

Němci zavedli opatření pro ztížení kryptoanalýzy- pomocí denního klíče se kódoval pouze klíč zprávy. Ten měl stejné nastavení propojovací desky i pozici rotorů, ale lišil se v nastavení rotorů.

- Odesílatel nastavil Enigmu na denní klíč (např. QCW), zakódoval jím nový klíč zprávy (např. PGH), který zakódoval 2x po sobě aby se vyloučila možnost chyby. Takže prvních šest znaků zprávy bylo PGHPGH, což se zakódovalo jako KIVBJE.
- Zbytek zprávy pak kódoval s nastavením rotorů na PGH.
- Příjemce prvních šest znaků KIVBJE dešifroval pomocí denního klíče (QCW), tím získal otevřený text PGHPGH, nastavil rotory na PGH a pak dešifroval zbytek zprávy.

Rejewski

- Sestrojil repliku vojenské verze. Dále věděl, že prvních šest písmen jsou dvakrát opakované tři písmena klíče zprávy. V našem případě se PGH zobrazilo na KIV, druhé PGH na BJE.
- V prvním případě se P zobrazilo na K, v druhém na B.
- Měl-li dost zpráv, vytvořil celou abecedu vztahů, kde na prvním řádku bylo K, v druhém řádku pod ním B, atd.
- Z toho vytvořil řetězce tak, že např. K se zobrazí na B, B se zobrazí na jiné písmeno a to se zobrazí opět na K.
- Tím získal řetězec délky tři. Pokud to provedl se všemi znaky abecedy, dostal několik řetězců různé délky.

Rejewski

- Sestrojil repliku vojenské verze. Dále věděl, že prvních šest písmen jsou dvakrát opakované tři písmena klíče zprávy. V našem případě se PGH zobrazilo na KIV, druhé PGH na BJE.
- V prvním případě se P zobrazilo na K, v druhém na B.
- Měl-li dost zpráv, vytvořil celou abecedu vztahů, kde na prvním řádku bylo K, v druhém řádku pod ním B, atd.
- Z toho vytvořil řetězce tak, že např. K se zobrazí na B, B se zobrazí na jiné písmeno a to se zobrazí opět na K.
- Tím získal řetězec délky tři. Pokud to provedl se všemi znaky abecedy, dostal několik řetězců různé délky.

Rejewski

- Sestrojil repliku vojenské verze. Dále věděl, že prvních šest písmen jsou dvakrát opakované tři písmena klíče zprávy. V našem případě se PGH zobrazilo na KIV, druhé PGH na BJE.
- V prvním případě se P zobrazilo na K, v druhém na B.
- Měl-li dost zpráv, vytvořil celou abecedu vztahů, kde na prvním řádku bylo K, v druhém řádku pod ním B, atd.
- Z toho vytvořil řetězce tak, že např. K se zobrazí na B, B se zobrazí na jiné písmeno a to se zobrazí opět na K.
- Tím získal řetězec délky tři. Pokud to provedl se všemi znaky abecedy, dostal několik řetězců různé délky.

Rejewski II- analýza rotorů

- Dále pak rozdělil problém analýzy na nastavení rotorů a nastavení propojovací desky.
- Propojovací deska neměla na délky řetězce žádný vliv.
- Zaměřil se na délku a počet řetězců, které ovlivňovaly pouze rotory. Tím snížil náročnost analýzy na 105 456 možností.
- Pak sestavil katalog délek a počtu řetězců, což znamenalo vyzkoušet všech 105 tisíc kombinací. Pak byl schopen pomocí katalogu najít správné nastavení Enigmy ihned po té, co vytvořil abecedu vztahů toho dne a z ní dostal počet a délku řetězců.

Rejewski II- analýza rotorů

- Dále pak rozdělil problém analýzy na nastavení rotorů a nastavení propojovací desky.
- Propojovací deska neměla na délky řetězce žádný vliv.
- Zaměřil se na délku a počet řetězců, které ovlivňovaly pouze rotory. Tím snížil náročnost analýzy na 105 456 možností.
- Pak sestavil katalog délek a počtu řetězců, což znamenalo vyzkoušet všech 105 tisíc kombinací. Pak byl schopen pomocí katalogu najít správné nastavení Enigmy ihned po té, co vytvořil abecedu vztahů toho dne a z ní dostal počet a délku řetězců.

Rejewski II- analýza rotorů

- Dále pak rozdělil problém analýzy na nastavení rotorů a nastavení propojovací desky.
- Propojovací deska neměla na délky řetězce žádný vliv.
- Zaměřil se na délku a počet řetězců, které ovlivňovaly pouze rotory. Tím snížil náročnost analýzy na 105 456 možností.
- Pak sestavil katalog délek a počtu řetězců, což znamenalo vyzkoušet všech 105 tisíc kombinací. Pak byl schopen pomocí katalogu najít správné nastavení Enigmy ihned po té, co vytvořil abecedu vztahů toho dne a z ní dostal počet a délku řetězců.

Rejewski III- propojovací deska

Pokud dešifroval text zprávy, dostal částečně čitelný text, například „plijedtedobelrina“. To pravděpodobně znamená „prijedte do berlina“.

- To tedy znamená, že R a L jsou propojena, ale A,I,E,B a N nejsou.
- Analýzou dalších vět mohl určit další písmena, které je nutno prohodit.
- Později pak sestavil mechanickou verzi svého katalogu délek řetězců, takzvanou bombu.
- Potřeboval šest jednotek, každou pro jedno z možných uspořádání rotorů, které pracovaly paralelně. Každá jednotka prošla všech 17576 kombinací a našla tu správnou.

