Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 10, číslo 10/2008 **15. října 2008**

10/2008

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1260 registrovaných odběratelů)

Obsah :

Příloha: simulátor historického šifrátoru Lorenz SZ 40, lorenz.zip

A. Podzimní *Soutěž v luštění 2008* začíná

Pavel Vondruška (pavel.vondruska@crypto-world.info)

Úvodní informace k soutěži

Letošní soutěž je doprovázena fiktivním příběhem z druhé světové války. Celý příběh, tak jako soutěž, se odehrává kolem snahy vyluštit důležitou depeši odvysílanou 15.října 1941. Depeše je zašifrována pomocí nového německého šifrátoru SZ 40. Řešitelé mohou použít funkční simulátor, který je přílohou k tomuto časopisu a časem bude volně dostupný na domovské stránce. Simulátor šifrátoru sestavil a naprogramoval můj student Petr Veselý v rámci letošní bakalářské práce na MFF UK. Část z jeho rozsáhlé práce je dostupná v tomto e-zinu pod názvem Příběh šifrovacího stroje Lorenz SZ.

Pravidla

Soutěž začala 15.10.2008 rozesláním e-mailu s výzvou k soutěži všem odběratelům e-zinu Crypto-World a končí v listopadu 2008 (přesný den bude uveden dodatečně). Zúčastnit soutěže se může pouze odběratel e-zinu Crypto-World. Vstup na stránku soutěže bude přes domovskou stránku Crypto-Worldu - ikona Soutěže nebo přímým voláním stránky soutěže http://soutez2008.crypto-world.info.

Při registraci musí řešitel zadat kód soutěže 2008, který mu byl zaslán společně s výzvou k soutěži 15. 10. 2008 (kód soutěže 2008 bude zaslán i všem nově registrovaným odběratelům e-zinu Crypto-World, kteří se během soutěže k jeho odběru přihlásí).

Soutěžící při registraci zadá své uživatelské jméno (login), autentizační heslo pro opětovné přihlášení a e-mail, na který mu je zasílán e-zin Crypto-World. Tento e-mail se dále na stránce nezobrazuje a je pro ostatní návštěvníky soutěže nedostupný. Slouží k odesílání pokynů a informací soutěžícím a k ověření, že uživatel je registrovaným odběratelem e-zinu.

Soutěžní úlohy budou letos zpřístupňovány po etapách. K některým úlohám budou zveřejněny dodatečné nápovědy, které ulehčí jejich vyluštění resp. jejich dešifraci. Nápovědy budou zveřejňovány v sekci Crypto-NEWS. Za vyřešení úlohy se připisují soutěžícímu body. Registrovaný řešitel zadává své odpovědi přes www rozhraní (vždy velkými písmeny)!
Zadává se "klíčové" slovo z vyluštěného textu, pomoc s výběrem klíčového slova bude uvedena v nápovědě, která bude zveřejněna v Crypto-NEWS a na stránce soutěže. Odpověď bude automaticky vyhodnocena a řešitel se ihned dozví, zda odpověděl správně nebo ne.

Na stránce soutěže bude průběžně zveřejňován aktuální stav. U každého řešitele bude v celkovém žebříčku uveden počet dosažených bodů a lze se podívat i na pořadí, ve kterém soutěžící úlohy vyřešil. O pořadí soutěžících rozhoduje celkový počet dosažených bodů, v případě rovnosti bodů je rozhodující, kdo dosáhl tohoto počtu bodů dříve! V případě, že soutěžící ještě nezískali žádné body, jsou uvedeni podle pořadí registrace.

Pro určení celkového pořadí je rozhodující stav v době oficiálního ukončení soutěže. První tři řešitelé získají cenu automaticky. Další ceny se vylosují mezi řešitele, kteří dosáhnou alespoň patnáct bodů.

Ceny

Děkujeme všem sponzorům soutěže: Zoner Press, BUSLab, SOOM, Crypto-World. Ceny byly představeny v minulém e-zinu 9/2008 a můžete se s nimi také seznámit na webu soutěže: http://soutez2008.crypto-world.info/index.php?crypto=ceny

Všem účastníkům soutěže přeji příjemnou zábavu a samozřejmě i hodně úspěchů!

B. John Wellington vzpomíná, pokračování příběhu

Pavel Vondruška (pavel.vondruska@crypto-world.info)

John Wellington si uvařil svůj oblíbený assamský čaj, posadil se do křesla z konce 18. století, což byla jedna z mála věcí, které z rodového majetku zdědil a ve kterém tak rád odpočíval a vzpomínal na svůj život. Zadíval se na zeď, kde byla jeho fotografie v uniformě důstojníka z druhé světové války. Pod fotografií viselo vysoké válečné vyznamenání CBE (Commander of the Order of the British Empire), které mu bylo na konci roku 1941 uděleno za zásluhy. Pomyslel si: „Škoda, že jsem tehdy nedostal Victoria Cross (VC - Viktoriin kříž – nejvyšší britské vyznamenání). Určitě jsem si jej za rozluštění zprávy z října 1945 zasloužil. Koneckonců vždyť i právě díky mému úspěchu mohl britský premiér Winston Churchill říci: „Před El Alameinem jsme nepoznali vítězství. Po El Alameinu jsme nepoznali porážku.“.“ Bitva u El Alameinu byla sice přesně o rok později než dešifroval tu zprávu, ale prvé informace o Rommelovi a jeho Afrika Korpsu měli přece Britové od něj! A je pravda, že kdyby se Němcům otevřela cesta k Suezskému průplavu a k naftovým polím Středního východu, tak kdo ví, jak by vše probíhalo… A navíc byl to přece on, kdo prvý luštil šifrátor Lorenz SZ 40! Nebýt mne a mých cenných informací a námi dodávaných zachycených depeší, tak by v Bletchley Parku nikdy tento šifrátor nedokázali luštit, tedy pokud jej vůbec luštili! Sice jeho stanice *Station Y* v Knockholtu byla i nadále úkolována, aby radiové depeše zachytávala a předávala do *Station X*, ale je otázka, zda je dokázali také dešifrovat …

Možná, že nakonec může za to, že jsem nedostal VC a nepřeřadili mne do *Station X* v Bletchley Parku, ten důstojník Hil ze SIS. Vzpomněl si, jak mu před udělením vyznamenání Hill říkal: „Víš, vedení uznalo, že tvé zásluhy jsou opravdu mimořádné a rozhodlo se Ti udělit CBE“. Hill pravděpodobně viděl v jeho očích zklamání, a tak dodal: „Možná si myslí, že kdyby Ti udělili KBE (Knight of the Order of the British Empire), bylo by ostatním kolegům a důstojníkům podezřelé za co jsi jej vlastně dostal. Sám premiér považuje výsledky, které jsme společně s Bletchley Parkem získali, za tak důležité, že se nesmí nic vyzradit o tom, že Lorenz lze za jistých okolností luštit; pochop to“.

