FAKULTA
APLIKOVANÝCH VĚD
ZÁPADOČESKÉ
UNIVERZITY
V PLZNI

Semestrální práce z KKY/HKUI

GORDON WELCHMAN

Pavla Sedláčková

19. 11. 2017

Gordon Welchman

Gordon Welchman - významný britský matematik a kryptoanalytik - se narodil 15. června 1906 v anglickém Bristolu a zemřel 8. října 1985 v Newburyportu (Massachusetts, USA). Jeho jméno je dnes i přes jeho velký přínos k tzv. počítačové revoluci téměř neznámé. Důvodem je skutečnost, že celý život pracoval na projektech, které podléhaly přísnému utajení.

V období druhé světové války byl zaměstnán spolu s nejvýznamnějšími matematiky své doby ve vládním kryptoanalytickém středisku Government Code and Cypher School (GC&CS) v Bletchley Park. Jejich úkolem bylo prolomit jedny z nejsložitějších šifer všech dob - německé zprávy kódované přístrojem Enigma. Enigma byla srdcem komunikačního systému Hitlerových armád, její kódovací systém byl považován za neprolomitelný. K převodu zpráv do tajné šifry používala kombinaci rotujících disků a elektrických obvodů, v závislosti na složitosti zprávy mohl stroj pro jeden text vytvořit téměř 159 triliónů různých kombinací.[1] Nastavení se navíc každý den o půlnoci měnilo.

K úspěšnému pokoření Enigmy a tím i k významnému zkrácení války přispěl vynález Welchmanova podřízeného Alana Turinga. Jednalo se o první počítač - stroj, který dokázal procházet množství kombinací nastavení Enigmy. První prototypy Turingova stroje přezdívaného Bomba však pracovaly příliš dlouho, takže nalezení správného kódu mohlo trvat hodiny i dny. Byl to právě Gordon Welchman, kdo vylepšením Bomby o tzv. diagonální desku zkrátil významně dobu výpočtu, čímž se teprve stal stroj skutečně použitelným.[2]

Welchman se však ve své práci neomezoval jen na prolomení šifer. Pochopil důležitost sledování způsobu komunikace a spojení nepřátelských vojsk. Všiml si, že německé zprávy začínají nezašifrovanou kombinací znaků, ja-

kousi adresou, která identifikovala od koho zpráva je a komu je určena. Začal tyto značky sledovat a analyzoval, kdo komu zprávy posílá a kde se tito účastníci nacházejí. Dokázal tak po čase určit přesnou pozici a sílu stovek německých armádních a leteckých formací. Jak se po letech sám Welchman vyjádřil pro televizi BBC: "Zdálo se, že ten potencionálně zlatý důl nikoho jiného nezajímal. Tak jsem přišel s podrobným plánem na průzkum spolupráce rádiového odposlechu, analýzy zachyceného provozu, dešifrování kódu z Enigmy, dekódování zpráv psaných prolomeným kódem a zpravodajského zpracování takto získaných informací."[3] Položil tím základ tzv. analýzy provozu a komunikačního zpravodajství. Dnes se obdobné metody používají např. pro analýzu sítí.

Po skončení války se Welchman rozhodl opustit Británii a odstěhovat se do USA, kde později získal i americké občanství. Měl pocit, že ve válkou zničené Británii by nemohl nadále rozvíjet svůj potenciál, což pro Ameriku neplatilo. Přestože právě válka skončila, Spojené státy se velmi obávaly nové hrozby z Ruska. Začátek konfliktu, dnes známého pod pojmem studená válka, přiměl USA k dalšímu zbrojení a k vývoji nových vojenských technologií. Nově vznikající institut The MITRE Corporation v americkém Massachusetts, zaměřený právě na vývoj tajných vojenských technologií, projevil o Welchmanovy zkušenosti velký zájem. Welchman získal americké občanství a nejvyšší stupeň bezpečnostní prověrky, jaká se civilním osobám udělovala.

Celé desítky let byl Welchman vázán vojenským tajemstvím k mlčení o všem, co se v období druhé světové války v Bletchley Parku odehrávalo. Slovy Simona Singha: "Přestože někteří z kryptoanalytiků přešli do GCHQ (Government Communication Headquarters), většina z nich se vrátila do svých civilních životů se závazkem mlčenlivosti, takže svou klíčovou roli ve spojeneckém válečném úsilí nemohli odhalit. Zatímco vojáci, kteří bojovali

v konvenčních bitvách, se směli pochlubit svými hrdinskými činy, kryptoanalytici, kteří sváděli intelektuální bitvy s nemenším významem, museli čelit zahanbení, že na otázky o svých válečných aktivitách nemohli odpovědět jinak než vyhýbavě."[4] Teprve v roce 1974 - téměř třicet let po skončení války - se rozhodla britská vláda promluvit o dosud neznámých hrdinech a zveřejnit informace o jejich významném přispění ke zkrácení války. Byla vydána vládou schválená kniha Frederica Winterbothama The Ultra Secret.[5] Ta poprvé odhalila světu roli, kterou ve vítězství nad nacisty sehrála kryptoanalýza. Welchman se mylně domníval, že konečně může promluvit, a začal sám sepisovat knihu vzpomínek. Do této doby dokonce ani jeho nejbližší rodinní příslušníci netušili, co vlastně za války dělal, a jaký přínos měla jeho činnost pro celý svět. V roce 1982 vydal knihu "The Hut Six Story - breaking the Enigma code"[6]. Byl však obviněn z porušení vojenského tajemství a z porušení paragrafu o nepovoleném sdílení kryptoanalytických tajemství zákona o špionáži, protože údajně zveřejnil detaily, které stále podléhaly utajení.

"Poslední tři roky života, naplněného hvězdnou kariérou, strávil bojem s nemocí, bojem o vlastní reputaci a s pocitem, že byl odvržen světem, který pomáhal vybudovat..."[7]

Reference

[1] GREENBERG, Joel. *Gordon Welchman - Bletchley Park's Architect of Ultra Intelligence*
Frontline Books, 2014

[2] LENDL, Christian. *Bletchley Park - British Cryptanalysis during World War II*
eBook, 2012

[3] *Tajná válka*
Dokumentární seriál BBC, 1977

[4] SINGH, Simon. *Kniha kódů a šifer - Utajování od starého Egypta po kvantovou kryptografii*
Dokořán, 2003

[5] WINTERBOTHAM, Frederic. *The Ultra Secret*
Weidenfeld and Nicolson, 1974

[6] WELCHMAN, Gordon. *The Hut Six Story - breaking the Enigma code*
McGraw-Hill, 1982

[7] *Muž, který rozluštil Hitlerovy šifry*
Filmový dokument USA, 2015