Rejewski III- propojovací deska

Pokud dešifroval text zprávy, dostal částečně čitelný text, například „plijedtedobelrina“. To pravděpodobně znamená „prijedte do berlina“.

- To tedy znamená, že R a L jsou propojena, ale A,I,E,B a N nejsou.
- Analýzou dalších vět mohl určit další písmena, které je nutno prohodit.
- Později pak sestavil mechanickou verzi svého katalogu délek řetězců, takzvanou bombu.
- Potřeboval šest jednotek, každou pro jedno z možných uspořádání rotorů, které pracovaly paralelně. Každá jednotka prošla všech 17576 kombinací a našla tu správnou.

Rejewski III- propojovací deska

Pokud dešifroval text zprávy, dostal částečně čitelný text, například „plijedtedobelrina“. To pravděpodobně znamená „prijedte do berlina“.

- To tedy znamená, že R a L jsou propojena, ale A,I,E,B a N nejsou.
- Analýzou dalších vět mohl určit další písmena, které je nutno prohodit.
- Později pak sestavil mechanickou verzi svého katalogu délek řetězců, takzvanou bombu.
- Potřeboval šest jednotek, každou pro jedno z možných uspořádání rotorů, které pracovaly paralelně. Každá jednotka prošla všech 17576 kombinací a našla tu správnou.

Rejewski III- propojovací deska

Pokud dešifroval text zprávy, dostal částečně čitelný text, například „plijedtedobelrina“. To pravděpodobně znamená „prijedte do berlina“.

- To tedy znamená, že R a L jsou propojena, ale A,I,E,B a N nejsou.
- Analýzou dalších vět mohl určit další písmena, které je nutno prohodit.
- Později pak sestavil mechanickou verzi svého katalogu délek řetězců, takzvanou bombu.
- Potřeboval šest jednotek, každou pro jedno z možných uspořádání rotorů, které pracovaly paralelně. Každá jednotka prošla všech 17576 kombinací a našla tu správnou.

Rejewski III- propojovací deska

Pokud dešifroval text zprávy, dostal částečně čitelný text, například „plijedtedobelrina“. To pravděpodobně znamená „prijedte do berlina“.

- To tedy znamená, že R a L jsou propojena, ale A,I,E,B a N nejsou.
- Analýzou dalších vět mohl určit další písmena, které je nutno prohodit.
- Později pak sestavil mechanickou verzi svého katalogu délek řetězců, takzvanou bombu.
- Potřeboval šest jednotek, každou pro jedno z možných uspořádání rotorů, které pracovaly paralelně. Každá jednotka prošla všech 17576 kombinací a našla tu správnou.

Rejewski IV- konec kryptoanalýzy

V roce 1938 němci zvýšili bezpečnost Enigmy tím, že všem operátorům dodali dva nové rotory.

- Do Enigmy bylo možno umístit kterékoliv tři z pěti rotorů v libovolné kombinaci. Tím zvýšili počet uspořádání na 60.
- Rejewski by musel postavit 10x více bomb, aby je byl schopen dešifrovat. To bylo drahé.
- Navíc němci přidali další čtyři propojovací kabely a tím měnili celkem dvacet písmen.
- Šéf Biura Szyfrow pozval šéfy francouzské a britské kryptoanalýzy a předvedl jim funkční bombu. S tím jim nabídl plány na výrobu bomb a dvě funkční Enigmy. Ty skončily v Anglii v Bletchley Parku, v sídle GC&CS (Goverment Code and Cypher School).

Rejewski IV- konec kryptoanalýzy

V roce 1938 němci zvýšili bezpečnost Enigmy tím, že všem operátorům dodali dva nové rotory.

- Do Enigmy bylo možno umístit kterékoliv tři z pěti rotorů v libovolné kombinaci. Tím zvýšili počet uspořádání na 60.
- Rejewski by musel postavit 10x více bomb, aby je byl schopen dešifrovat. To bylo drahé.
- Navíc němci přidali další čtyři propojovací kabely a tím měnili celkem dvacet písmen.
- Šéf Biura Szyfrow pozval šéfy francouzské a britské kryptoanalýzy a předvedl jim funkční bombu. S tím jim nabídl plány na výrobu bomb a dvě funkční Enigmy. Ty skončily v Anglii v Bletchley Parku, v sídle GC&CS (Goverment Code and Cypher School).

Rejewski IV- konec kryptoanalýzy

V roce 1938 němci zvýšili bezpečnost Enigmy tím, že všem operátorům dodali dva nové rotory.

- Do Enigmy bylo možno umístit kterékoliv tři z pěti rotorů v libovolné kombinaci. Tím zvýšili počet uspořádání na 60.
- Rejewski by musel postavit 10x více bomb, aby je byl schopen dešifrovat. To bylo drahé.
- Navíc němci přidali další čtyři propojovací kabely a tím měnili celkem dvacet písmen.
- Šéf Biura Szyfrow pozval šéfy francouzské a britské kryptoanalýzy a předvedl jim funkční bombu. S tím jim nabídl plány na výrobu bomb a dvě funkční Enigmy. Ty skončily v Anglii v Bletchley Parku, v sídle GC&CS (Goverment Code and Cypher School).