John si dodnes pamatuje na hořkost té chvíle. Vždyť se Hill ani nezmínil, že by na velitelství uvažovali o udělení VC a navíc vyzdvihl zásluhy Bletchley Parku. Vždyť to byl přece ON, kdo zprávu vyluštil a ostatně nebýt Reise a jeho geniální pomoci, tak by si v Bletchley Parku také ani neškrtli. Tím si byl jist.

Je rok 1975, 30 let po válce a informace o Bletchley Parku byly odtajněny. O obrovském úspěchu v boji s Enigmou se již běžně píše. O tom, že by tehdy dokázali luštit také

Lorenze, nikde nic nenašel. Byl jsem tedy asi opravdu jediný, kdo alespoň některé zprávy zašifrované Lorenzem SZ 40 vyluštil. A musím o tom stále mlčet. Zasloužil bych si větší uznání a společenské ocenění. Kdyby mi alespoň tehdy dali ten Viktoriin kříž.

Jenže John Wellington se velice mýlil. V Bletchley Parku zcela nezávisle na něm dosáhli dalšího pozoruhodného výsledku. Na základě analýzy provozu (zejména jednoho náhodného výpadku) a chyby obsluhy šifrátorů, která 30. srpna 1941 odvysílala dvě depeše se shodným indikátorem *HQIBPEXEZMUG* (přezdívané podle něj „ZMUG“) se jim podařilo na základě důmyslných statistických analýz zcela rekonstruovat celé zařízení Lorenz SZ 40. Získali tak prakticky až do konce války přístup k informacím o strategických plánech nepřítele. K luštění zachycených zpráv byla zkonstruována řada zařízení zcela nové konstrukce, včetně elektronkových počítačů Colossus, prvních elektronických částečně programovatelných počítačů na světě. Toto tajemství bylo považováno za tak velké, že na konci války byly počítače Colossus na základě rozkazu Winstona Churchilla zničeny.

Teprve v roce 1976 se informace o počítačích Colossus dostaly na veřejnost a až v roce 2000 byla zpřístupněna dobová oficiální zpráva o luštění této šifry (General Report on Tunny).

Toto vše však John Wellington, který do dění v *Station X* zasvěcen nebyl, nevěděl.

John pomalu popíjí svůj zelený čaj a vzpomíná na podzim roku 1941, kdy slavil svůj největší životní triumf. Byl to ten večer, kdy si zavolal důstojníka SIS Hilla a položil před něj dešifrovaný obsah depeše, odvysílané 15.října a zašifrované do té doby zcela neznámým šifrátorem Lorenz SZ 40.

Hill předal svému pobočníkovi obsah depeše s přísným rozkazem, aby ihned cestou speciální svodky zajistil dodání k ministerskému předsedovi a zařídil předání do analytického oddělení generálního štábu. Po té usedl naproti Johnovi a souhlasil s porušením vojenských předpisů a přijal i sklenku dobré whisky. Připil si s Johnem. Poblahopřál mu a celý nedočkavý čekal na jeho vyprávění, jak se mu podařilo obsah depeše získat.

John začal pomalu vykládat. Chtěl si vychutnat tento okamžik a tak nijak nespěchal. Popisoval i to, co již Hill věděl, ale ten jej nepřerušoval. Věděl, že ten slavnostní okamžik se již nevrátí a nechával jej proto Johnovi vychutnat.

John popisoval, jak Reis oznámil, že pomocí šifrátoru SZ bude v polovině října odvysílána důležitá zpráva. Zprávu se podařilo zachytit. Zmínil se, že Reis také slíbil pomoc i s dodáním technických dat tohoto nového šifrátoru. Připomněl, že Reisovi zrovna v tuto kritickou dobu došly bločky s hesly pro bezpečné agenturní spojení.

John dokonce ocitoval část z poslední zašifrované Reisovy depeše: *„Pokud mi hesla dojdou a já nebudu moci šifrovat odesílané zprávy dohodnutým způsobem, použiji nějaký jiný, třeba slabý systém. Psát budu jen v náznacích. Informaci o nastavení šifrátoru rozdělím do více zpráv a budu je posílat po částech různými kanály. Věřím, že vše dobře poskládáte. Nemohu postupovat jinak, neboť bych se prozradil“*.

Pak začal John konečně popisovat to, co dosud Hill nevěděl. Reis skutečně do písmene splnil to, co v předchozí depeši slíbil. Během října Reis odvysílal řadu krátkých zpráv, které se podařilo zachytit, byly zašifrovány klasickými šifrovými a často i velmi slabými metodami. Tyto zprávy obsahovaly odkazy na různé články, vědecké studie, fotografie apod., které byly běžně dostupné. John je podle obsahu dešifrovaných depeší snadno vyhledal a zjistil, že se na těchto odkazech vyskytují různě dlouhé řetězce složené z 0 a 1. Tyto řetězce si John pečlivě schovával. Zpočátku netušil co s nimi. Teprve když Reis poslal technická data o šifrátoru SZ a to cestou kurýra přes Casablancu a podařilo se jej podle těchto údajů ve *Station Y* zrekonstruovat, pochopil. Odkazy vedly na vzorky kol, která byla pro odvysílání důležité zprávy použita. Jeden z odkazů vedl i na počáteční nastavení kol. Tento odkaz byl zvlášť zajímavý. Byla to náhoda, ale nastavení téměř odpovídalo telefonnímu číslu, na které pak stačilo pouze v jednom textu upozornit. Obdivoval Reise, jak využil běžně dostupná data nebo jak se mu podařilo do stávajících volně dostupných informací data nenápadně uložit. Pak již stačilo málo, naučit se SZ 40 ovládat. To, že to opravdu zvládl, si ověřil mimo jiné i dešifrováním zpráv, které Reis poslal. K zašifrování a dešifrování byly použity vzorky a nastavení, které byly uvedeny jako testovací. Nakonec všechny získané vzorky kol správně poskládal. Byl to sice malý rébus, ale vyřešil jej poměrně rychle, neboť mnoho možností nebylo. Podle dříve získané nápovědy přidal počáteční nastavení. Pak nedočkavě spustil dešifrovací mód. Jakmile se objevilo prvé slovo dešifrované depeše PATNACTEHO …., věděl, že dosáhl úspěchu. Dokončil dešifraci a zavolal Hilla. Tak a to je vše. Ukončil své vyprávění.

Hill vstal, podal Johnovi ruku a řekl: „Vlast Ti to nikdy nezapomene. Čeká Tě významné ocenění“.