Rejewski IV- konec kryptoanalýzy

V roce 1938 němci zvýšili bezpečnost Enigmy tím, že všem operátorům dodali dva nové rotory.

- Do Enigmy bylo možno umístit kterékoliv tři z pěti rotorů v libovolné kombinaci. Tím zvýšili počet uspořádání na 60.
- Rejewski by musel postavit 10x více bomb, aby je byl schopen dešifrovat. To bylo drahé.
- Navíc němci přidali další čtyři propojovací kabely a tím měnili celkem dvacet písmen.
- Šéf Biura Szyfrow pozval šéfy francouzské a britské kryptoanalýzy a předvedl jim funkční bombu. S tím jim nabídl plány na výrobu bomb a dvě funkční Enigmy. Ty skončily v Anglii v Bletchley Parku, v sídle GC&CS (Goverment Code and Cypher School).

Rejewski IV- konec kryptoanalýzy

V roce 1938 němci zvýšili bezpečnost Enigmy tím, že všem operátorům dodali dva nové rotory.

- Do Enigmy bylo možno umístit kterékoliv tři z pěti rotorů v libovolné kombinaci. Tím zvýšili počet uspořádání na 60.
- Rejewski by musel postavit 10x více bomb, aby je byl schopen dešifrovat. To bylo drahé.
- Navíc němci přidali další čtyři propojovací kabely a tím měnili celkem dvacet písmen.
- Šéf Biura Szyfrow pozval šéfy francouzské a britské kryptoanalýzy a předvedl jim funkční bombu. S tím jim nabídl plány na výrobu bomb a dvě funkční Enigmy. Ty skončily v Anglii v Bletchley Parku, v sídle GC&CS (Goverment Code and Cypher School).

Nástup Turinga

4. září 1939 nastoupil do Bletchley Parku Alan Turing a začal rozvíjet práci Rejewskiho. Ta vycházela z faktu, že operátoři vysílali klíč zprávy dvakrát po sobě. To snižovalo bezpečnost Enigmy. Dalo se očekávat, že němci přestanou klíč zprávy opakovat.

- Turing si všiml, že za dobu dešifrování Enigmy shromáždili knihovnu dešifrovaných textů, které měly pevný protokol.
- Vždy v 6 hodin posílali němci zprávy o počasí, takže o zprávě po šesté ráno říct, že na konkrétním místě bude mít slovo wetter (počasí).
- Takové vazbě se říká tahák (crib).

Nástup Turinga

4. září 1939 nastoupil do Bletchley Parku Alan Turing a začal rozvíjet práci Rejewskiho. Ta vycházela z faktu, že operátoři vysílali klíč zprávy dvakrát po sobě. To snižovalo bezpečnost Enigmy. Dalo se očekávat, že němci přestanou klíč zprávy opakovat.

- Turing si všiml, že za dobu dešifrování Enigmy shromáždili knihovnu dešifrovaných textů, které měly pevný protokol.
- Vždy v 6 hodin posílali němci zprávy o počasí, takže o zprávě po šesté ráno říct, že na konkrétním místě bude mít slovo wetter (počasí).
- Takové vazbě se říká tahák (crib).

Nástup Turinga

4. září 1939 nastoupil do Bletchley Parku Alan Turing a začal rozvíjet práci Rejewskiho. Ta vycházela z faktu, že operátoři vysílali klíč zprávy dvakrát po sobě. To snižovalo bezpečnost Enigmy. Dalo se očekávat, že němci přestanou klíč zprávy opakovat.

- Turing si všiml, že za dobu dešifrování Enigmy shromáždili knihovnu dešifrovaných textů, které měly pevný protokol.
- Vždy v 6 hodin posílali němci zprávy o počasí, takže o zprávě po šesté ráno říct, že na konkrétním místě bude mít slovo wetter (počasí).
- Takové vazbě se říká tahák (crib).

Nástup Turinga II

- Turing napodobil Rejewskiho a rozhodl se pro podobné smyčky, které ale neměly nic společného s klíčem zprávy. Využíval taháky.
- Vliv propojovací desky eliminoval tak, že propojil jednotlivé „bomby“ za sebou.
- Turingova bomba stála 100 000 liber, první Victory, pak Agnus Dei.

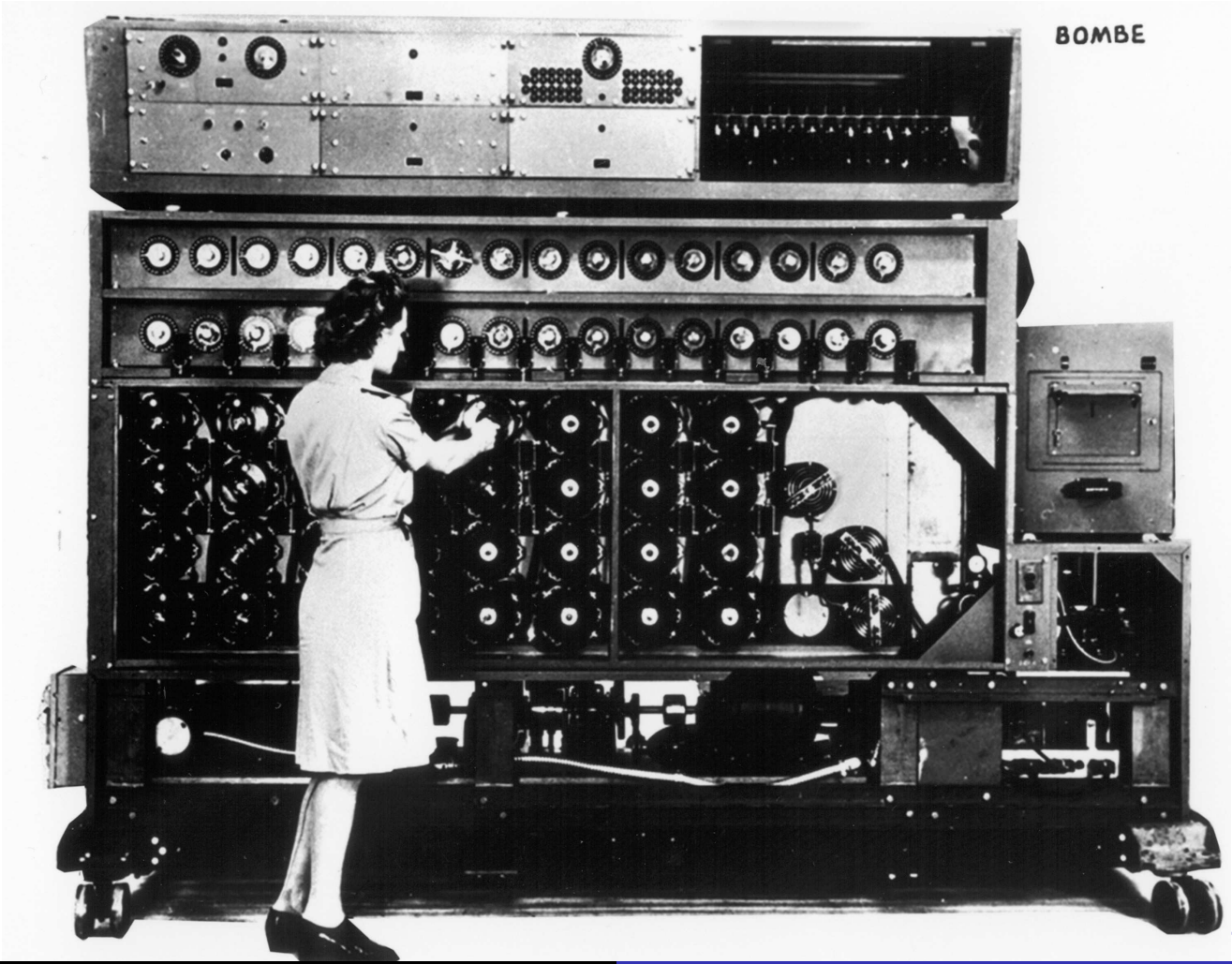
Zvěst o Turingově průlomu znamenala, že vedoucí kryptoanalytici GC&CS začali považovat Turinga za prvotřídního odborníka a génia, ale nikdo mimo Goverment Code and Cypher School neměl ani ponětí o Turingově výkonu. Vše vše co souviselo s Bletchley Parkem bylo přísně tajné.

Nástup Turinga II

- Turing napodobil Rejewskiho a rozhodl se pro podobné smyčky, které ale neměly nic společného s klíčem zprávy. Využíval taháky.
- Vliv propojovací desky eliminoval tak, že propojil jednotlivé „bomby“ za sebou.
- Turingova bomba stála 100 000 liber, první Victory, pak Agnus Dei.

Zvěst o Turingově průlomu znamenala, že vedoucí kryptoanalytici GC&CS začali považovat Turinga za prvotřídního odborníka a génia, ale nikdo mimo Goverment Code and Cypher School neměl ani ponětí o Turingově výkonu. Vše vše co souviselo s Bletchley Parkem bylo přísně tajné.

Nástup Turinga III- Bomba



Lorenz

Němci měli mnohem sofistikovanější šifru Lorenz, kterou šifrovali pomocí stroje nazývaným Tunny. Operátor zadával na klávesnici otevřený text, zařízení jej automaticky šifrovalo a na druhé straně pak vystupoval opět otevřený text.

- První zprávy šifrované Tunny byly zachyceny v červnu 1941.
- Nejpre se dešifrovaly elektromechanickým strojem Heath Robinson.
- Následně prvním elektronickým počítačem na světě názvaným Colossus. Byl sestaven z 1600 elektronek.

Lorenz

Němci měli mnohem sofistikovanější šifru Lorenz, kterou šifrovali pomocí stroje nazývaným Tunny. Operátor zadával na klávesnici otevřený text, zařízení jej automaticky šifrovalo a na druhé straně pak vystupoval opět otevřený text.

- První zprávy šifrované Tunny byly zachyceny v červnu 1941.
- Nejpre se dešifrovaly elektromechanickým strojem Heath Robinson.
- Následně prvním elektronickým počítačem na světě názvaným Colossus. Byl sestaven z 1600 elektronek.