John dopil. Podíval se ještě jednou na svoji fotografii a medaili, kterou za své zásluhy získal. Smutně pokýval hlavou a pomyslel si, kdybych o tom alespoň nemusel mlčet a mohl svému vnukovi vyprávět…. Proč, proboha, se třicet let po válce stále informace o luštění šifrátoru SZ 40 tají? Proč není možno říci, že depeše z října 1941 byla vyluštěna a její obsah měla britská armáda k dispozici?

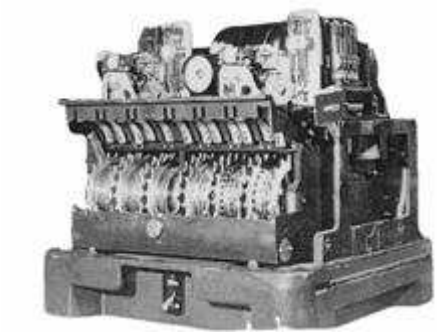
C. Příběh šifrovacího stroje Lorenz SZ

Petr Veselý, MFF UK Praha, (p.vesely@matfyz.cz)

1. Úvod

Úspěchy britských kryptoanalytiků, kteří v přísně utajeném středisku v Bletchley Parku rozbili za druhé světové války mnohé šifry používané státy Osy, dodnes přitahují pozornost laické i odborné veřejnosti. Jejich práce obsahuje příklady invenčního využití matematiky i názorné ukázky toho, jak katastrofální důsledky pro bezpečnost šifrového systému může mít nedůslednost v dodržování základních kryptografických pravidel, což ji činí stále aktuálním zdrojem inspirace a ponaučení. Kromě toho jsou teprve v posledních letech veřejnosti zpřístupňovány dobové dokumenty, které odhalují dosud neznámé informace a detaily.

Ve stínu patrně nejznámější válečné šifry Enigma dlouho zůstávala historie prolomení šifrového systému Lorenz, pracujícího na principu Vernamovy šifry, který používala německá armáda k zabezpečení dálnopisné komunikace na nejvyšší úrovni velení. Přitom tento úspěch je hodný pozornosti přinejmenším ze dvou důvodů. Zaprvé, neznámou konstrukci šifrovacího přístroje se pracovníkům Bletchley Parku podařilo odvodit pouhým zkoumáním necelých čtyř tisíc znaků pseudonáhodného klíče, které získali díky hrubé chybě německého operátora. Dosáhli toho dokonce již během zkušebního provozu šifrátoru a získali tak prakticky až do konce války přístup k informacím o strategických plánech nepřítele. Zadruhé, k luštění zachycených zpráv byla zkonstruována řada pokročilých výpočetních zařízení, včetně elektronkových počítačů Colossus, prvních elektronických částečně programovatelných počítačů na světě.



Přístroj Lorenz SZ (převzato z [1])

V posledních letech se šifra Lorenz dostává do středu zájmu a věnuje se jí odborná i populární literatura (pravděpodobně však zatím žádná v českém jazyce). Jedním z důvodů je zpřístupnění dobové oficiální zprávy o luštění této šifry, General Report on Tunny, v roce 2000. Dalším je nedávné úspěšné dokončení projektu sestavení funkční repliky počítače Colossus přímo v Bletchley Parku. Okolnosti rozbití šifrového systému Lorenz jsou tématem tohoto článku.

Druhá kapitola stručně popisuje dějiště vyprávěného příběhu a seznamuje s jeho hlavními aktéry, jimiž jsou šifrovací přístroj Lorenz SZ a kryptoanalytické středisko v Bletchley Parku.

Ve třetí části je podrobně popsán princip fungování přístroje Lorenz ve všech užívaných verzích a způsob jeho použití.

Chronologie boje britských luštitelů s šifrou Lorenz je předmětem čtvrté kapitoly.

Poslední dvě části stručně seznamují s některými konkrétními událostmi, které prolomení systému Lorenz ovlivnilo, a s poválečnými osudy Bletchley Parku.

2. Historický přehled

Během 2. světové války se německé ozbrojené síly na cestě za ovládnutím Evropy setkaly s potřebou bezpečného a spolehlivého spojení na ose mezi hlavním štábem, velitelstvími armádních skupin a jednotlivými bojovými jednotkami. Tomuto účelu sloužila řada šifrovacích přístrojů domácí výroby, které byly často modifikacemi komerčních produktů z předválečné doby. Zpravidla šlo o rotorové šifrátory, k jejichž nejvíce ceněným (a přeceňovaným) vlastnostem patřila v té době bezkonkurenční mohutnost klíčového prostoru.

Nejrozšířenějším přístrojem byla známá Enigma, která sloužila k předběžnému šifrování zpráv (off-line šifrování) před jejich odesláním běžným komunikačním kanálem, většinou Morseovou abecedou. Používalo se několik různých konstrukčních variant šifrátoru a díky své přenosnosti patřila Enigma mimo jiné do výbavy bojových útvarů nejnižší úrovně. Byly vyrobeny řádově desítky tisíc kusů.

Šifrátory řady Geheimschreiber T52 firmy Siemens & Halske AG, původně patentované v Německu a ve Spojených státech (US Patent No. 1912983, „Secret telegraph system“ z roku 1933), byly šifrovací dálnopisy založené na Vernamově principu, umožňující on-line šifrovanou komunikaci po pevné lince, později byla vyvinuta i bezdrátová verze. Tato zařízení používala především Luftwaffe a námořnictvo a bylo vyrobeno asi tisíc kusů.

Lorenz SZ40 (a následné verze SZ42A, SZ42B) vyráběný společností C. Lorenz AG byl přídavným šifrovacím modulem k bezdrátovému dálnopisu a umožňoval rovněž přenos šifrovaných zpráv on-line. Jeho konstrukce pravděpodobně nebyla veřejně známá. Používal se na citlivých linkách mezi nejvyšším velitelstvím pozemní armády v Berlíně a hlavními stany armádních skupin v okupované Evropě a severní Africe.

Šifrátor Lorenz SZ40 byl zprvu nasazen do zkušebního provozu na lince mezi Berlínem, Athénami a Soluní v červnu 1941. Zprávy byly přenášeny ve formátu přístroje Hellschreiber (zařízení funkcí podobné faxu) a na přijímající stanici tisknuty na papírovou pásku. Po více než roce zkoušek, během něhož se upravila pravidla používání přístroje, bylo v říjnu 1942 zahájeno ostré vysílání na linkách Berlín – Soluň a Královec – jižní Rusko, nyní již v Baudotově dálnopisném kódu. Komunikační linku vždy tvořily dva páry bezdrátových dálnopisů s šifrovacím modulem (po jednom přijímači a vysílači na každém konci linky), každý pár byl vybaven stejnou sadou klíčů (odlišnou od klíčů ostatních linek).