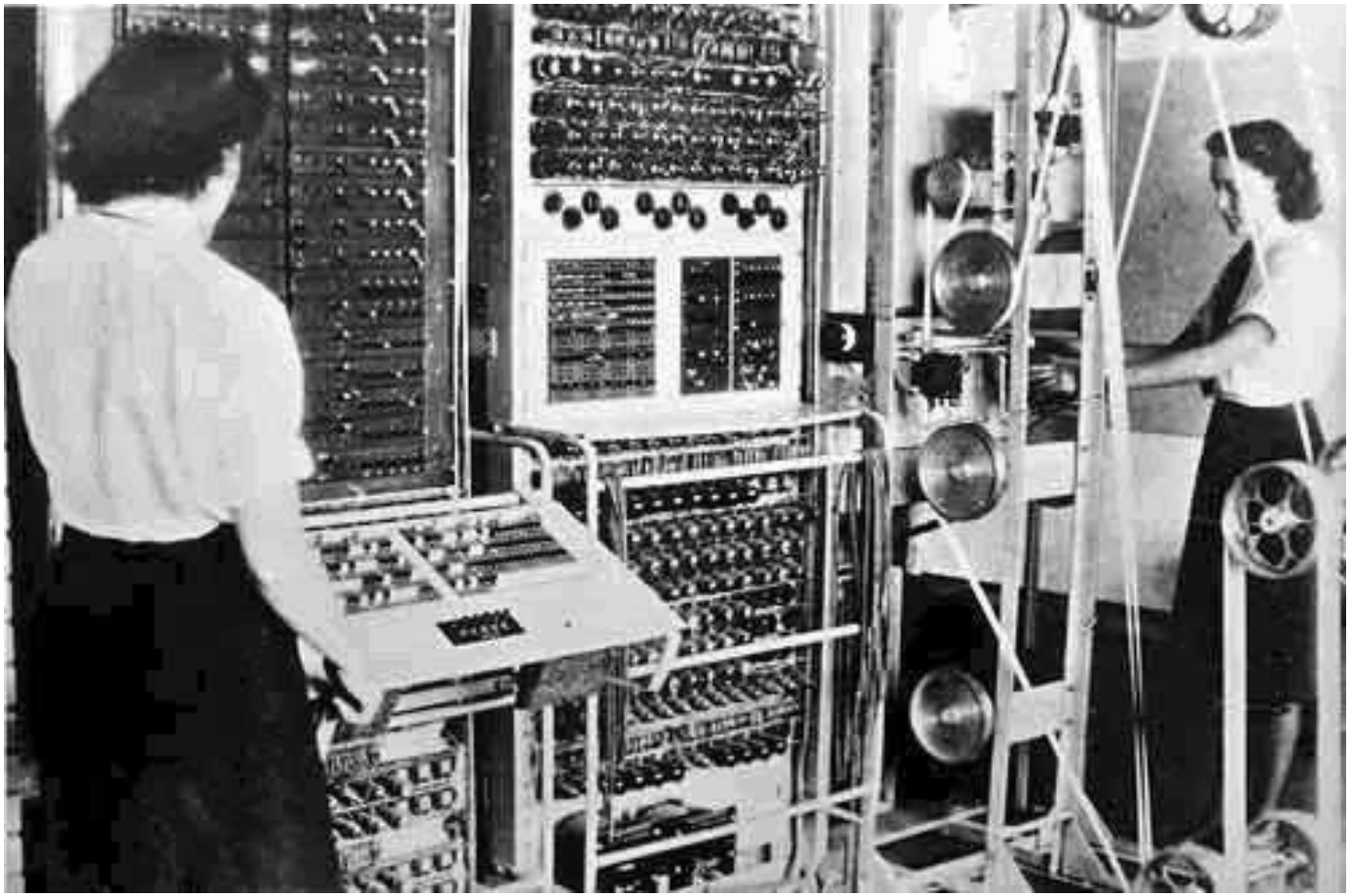
Colossus

- Konstrukci tohoto počítače zahájil Turing s Thomas H. Flowersem lednu 1943. V prosinci téhož roku jej uvedli do provozu.
- První programovatelný počítač na světě, i když neuměl například desítkové násobení.
- Colossus byl po válce zničen, nesmělo se o něm mluvit ani psát.
- Prvenství elektronického počítače přiznáno univerzitě v Pelsylvánii, 1946 vytvořili Electronic Numerical Integrator And Computer (ENIAC).
- Byl složen z 18 000 elektronek a potřeboval 150 kW energie, každý den bylo nutno najít a vyměnit 50 vadných elektronek.

Colossus

- Konstrukci tohoto počítače zahájil Turing s Thomas H. Flowersem lednu 1943. V prosinci téhož roku jej uvedli do provozu.
- První programovatelný počítač na světě, i když neuměl například desítkové násobení.
- Colossus byl po válce zničen, nesmělo se o něm mluvit ani psát.
- Prvenství elektronického počítače přiznáno univerzitě v Pelsylvánii, 1946 vytvořili Electronic Numerical Integrator And Computer (ENIAC).
- Byl složen z 18 000 elektronek a potřeboval 150 kW energie, každý den bylo nutno najít a vyměnit 50 vadných elektronek.

Colossus II



Riemannova hypotéza

- Riemannova hypotéza se týká netriviálních nulových bodů funkce Zeta $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$.
- Tvrdí, že všechny tyto body (kterých je nekonečně mnoho) leží ve středu kritického pásu $0 < Re(s) < 1$ ($Re(s) = \frac{1}{2}$).
- Mimo netriviální nulové body existují triviální nulové body. Jsou to $s = -2, -4, -6, \ldots$.
- Do dnešního dne nebyla Riemannova hypotéza ani potvrzena ani vyvrácena.
- Jedná se o jediný problém z 23 matematických problémů vybraných Hilbertem v roce 1900 a jedním ze sedmi, na který vypsal Clayův matematický institut odměnu za jejich potvrzení nebo vyvrácení.
- Turing koketoval s myšlenkou, že je RH nedokazatelná.

Riemannova hypotéza

- Riemannova hypotéza se týká netriviálních nulových bodů funkce Zeta $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$.
- Tvrdí, že všechny tyto body (kterých je nekonečně mnoho) leží ve středu kritického pásu $0 < Re(s) < 1$ ($Re(s) = \frac{1}{2}$).
- Mimo netriviální nulové body existují triviální nulové body. Jsou to $s = -2, -4, -6, \ldots$.
- Do dnešního dne nebyla Riemannova hypotéza ani potvrzena ani vyvrácena.
- Jedná se o jediný problém z 23 matematických problémů vybraných Hilbertem v roce 1900 a jedním ze sedmi, na který vypsal Clayův matematický institut odměnu za jejich potvrzení nebo vyvrácení.
- Turing koketoval s myšlenkou, že je RH nedokazatelná.

Riemannova hypotéza II

- Ve třicátých letech Titchmarsh spočítal, že 1041 v rozsahu $0 < Im(s) < 1468$, všechny vyhovují Riemannově hypotéze.
- Turing byl první, kdo využil k výpočtu funkce Zeta elektronický počítač.
- V roce 1950 použil počítač Manchester Mark I a rozšířil Titchmarshův výsledek na 1104 nulových bodů v rozsahu $0 < Im(s) < 1540$.
- Tyto nulové body počítal Manchester Mark I od tří hodin odpoledne do osmi hodin ráno.

Riemannova hypotéza II

- Ve třicátých letech Titchmarsh spočítal, že 1041 v rozsahu $0 < Im(s) < 1468$, všechny vyhovují Riemannově hypotéze.
- Turing byl první, kdo využil k výpočtu funkce Zeta elektronický počítač.
- V roce 1950 použil počítač Manchester Mark I a rozšířil Titchmarshův výsledek na 1104 nulových bodů v rozsahu $0 < Im(s) < 1540$.
- Tyto nulové body počítal Manchester Mark I od tří hodin odpoledne do osmi hodin ráno.

Riemannova hypotéza III

- Důležitější je Turingův předválečný výpočet 1054 nulových bodů v rozsahu $2\pi 63^2 \geq Im(s) \geq 2\pi 64^2$. Všechny leží na kritické přímce. $2\pi 63^2$ je přibližně 25 000.
- Všechny výpočty netriviálních nulových bodů až do dnešní doby se provádí Turingovou metodou.
- Víme, že Riemannova hypotéza platí pro prvních 10^{13} nulových bodů, několik desítek miliard nulových bodů okolo řádu 10^{23} a 10^{24} a několik stovek nulových bodů okolo řádu 10^{32}.

Riemannova hypotéza III

- Důležitější je Turingův předválečný výpočet 1054 nulových bodů v rozsahu $2\pi 63^2 \geq Im(s) \geq 2\pi 64^2$. Všechny leží na kritické přímce. $2\pi 63^2$ je přibližně 25 000.
- Všechny výpočty netriviálních nulových bodů až do dnešní doby se provádí Turingovou metodou.
- Víme, že Riemannova hypotéza platí pro prvních 10^{13} nulových bodů, několik desítek miliard nulových bodů okolo řádu 10^{23} a 10^{24} a několik stovek nulových bodů okolo řádu 10^{32}.

Manchester I

- Od roku 1948 vyučoval na univerzitě v Manchesteru, byl členem Matematického oddělení v Národní fyzikální laboratoři a pracoval pro GCHQ.
- Seznámil se s článkem Von Neumanna „První náčrt zprávy o EDVACu“. Na jeho základě vypracoval plán na Automatic Computing Engine, ACE.
- Počítače Turing prakticky využíval v 50. letech, kdy pracoval na teoretickém vysvětlení morfogeneze.
- Je autorem prvního šachového programu TurboChamp. Partie TurboChamp vs. Alick Glennie, 1951.
- TurboChamp se pokusil neúspěšně spustit i na Manchester Mark 1.

Manchester I

- Od roku 1948 vyučoval na univerzitě v Manchesteru, byl členem Matematického oddělení v Národní fyzikální laboratoři a pracoval pro GCHQ.
- Seznámil se s článkem Von Neumanna „První náčrt zprávy o EDVACu“. Na jeho základě vypracoval plán na Automatic Computing Engine, ACE.
- Počítače Turing prakticky využíval v 50. letech, kdy pracoval na teoretickém vysvětlení morfogeneze.
- Je autorem prvního šachového programu TurboChamp. Partie TurboChamp vs. Alick Glennie, 1951.
- TurboChamp se pokusil neúspěšně spustit i na Manchester Mark 1.

Manchester II

- 1952 se v souvislosti s krádeží v Turingově domě policie dověděla o jeho vztahu s devatenáctiletým Arnoldem Murrayem z Manchesteru.
- To bylo ve Velké Británii do roku 1994 trestné. Proto mu byl odepřen další přístup k utajovaným informacím.
- Turing byl zatčen a 31. března 1952 odsouzen. Musel volit mezi ročním vězením nebo probací (organo-therapic treatment).
- Mohl přednášet, ale nedostal vízum do Ameriky, kde chtěl spolupracovat s Von Neumannem.