S postupem Hitlerových vojsk se otevíraly další komunikační spoje a od roku 1943 byly stroje SZ40 nahrazovány novějšími modely SZ42A. V době spojenecké invaze do Normandie v roce 1944 síť tvořilo celkem 26 linek s dvěma centrálními ústřednami ve Straußbergu u Berlína a v Královci.

Po první světové válce, v roce 1919, vznikla v Británii sloučením námořní a armádní šifrové služby nová organizace s kryptickým názvem Government Code and Cypher School (GC&CS). Jejím úkolem byl návrh bezpečných způsobů komunikace pro britskou vládu a především luštění zahraničních šifer.

V roce 1939 se GC&CS přestěhovala z bombardováním ohroženého Londýna do venkovského sídla v Bletchley Parku, 80 km severozápadně od metropole. Vzniklo tam přísně tajné kryptoanalytické středisko označované Station X. Původní smysl tohoto názvu je prozaický: šlo o v pořadí desáté zařízení zřízené v zemi tajnou službou MI6.

Zde Britové po celou válku úspěšně pracovali na luštění desítek různých šifer zemí Osy, zejména Německa. Nepřátelský rádiový provoz byl monitorován systémem odposlouchávacích stanic, tzv. Stations Y, rozmístěných po Británii (některé byly např. i v Palestině nebo Indii), a zaznamenané depeše byly dopravovány do Bletchley kurýry na motocyklech a později přímým dálnopisným spojením.

V lednu 1945 údajně ve stanici X pracovalo až 9000 lidí. Byli mezi nimi přední matematici (Alan Turing, Max Newman, William Tutte aj.), lingvisté a experti v různých oborech,

například šachisté nebo i úspěšní luštitelé náborové křížovky v Daily Telegraph. Většinu osazenstva však tvořily ženy, zejména příslušnice ženského pomocného námořního sboru (WRNS).

3. Funkce šifrovacího stroje Lorenz SZ

Obecné poznámky

Přístroj Lorenz SZ je ve všech verzích přídavným modulem bezdrátového dálnopisu (písmena SZ jsou zkratkou německého slova Schlüsselzusatzgerät, šifrovací přídavné zařízení).

Dálnopis je telekomunikační zařízení, velmi rozšířené po většinu 20. století, které vzhledem i konstrukcí připomíná elektromechanický psací stroj. Umožňuje elektronicky přenášet psaný text po lince nebo bezdrátově a tisknout zprávy vysílané jinými dálnopisy. Jednotlivé znaky jsou kódovány pětibitovým Baudotovým kódem, označovaným také ITA2 (International Telegraph Alphabet No. 2). Většina kódových slov má dva významy (Letter Shift, Figure Shift), mezi kterými se přepíná pomocí kontrolních znaků. Významy některých slov v horním registru (Figures) nejsou přesně určeny a závisí na zemi použití. Tabulka 1 ukazuje význam slov Baudotova kódu podle zmíněné zprávy General Report on Tunny [1]. Konkrétní signál odpovídající tečce či křížku závisí na podobě komunikační linky.

	Figures	NULL	5	CR	9	space	£	,	.	LF	)	4	&	8	0	:	=	3	+	□	?	´	6	%	/	-	2	□	FIG	7	1	(	LTR
	Letters		T		O		H	N	M		L	R	G	I	P	C	V	E	Z	D	B	S	Y	F	X	A	W	J		U	Q	K	
impuls	1	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	2	●	●	●	●	●	●	●	●	x	x	x	x	x	x	x	x	●	●	●	●	●	●	●	●	x	x	x	x	x	x	x	x
	3	●	●	●	●	x	x	x	x	●	●	●	●	x	x	x	x	●	●	●	●	x	x	x	x	●	●	●	●	x	x	x	x
	4	●	●	x	x	●	●	x	x	●	●	x	x	●	●	x	x	●	●	x	x	●	●	x	x	●	●	x	x	●	●	x	x
	5	●	x	●	x	●	x	●	x	●	x	●	x	●	x	●	x	●	x	●	x	●	x	●	x	●	x	●	x	●	x	●	x

Tab. 1: Baudotův kód (podle [1]). Významy kontrolních znaků: CR – carriage return; LF – line feed; FIG – přepnout na horní registr (Figure Shift); LTR – přepnout na dolní registr (Letter Shift). Znaky D a J mají v horním registru po řadě význam Kdo jsi? a zvonek

Zprávu v Baudotově kódu lze chápat jako pět tzv. impulsů. První impuls je posloupností prvních bitů znaků tvořících zprávu (vyjádřených v Baudotově kódu), druhý impuls tvoří druhé bity znaků atd. V dalším textu budou namísto teček a křížků používána po řadě čísla 0 a 1.

Typ šifry

Samotná šifra Lorenz je Vernamova typu, šifrový text je tvořen součtem otevřeného textu s pseudonáhodnou posloupností stejné délky, generovanou strojem Lorenz SZ. Sčítání jednotlivých znaků je definováno jako sčítání jejich Baudotových reprezentací po jednotlivých bitech, jak ukazuje následující příklad:

$$A+B=\begin{pmatrix}1\\1\\0\\0\\0\end{pmatrix}+\begin{pmatrix}1\\0\\0\\1\\1\end{pmatrix}=\begin{pmatrix}0\\1\\0\\1\\1\end{pmatrix}=G$$

V běžném provozu se zpráva tiskla na nekonečnou pásku, otevřený text proto nikdy neobsahoval řídicí znaky pro začátek nové řádky (CR, LF), rovněž se v něm nevyskytoval nulový znak. Pseudonáhodný klíč, a tedy i šifrový text, obsahoval všech 32 znaků kódu.

Během zkušebního provozu (červen 1941 až říjen 1942) byl text po zašifrování převeden do formátu používaného přístrojem Hellschreiber a přenášen v této formě. Hellschreiber, zařízení vynalezené v roce 1929 Rudolfem Hellem, je považován za předchůdce faxu. Přenášené znaky jsou vysílány po jednotlivých pixelech, výška řádku je 7 pixelů. Na přijímacím zařízení jsou znaky tisknuty na pásku. Jeho výhodou je především dobrá čitelnost textu i při nekvalitním spojení.

V únoru 1942 se přešlo na vysílání přímo v Baudotově kódu.

Vnitřní konstrukce stroje Lorenz SZ40

Šifrovací stroj Lorenz SZ40 je zástupcem ve své době velmi oblíbené třídy rotorových šifrovacích zařízení. Jeho hlavní část tvoří 12 rotorů na společné ose vybavených po obvodu výklopnými kolíčky. Tyto kolíčky mohou být nastaveny do dvou poloh. Svislé činné postavení kolíčku (německy označované jako Nocke, výstupek, vačka), odpovídá binární hodnotě 1 a šikmé nečinné (keine, žádná) hodnotě 0. Nastavení všech kolíčků daného kola se označuje jako vzorek tohoto kola (v anglických zdrojích je používán termín wheel pattern).