Manchester II

- 1952 se v souvislosti s krádeží v Turingově domě policie dověděla o jeho vztahu s devatenáctiletým Arnoldem Murrayem z Manchesteru.
- To bylo ve Velké Británii do roku 1994 trestné. Proto mu byl odepřen další přístup k utajovaným informacím.
- Turing byl zatčen a 31. března 1952 odsouzen. Musel volit mezi ročním vězením nebo probací (organo-therapic treatment).
- Mohl přednášet, ale nedostal vízum do Ameriky, kde chtěl spolupracovat s Von Neumannem.

Manchester III

- 7. června 1954 Turing zemřel na otravu kyanidem draselným. Tím mělo být napuštěno jablko, kterého snědl několik soust.
- Přítomnost kyanidu v jablku nebyla testována. Jako příčina smrti byl kyanid určen až při pitvě.
- Podle oficiálně se jednalo o sebevraždu, čímž byly odmítnuty spekulace o náhodě nebo o vraždě.

Manchester III

- 7. června 1954 Turing zemřel na otravu kyanidem draselným. Tím mělo být napuštěno jablko, kterého snědl několik soust.
- Přítomnost kyanidu v jablku nebyla testována. Jako příčina smrti byl kyanid určen až při pitvě.
- Podle oficiálně se jednalo o sebevraždu, čímž byly odmítnuty spekulace o náhodě nebo o vraždě.

Manchester III

- 7. června 1954 Turing zemřel na otravu kyanidem draselným. Tím mělo být napuštěno jablko, kterého snědl několik soust.
- Přítomnost kyanidu v jablku nebyla testována. Jako příčina smrti byl kyanid určen až při pitvě.
- Podle oficiálně se jednalo o sebevraždu, čímž byly odmítnuty spekulace o náhodě nebo o vraždě.

Turingovo ocenění

- Na počest Turinga je od roku 1966 udílena Turingova cena, jedno z nejvýznamnějších informatických ocenění.
- 1999 časopis Time označil Turinga jako jednoho ze 100 nejdůležitějších lidí 20. století za přínos k rozvoji umělé inteligence a počítačů.
- 2007 byla zhotovena plně funkční replika Colossus Mark 2.

Turingovo ocenění

- Na počest Turinga je od roku 1966 udílena Turingova cena, jedno z nejvýznamnějších informatických ocenění.
- 1999 časopis Time označil Turinga jako jednoho ze 100 nejdůležitějších lidí 20. století za přínos k rozvoji umělé inteligence a počítačů.
- 2007 byla zhotovena plně funkční replika Colossus Mark 2.

Turingovo ocenění

- Na počest Turinga je od roku 1966 udílena Turingova cena, jedno z nejvýznamnějších informatických ocenění.
- 1999 časopis Time označil Turinga jako jednoho ze 100 nejdůležitějších lidí 20. století za přínos k rozvoji umělé inteligence a počítačů.
- 2007 byla zhotovena plně funkční replika Colossus Mark 2.

Snaha o rehabilitaci

- V září 2009 se britský premiér Gordon Brown jménem vlády omluvil Alanu Turingovi za příkoří, které mu bylo způsobeno.
- V prosinci 2011 byla na stránce Direct Gov vytvořena petice, která žádala, aby byl Turing omilostněn. Získala přes 43 tisíc podpisů.
- Lord McNally, tehdejší tajemník Ministerstva spravedlnosti, se jí odmítl zabývat: Turing byl „náležitě odsouzen“.
- Veřejná kampaň za Turingovo očištění trvala roky. Podporovali ji např. bývalý premiér Británie Gordon Brown a slavný vědec Stephen Hawking.

Snaha o rehabilitaci

- V září 2009 se britský premiér Gordon Brown jménem vlády omluvil Alanu Turingovi za příkoří, které mu bylo způsobeno.
- V prosinci 2011 byla na stránce Direct Gov vytvořena petice, která žádala, aby byl Turing omilostněn. Získala přes 43 tisíc podpisů.
- Lord McNally, tehdejší tajemník Ministerstva spravedlnosti, se jí odmítl zabývat: Turing byl „náležitě odsouzen“.
- Veřejná kampaň za Turingovo očištění trvala roky. Podporovali ji např. bývalý premiér Británie Gordon Brown a slavný vědec Stephen Hawking.

Snaha o rehabilitaci

- V září 2009 se britský premiér Gordon Brown jménem vlády omluvil Alanu Turingovi za příkoří, které mu bylo způsobeno.
- V prosinci 2011 byla na stránce Direct Gov vytvořena petice, která žádala, aby byl Turing omilostněn. Získala přes 43 tisíc podpisů.
- Lord McNally, tehdejší tajemník Ministerstva spravedlnosti, se jí odmítl zabývat: Turing byl „náležitě odsouzen“.
- Veřejná kampaň za Turingovo očištění trvala roky. Podporovali ji např. bývalý premiér Británie Gordon Brown a slavný vědec Stephen Hawking.

Rehabilitace I

- 23. června 2012 uplynulo 100 let od Turingova narození. Universitě v Manchesteru upořádala na jeho počest konferenci, kde byla celá řada osobností světa IT (David Ferrucci z IBM nebo „otec internetu“ Vint Cerf).
- Zde Turingův šachový algoritmus TruboChapm sehrál další partii, tentokrát na počítači. Protihráč byl nejlepší šachista dosavadní historie Garry Kasparov (jehož prohra s počítačem Deep Blue v roce 1997 byla dalším milníkem v historii počítačového šachu).
- The Register s odkazem na Turinga poznamenal, že Kasparov lidské hráče snadno poráží a v tomto smyslu TurboChamp vlastně úspěšně složil Turingův test inteligence.