Počty kolíčků na jednotlivých kolech jsou vzájemně nesoudělné. V každém šifrovacím kroku je jeden z kolíčků každého kola aktivní, tzn. jeho nastavení ovlivňuje podobu klíče nebo další chování přístroje. Po otočení rotoru se stane aktivním následující kolíček.

Rotory lze podle funkce rozdělit do tří kategorií. Dvě pětičlenné skupiny, v Bletchley Parku označované jako kola ψ (ψ_1, ψ_2, ψ_3, ψ_4, ψ_5 o velikostech po řadě 43, 47, 51, 53 a 59) a kola χ (χ_1, χ_2, χ_3, χ_4, χ_5 o velikostech 41, 31, 29, 26 a 23) vytváří klíč, zbylá dvě tzv. kola μ (μ_1, μ_2 o velikostech 61 a 37) se nazývají řídicí (anglicky motor wheels), protože řídí otáčení rotorů.

Pořadí rotorů na ose zleva je ψ_1, ψ_2, ψ_3, ψ_4, ψ_5, μ_2, μ_1, χ_1, χ_2, χ_3, χ_4, χ_5 (některé zdroje uvádějí odlišné pořadí, v němž kola χ tvoří počáteční pětici a rotory ψ pětici koncovou).

V každém kroku šifrování přístroj vygeneruje jeden znak klíče, tedy pětibitové slovo Baudotova kódu, následujícím jednoduchým způsobem: i-tý bit je součtem nastavení aktivních kolíčků kola ψ_i a kola χ_i.

Na konci šifrovacího kroku se některé rotory otočí o jednu pozici. Otáčení se řídí těmito pravidly:

- kola χ se otáčí v každém kroku
- kolo μ_1 se otáčí v každém kroku
- kolo μ_2 se otočí pouze tehdy, je-li hodnota aktivního kolíčku μ_1 (před otočením) 1
- kola ψ se všechna otočí pouze tehdy, pokud je hodnota aktivního kolíčku μ_2 (před případným otočením) 1; v opačném případě zůstávají všechna stát

Binární posloupnost generovanou během šifrování rotorem χ_i, $1 \le i \le 5$, budeme značit rovněž symbolem χ_i. Posloupnost χ_i je tedy periodickým rozšířením vzorku daného kola. Podobně označíme $\psi_\mathbf{i}$, $1 \le i \le 5$, binární posloupnost, kterou by vytvářelo kolo $\psi_\mathbf{i}$, pokud by se otáčelo v každém kroku. Příslušnou rozšířenou sekvenci, v níž se některé prvky opakují vlivem nepravidelného pohybu kola $\psi_\mathbf{i}$, budeme značit $\psi_\mathbf{i}'$. Písmenem χ (respektive ψ, ψ') bez indexu bude označována posloupnost znaků (nebo ekvivalentně příslušných slov Baudotova kódu), jejíchž pět impulsů tvoří posloupnosti χ_i ($\psi_\mathbf{i}$, $\psi_\mathbf{i}'$).

S přihlédnutím k zavedenému značení lze šifrovací algoritmus charakterizovat rovnicí

$$\mathbf{C} = \mathbf{P} + \chi + \psi',$$

kde **C** je posloupnost šifrového textu a **P** posloupnost otevřeného textu.

Nepravidelný pohyb kol ψ měl zvýšit bezpečnost systému, avšak skutečnost, že se tyto rotory buď otáčely vždy všechny společně, nebo všechny společně stály, se ukázala být jednou z největších slabin systému. Důsledkem této vlastnosti je, že po sobě jdoucí znaky v posloupnosti ψ' jsou často shodné, díky čemuž lze tuto sekvenci odlišit od náhodné posloupnosti znaků (v praxi se při luštění využívalo nerovnoměrné distribuce bigramů v sekvenci $\mathbf{P} + \psi'$).

Klíče a nastavení přístroje

Klíč každé zprávy se skládá z několika částí, které lze rozdělit do dvou skupin. Dlouhodobý klíč tvoří vzorky kol a způsob kódování jejich počátečního nastavení. Klíč zprávy tvoří počáteční nastavení rotorů při šifrování dané zprávy.

Vzorky kol se na každé komunikační lince měnily v pravidelných intervalech. Během zkušebního provozu, tj. od června 1941 do října 1942, se měnily vzorky kol ψ_i jednou za tři měsíce, vzorky kol χ_i s měsíční frekvencí a vzorky řídicích kol μ_i každý den. Po nasazení šifrovacího přístroje do ostrého provozu byla platnost vzorků kol ψ_i zkrácena na jeden měsíc. Od 1. srpna 1944 se všechny vzorky měnily denně. Tak časté změny klíče však s blížící se německou porážkou narážely na logistické problémy. Britským kryptoanalytikům se dokonce podařilo odposlechnout a rozluštit depeše obsahující nastavení přístroje na další období, což je prohřešek proti základním kryptografickým pravidlům (kterého se ale během války dopouštěl třeba i český odboj, čehož zase s úspěchem využívali němečtí luštitelé).

Klíč zprávy, tzn. počáteční nastavení rotorů, se dohodnutým způsobem zakódoval a přenášel se pomocí indikátorové skupiny v otevřené hlavičce depeše. Během zmíněného zkušebního období měl indikátor podobu dvanácti písmen, přenášených pomocí německé hláskovací tabulky. Každému rotoru byla přiřazena jiná jednoduchá záměna vybraných počátečních pozic za písmena, která platila jeden měsíc.

Tento způsob předávání nastavení přístroje umožňoval kryptoanalytikům rozpoznat zprávy zašifrované s použitím stejného klíče (což je další porušení kryptografických pravidel, jehož se němečtí operátoři často dopouštěli), které je možné snadno rozluštit. S přibývajícím počtem rozluštěných zpráv v daném období platnosti substitucí také rostl počet písmen v indikátorech, jejichž význam byl známý, což usnadňovalo luštění dalších depeší. Byla dokonce vyvinuta metoda, jak pomocí indikátorů nalézt vzorky kol.

S přechodem k ostrému provozu byly zavedeny číselné indikátory, přičemž operátoři na obou koncích komunikační linky měli pravděpodobně k dispozici stejnou tabulku s očíslovanými nastaveními. Takový indikátor stále umožňuje rozpoznat zprávy zašifrované stejným klíčem, ale neposkytuje žádné další informace.

Vlastní klíč každé zprávy je tvořen počátečním nastavením rotorů. Během zkušebního provozu pravděpodobně radista volil počáteční nastavení kol sám (z těch, které měly substitucí přiřazeno nějaké písmeno). Po zavedení číselných indikátorů se zřejmě postupně používala nastavení z předem dohodnutého očíslovaného seznamu.

Stroj Lorenz SZ má, podobně jako jiné rotorové šifrovací stroje, obrovskou mohutnost klíčového prostoru. Možných počátečních nastavení je více než 10^{19} (takový je součin velikostí všech rotorů). Možných vzorků všech kol je teoreticky

$$2^{23+26+29+31+37+41+43+47+51+53+59+61} = 2^{501} > 10^{150}.$$

Vzorky však nelze nastavit libovolně, protože některá nastavení produkují slabou pseudonáhodnou posloupnost. Britové odhadovali počet použitelných nastavení jen vzorků kol χ na 10^{38}.

Pozdější verze přístroje

V průběhu války byly s cílem zvýšit bezpečnost šifrovacího stroje zavedeny některé úpravy způsobu řízení společného otáčení kol ψ. Všechny fungovaly na stejném principu:

v každém kroku se z vnitřního stavu přístroje spočítala jednobitová hodnota, nazývaná omezení (v anglických zdrojích limitation). Podmínka rotace kol ψ se pak upravila následujícím způsobem:

- označme binární hodnotu aktivního kolíčku μ_2 (před případným otočením) $\mathbf{m}$ a aktuální hodnotu omezení $\mathbf{l}$. Kola ψ se otočí právě tehdy, když platí

$$\mathbf{m} \vee \neg\, \mathbf{l} = 1$$

Omezení se v závislosti na verzi přístroje počítalo jako součet některých z následujících hodnot:

a = hodnota kolíčku kola χ_2 aktivního v předchozím kroku šifrování
b = hodnota kolíčku kola ψ_1 aktivního v předminulém kroku šifrování
c = hodnota 5. impulsu otevřeného textu v předminulém kroku šifrování

Poslední omezení, německy zvané Klartextfunktion, efektivně znemožňuje snadné luštění zpráv zašifrovaných stejným klíčem, protože pseudonáhodná posloupnost závisí i na otevřeném textu. Stejně efektivně ale znemožňuje dešifrování zbytku textu v případě, že dojde k chybnému přijetí některého znaku zašifrované zprávy. Tato se funkce zkušebně používala v březnu 1943 na lince mezi Římem a armádou maršála Rommela v Tunisku a poté i na linkách v Evropě v prosinci 1943 a v roce 1944, pokaždé se ale od jejího užívání upustilo (naposledy v prosinci 1944) právě kvůli problémům s dešifrací v případě nedokonalého spojení.

Následující Tabulka 2 obsahuje označení jednotlivých verzí šifrovacího stroje Lorenz SZ, datum uvedení do provozu a omezení, která implementovala.

verze přístroje	uvedení do provozu	používaná omezení
Lorenz SZ40	červen 1941	žádná
Lorenz SZ42A	únor 1943	a nebo $a + c$
Lorenz SZ42B	červen 1944	$a + b$ nebo $a + b + c$

Tab. 2: Verze šifrátoru Lorenz SZ, datum uvedení do provozu a používaná omezení

4. Úspěchy Bletchley Parku

První poznatky o šifře

Krátce po německé invazi do Ruska v červnu 1941 byla zachycena pravidelná šifrovaná rádiová komunikace mezi Vídní a Athénami, která používala formát přístroje Hellschreiber. Britští kryptoanalytici ve výzkumném oddělení Bletchley Parku na základě předcházejících cvičných zpráv na téže lince usoudili, že jde o dálnopisné spojení, a dali mu kódové označení TUNNY (německý dálnopisný provoz byl v Bletchley označován jako FISH a jednotlivé šifrové systémy i komunikační linky byly pojmenovávány po různých vodních tvorech, šifra T52 měla například krycí jméno Sturgeon). Odposlechem depeší šifrovaných novým systémem byla pověřena stanice Y v Knockholtu v Kentu jižně od Londýna.

Zprávy měly standardizovanou podobu: nešifrovaná úvodní část obsahovala číslo depeše a sekvenci dvanácti slov německé hláskovací tabulky, dvanáctipísmenný indikátor nastavení přístroje. Funkci mezery plnil znak 9, sekvence 99999 pak uvozovala vlastní šifrový text. Kromě 26 písmen standardní abecedy se v textu vyskytovaly znaky 3, 4, 8, 9, + a /.

Prvotní domněnku, že k vysílání zpráv je používán dálnopis a text poté převáděn z Baudotova kódu do formátu Hellschreiberu, potvrdilo 22. července zachycení několika zpráv, které obsahovaly pouze 16 různých znaků, přičemž z písmen abecedy se v nich vyskytovala právě ta, jejichž Baudotova reprezentace začíná nulou. Při jejich vysílání byl zřejmě dálnopis porouchaný a první bit každého znaku původní zprávy změnil na nulu. Z indikátorů zpráv, obsahujících například řetězce H/INRICH nebo TH/O3OR, bylo možné snadno odvodit Baudotovy reprezentace symbolů nepatřících mezi 26 písmen abecedy: / se kupříkladu zjevně liší od (známé) reprezentace E v hodnotě prvního bitu. Výsledkem byla následující převodní tabulka používaných znaků a jim odpovídajících slov Baudotova kódu (Tabulka 3), přičemž označení kontrolních znaků symboly 3, 4, 8, 9, + a / se v Bletchley Parku pravděpodobně používalo jako konvence i poté, co byl Hellschreiber nahrazen v únoru 1942 přímou komunikací pomocí dálnopisů.

/	T	3	O	9	H	N	M	4	L	R	G	I	P	C	V	E	Z	D	B	S	Y	F	X	A	W	J	+	U	Q	K	8
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Tab. 3: Znaky používané na lince Vídeň-Athény při komunikaci pomocí přístroje Hellschreiber a příslušná slova Baudotova kódu

Poměrně často byly zachycovány dvojice zpráv se stejným indikátorem a zašifrované tedy stejným klíčem, což je velká nedůslednost v dodržování kryptografických pravidel. Zkoumáním takových párů Britové odvodili, že použitá šifra je Vernamova typu, a snadno uhodli, jak je definováno sčítání znaků zprávy a klíče.

Opakované použití klíče je totiž největší slabinou Vernamovy šifry: jsou-li dva texty zašifrovány s použitím stejného klíče, tj. pokud platí

$$c_1 = p_1 + k,\ c_2 = p_2 + k,$$

pak rozdíl šifrových zpráv je rovný rozdílu otevřených zpráv:

$$c_1 - c_2 = (p_1 + k) - (p_2 + k) = p_1 - p_2.$$

Zná-li nebo uhodne-li útočník část jedné z otevřených zpráv, snadno pomocí uvedené rovnosti dopočítá odpovídající úsek druhé zprávy. Díky redundanci textu pak pravděpodobně dokáže rozšířit známé části otevřených textů a v ideálním případě tak vyluštit obě zprávy. Současně s nimi získá i použitý klíč *k*.