Rehabilitace I

- 23. června 2012 uplynulo 100 let od Turingova narození. Universitě v Manchesteru upořádala na jeho počest konferenci, kde byla celá řada osobností světa IT (David Ferrucci z IBM nebo „otec internetu“ Vint Cerf).
- Zde Turingův šachový algoritmus TruboChapm sehrál další partii, tentokrát na počítači. Protihráč byl nejlepší šachista dosavadní historie Garry Kasparov (jehož prohra s počítačem Deep Blue v roce 1997 byla dalším milníkem v historii počítačového šachu).
- The Register s odkazem na Turinga poznamenal, že Kasparov lidské hráče snadno poráží a v tomto smyslu TurboChamp vlastně úspěšně složil Turingův test inteligence.

Rehabilitace I

- 23. června 2012 uplynulo 100 let od Turingova narození. Universitě v Manchesteru upořádala na jeho počest konferenci, kde byla celá řada osobností světa IT (David Ferrucci z IBM nebo „otec internetu“ Vint Cerf).
- Zde Turingův šachový algoritmus TruboChapm sehrál další partii, tentokrát na počítači. Protihráč byl nejlepší šachista dosavadní historie Garry Kasparov (jehož prohra s počítačem Deep Blue v roce 1997 byla dalším milníkem v historii počítačového šachu).
- The Register s odkazem na Turinga poznamenal, že Kasparov lidské hráče snadno poráží a v tomto smyslu TurboChamp vlastně úspěšně složil Turingův test inteligence.

Rehabilitace II

- 24. 12. 2013 byla Turingovi udělena královská milost. Byl tím zbaven všech obvinění.
- Milost se většinou v Británii uděluje pouze, když se obvinění ukáže jako neplatné, nebo pokud o něj požádá rodina na základě nevinnosti pachatele.
- Ministr spravedlnosti má právo požádat královnu o milost, když předchozí dva způsoby nelze použít.

Rehabilitace III

Ministr spravedlnosti Velké Británie Chris Grayling: „Doktor Alan Turing byl mimořádný muž, s mimořádnou myslí. Jeho genialita pomohla ukončit válku a zachránila tisíce životů. Jeho pozdější život byl zastíněn jeho odsouzením za homosexualitu. Tento rozsudek bychom nyní považovali za nespravedlivý a diskrimační a proto byl rozsudek odvolán. Turing si zaslouží být uznáván za jeho přínosy ve válečném tažení a ve vědě o počítačích. Milost od královny je adekvátní hold tomuto skvělému muži.“

Závěr

- P. Tatchell: „Přestože nemám žádný důkaz, že byl zavražděn, myslím si, že musíme prozkoumat možnost, že mohl být zabit bezpečnostními službami. Bylo na něj nahlíženo jako na velké bezpečnostní riziko.“
- Glyn Hughes, tvůrce památníku Alana Turinga v Manchesteru: „Považuji za velmi potěšující, že mu byla konečně udělena milost. Když jsme začali se snahou učinit ho slavným, zajistit uznání, bylo velmi složité sehnat peníze,“ řekl. „Žádná z velkých počítačových firem nechtěla na jeho památník přispět ani cent. Teď by to možná udělaly.“

Dotazy?
Děkuji za pozornost.

Závěr

- P. Tatchell: „Přestože nemám žádný důkaz, že byl zavražděn, myslím si, že musíme prozkoumat možnost, že mohl být zabit bezpečnostními službami. Bylo na něj nahlíženo jako na velké bezpečnostní riziko.“
- Glyn Hughes, tvůrce památníku Alana Turinga v Manchesteru: „Považuji za velmi potěšující, že mu byla konečně udělena milost. Když jsme začali se snahou učinit ho slavným, zajistit uznání, bylo velmi složité sehnat peníze,“ řekl. „Žádná z velkých počítačových firem nechtěla na jeho památník přispět ani cent. Teď by to možná udělaly.“

Dotazy?
Děkuji za pozornost.

Závěr

- P. Tatchell: „Přestože nemám žádný důkaz, že byl zavražděn, myslím si, že musíme prozkoumat možnost, že mohl být zabit bezpečnostními službami. Bylo na něj nahlíženo jako na velké bezpečnostní riziko.“
- Glyn Hughes, tvůrce památníku Alana Turinga v Manchesteru: „Považuji za velmi potěšující, že mu byla konečně udělena milost. Když jsme začali se snahou učinit ho slavným, zajistit uznání, bylo velmi složité sehnat peníze,“ řekl. „Žádná z velkých počítačových firem nechtěla na jeho památník přispět ani cent. Teď by to možná udělaly.“

Dotazy?

Děkuji za pozornost.

Závěr

- P. Tatchell: „Přestože nemám žádný důkaz, že byl zavražděn, myslím si, že musíme prozkoumat možnost, že mohl být zabit bezpečnostními službami. Bylo na něj nahlíženo jako na velké bezpečnostní riziko.“
- Glyn Hughes, tvůrce památníku Alana Turinga v Manchesteru: „Považuji za velmi potěšující, že mu byla konečně udělena milost. Když jsme začali se snahou učinit ho slavným, zajistit uznání, bylo velmi složité sehnat peníze,“ řekl. „Žádná z velkých počítačových firem nechtěla na jeho památník přispět ani cent. Teď by to možná udělaly.“

Dotazy?
Děkuji za pozornost.