Zde Britům naopak pomohla německá důslednost. Vysílané depeše měly zpravidla ustálené hlavičky, například SPRUCHNUMMER, číslo zprávy. Pracovníci Bletchley Parku si toho byli vědomi a hádání částí zpráv pro ně tedy nebyl problém. Dlouho se však nedařilo získat dostatečně dlouhý úsek klíče, ze kterého by bylo možné zjistit funkci pseudonáhodného generátoru. Ještě před koncem testovacího období jim k tomu však Němci sami poskytli solidní příležitost.

HQIBPEXEZMUG

Dne 30. srpna 1941 byly zachyceny dvě depeše se shodným indikátorem HQIBPEXEZMUG (přezdívané podle něj „ZMUG“), kratší z nich měla délku 3976 znaků. Tyto zprávy se shodovaly v prvních 7 znacích. Byl spočten rozdíl šifrových textů a jako

začátek otevřeného textu jedné ze zpráv bylo vyzkoušeno zmíněné slovo SPRUCHNUMMER, výsledkem byl řetězec SPRUCHNR9++U na začátku druhé depeše.

Tyto dvě zprávy byly až na několik nejistých znaků vyluštěny v celé délce kratší zprávy, o což se dvouměsíční prací zasloužil plukovník John H. Tiltman. Ukázalo se, že jde obsahově o dvě verze téhož sdělení, lišící se pouze v použití zkratek, interpunkce, v překlepech atd., což výrazně usnadnilo luštění.

Díky tomuto hrubému porušení bezpečnostních pravidel ze strany německého operátora se podařilo britským analytikům získat téměř souvislou sekvenci klíče o délce 3976 znaků, která stačila k rozbití celého šifrovacího algoritmu.

Důvodem opakovaného poslání zprávy byly atmosférické poruchy, které poškodily první zprávu. Operátor na druhém konci linky pak nešifrovaně požádal o opakování depeše. Pokud by radista poslal zprávu znovu v přesně stejném znění, ke kompromitaci by nedošlo. Při psaní zprávy na klávesnici ale byly odchylky v interpunkci nebo mezerách velmi pravděpodobné, navíc operátor při druhém vysílání zřejmě kvůli únavě častěji používal zkratky.

Německá strana si možná toto ohrožení bezpečnosti uvědomila, protože „rádiový provoz na lince na několik dní téměř utichl a do konce roku 1941 už nebyly zachyceny žádné další zprávy šifrované stejným klíčem [1].“

Získanou posloupnost pseudonáhodného klíče zkoumali britští kryptoanalytici ve snaze odhalit algoritmus, kterým je generován. Dlouho nebyli úspěšní, protože vycházeli z chybného předpokladu, že jednotlivé impulsy klíče jsou součty periodických posloupností. Po třech měsících, v lednu 1942, byl touto prací pověřen mladý matematik William T. Tutte. Tomu se podařil velký a v podstatě náhodný průlom: pracoval s informací, že na poslední pozici indikátoru se každý měsíc u všech zpráv vyskytovalo pouze 23 různých písmen, zatímco na ostatních pozicích se mohlo objevit kterékoli z 25 používaných písmen (v indikátoru se nikdy nepoužíval znak J). Očekával tedy periodu 23 nebo 25 a proto vypsal první impuls klíče do tabulky o $23 \cdot 25 = 575$ sloupcích. Všiml si častých diagonálních opakování, tzn. shodných sekvencí vzdálených o násobky 574. Dále už pracoval s číslem 41, které je dělitelem 574. Tak zjistil, že první impuls je součtem periodické posloupnosti o periodě 41 a jiné posloupnosti, jež vznikla ze sekvence o periodě 43 opakováním některých bitů. Nedlouho potom už byla Britům známá celá konstrukce stroje Lorenz SZ40, jak byla popsána výše.

Rozklad jednotlivých impulsů na součty periodických a „téměř periodických“ posloupností byl možný jen díky tomu, že vzorky kol použité pro šifrování zpráv ZMUG produkovaly slabý klíč. Rozložení bigramů v posloupnostech ψ_i' totiž bylo velmi nerovnoměrné (po sobě jdoucí bity se přibližně ze 70% shodovaly), což umožňovalo jednoduchými statistickými výpočty zjistit jak periody, tak vzorky kol χ. Nejpozději v březnu 1942 Němci zavedli opatření, která používání takto slabých klíčů předcházela; to už však byl systém prolomen. Sami britští kryptoanalytici ve své zprávě [1] přiznávají, že by šifru Lorenz SZ40 pravděpodobně nikdy neprolomili, nemít k dispozici dostatečně dlouhý úsek pseudonáhodného klíče se zmíněnou slabinou.

Počáteční úspěchy v luštění

Po tomto úspěchu se Britové vrátili ke zprávám zachyceným ve stejném období jako depeše ZMUG, zejména ke dvojicím se stejnými indikátory, jejichž luštění bylo nyní, se znalostí více typických používaných slov a zkratek, snazší. Zjistili tak například, jak dlouho platí vzorky jednotlivých kol. Nechali si také postavit vlastní exemplář šifrátoru.

Luštění odposlechnutých depeší bylo logicky rozděleno na dvě fáze: nalezení vzorků kol pro dané období (wheel breaking) a hledání počátečních nastavení kol pro jednotlivé zprávy (wheel setting).

Hledání vzorků bylo možné pouze s dostatkem zpráv tyto vzorky používajících, často se tedy podařilo uspět až koncem období platnosti vzorků. Velkou pomocí byly zprávy šifrované stejnými klíči, z nichž byli nakonec kryptoanalytici schopni vzorky určit i přesto, že byla odstraněna slabina klíče zpráv ZMUG v podobě nerovnoměrné distribuce bigramů. Britové byli ostatně na depeších se stejnými klíči stále méně závislí a Němci je také vysílali s menší frekvencí. Podařilo se dokonce vyvinout metodu, jak vzorky kol rekonstruovat pouze z indikátorových skupin dostatečného počtu zpráv.

Po nalezení vzorků přišlo na řadu hledání nastavení kol jednotlivých depeší. Při tom se využívalo znalosti typických hlaviček zpráv a tomuto úkolu se věnovali především znalci německého jazyka, jejichž nezbytnou kvalifikací bylo umění sčítat zpaměti písmena v Baudotově kódu.

V červenci 1942 byla v Bletchley založena samostatná sekce zabývající se šifrou Lorenz, podle svého vedoucího Ralpha P. Testera zvaná Testery, a ve stejném měsíci se poprvé podařilo rozluštit aktuální zprávy.

Říjen 1942 však znamenal konec experimentálního provozu šifrátoru. Němečtí radisté upustili od užívání písmenných indikátorů, různé zprávy zašifrované se stejným nastavením se dařilo získat jen zřídka a byla také zavedena praxe vkládání náhodně zvolených německých výrazů na začátek zprávy, aby se předešlo útokům na obvyklé hlavičky. Výzkumné oddělení proto dostalo úkol najít spolehlivější způsoby luštění zpráv, založené na statistických vlastnostech pseudonáhodného klíče.

Takový postup byl k dispozici již o měsíc později a jeho objevitelem nebyl nikdo jiný než W. T. Tutte. Metoda útočila přímo na zdánlivou největší přednost stroje Lorenz SZ40, nepravidelný pohyb rotorů ψ. Ukázalo se, že konkrétní implementace, v níž se všechny rotory buď společně otočí, nebo společně stojí, je naopak slabinou, která se stala šifrátoru osudnou.

Statistické metody

Tutteho metoda umožňovala hledání počátečních nastavení rotorů χ a pracovala s tzv. diferencemi posloupností podle následující definice.

Definice. *Buď* $\boldsymbol{S} = s_1s_2s_3\ldots s_n$ *binární posloupnost. Pak* diferencí $\boldsymbol{S}$ *neboli* $\Delta\boldsymbol{S}$ *nazveme binární posloupnost* $t_1t_2t_3\ldots t_{n-1}$ *definovanou vztahem*

$$t_i = s_i + s_{i+1},\ 1 \leq i < n.$$

Z již zmíněné rovnice

$$\mathbf{C} = \mathbf{P} + \chi + \psi'$$

popisující šifrování strojem Lorenz SZ40, kde **C** je šifrový text, **P** otevřený text a χ a ψ' posloupnosti znaků tvořených po řadě koly χ a ψ vyplývá

$$\mathbf{C} + \chi = \mathbf{P} + \psi'.$$

Je zřejmé, že platí rovněž

$$\Delta\mathbf{C} + \Delta\chi = \Delta\mathbf{P} + \Delta\psi'.$$

Z nerovnoměrnosti rozdělení bigramů v otevřeném textu vyplývá nerovnoměrnost rozdělení znaků v $\Delta\mathbf{P}$. Společný nepravidelný pohyb kol ψ způsobuje velký podíl bigramů tvořených stejnými znaky v posloupnosti ψ', což je příčinou stejně velkého podílu znaku / (s Baudotovou reprezentací (0, 0, 0, 0, 0)) v sekvenci $\Delta\psi'$, přestože počty nul a jedniček jsou v každém impulsu posloupnosti $\Delta\psi'$ vyrovnané díky zmíněnému pravidlu zavedenému v březnu 1942.

Protože symbol / je při zavedeném sčítání znaků neutrální prvek, rozdělení znaků v součtu posloupností $\Delta P + \Delta\psi'$ je rovněž nerovnoměrné a koreluje s rozdělením znaků v diferenci otevřeného textu. Při hledání počátečních nastavení kol χ pak útočník může počítat $\Delta\mathbf{C} + \Delta\chi$ pro všechna nastavení kol a najít díky popsané vlastnosti to správné. Rovnoměrné rozdělení bigramů v jednotlivých posloupnostech ψ_i' efektivně brání provedení popsaného útoku na jediném impulsu, ale Tutteho důležitým poznatkem byl fakt, že není nutné ani hledat

nastavení všech kol χ současně, stačí pracovat s jejich dvojicemi. Například možných nastavení kol χ_1 a χ_2 je pouze $41 \cdot 31 = 1271$.

Popsaný postup se ukázal jako teoreticky funkční, ale protože vyžadoval příliš mnoho výpočtů, nebyl vhodný pro práci s tužkou a papírem. Max Newman se ujal úkolu navrhnout nějaké mechanické zařízení, které by výpočty urychlilo.

Nastavení kol ψ bylo při použití této metody většinou stále hledáno manuálními metodami. Lingvisté ve službách Bletchley znali nejen různé často používané obraty a zkratky, ale i jejich diferencované ekvivalenty, a byli tedy schopni otevřený text získat. S přibývajícím počtem vyluštěných zpráv se dařilo odvodit vzorky řídicích kol i kol ψ, což práci dále usnadňovalo.

Účinnost statistických metod při rozpoznávání správných nastavení dále vylepšil především Alan Turing, který k tomuto účelu vytvořil celou matematickou teorii zvanou sekvenční analýza.

Mechanizace

Výsledkem práce Maxe Newmana byl přístroj Heath Robinson, pojmenovaný podle britského kreslíře bizarních obrázků. Zařízení bylo uvedeno do provozu v červnu 1943 v novém oddělení zvaném Newmanry, jehož úkolem bylo luštit šifru Lorenz mechanickými prostředky. Robinson byl složitý elektromechanický čítač, do něhož se zpráva a vzorky kol χ vkládaly na dvou děrovaných papírových smyčkách.

Přístroj potvrdil správnost Newmanova návrhu, ale k praktickému použití se příliš nehodil kvůli velké poruchovosti a problémům při synchronizaci pásek. Bylo objednáno několik dalších kusů, ale Newman začal spolu s Tommym Flowersem z výzkumného oddělení britské pošty v Dollis Hill a dalšími inženýry pracovat na mnohem pokročilejším přístroji, který by vzorky kol generoval elektronicky. Výsledkem jedenáctiměsíční práce byl elektronkový počítač Colossus.

První Colossus byl dopraven do Bletchley Parku 18. ledna 1944. Obsahoval 1500 elektronek a zprávu na děrované papírové pásce dokázal číst rychlostí 5000 znaků za sekundu (páska se pohybovala rychlostí 12m/s, tj. cca. 30 mil za hodinu), takže byl pětkrát rychlejší než Heath Robinson.

Během několika týdnů testování se počítač natolik osvědčil, že byly v březnu objednány další čtyři exempláře vylepšeného modelu Colossus Mark II, v dubnu byla objednávka zvýšena na dvanáct. Traduje se, že když Max Newman žádal Flowerse, aby první z nich byl připraven k prvnímu červnu (poptávka po informacích s blížící se invazí do Normandie rostla), inženýr odpověděl: „Věděl jsem, že se vrátíte a už jsem objednal součástky…[6]“ První Colossus II skutečně dorazil do Bletchley v červnu 1944 a další následovaly každý měsíc, celkem bylo včetně prvního vyrobeno deset strojů.

Colossus byl částečně programovatelný a bylo možné jej použít k hledání počátečních nastavení všech rotorů (nejen kol χ) a dokonce i k určení vzorků kol, byla-li k dispozici vhodná a dostatečně dlouhá zpráva (způsob nalezl Donald Michie).

Další verze šifrátoru

Němci se s postupem války snažili zvyšovat bezpečnost své komunikace zaváděním nových verzí šifrátoru. Lorenz SZ42A byl nasazen do provozu v únoru 1943, ještě před dokončením prvního přístroje Robinson. O měsíc později byla na lince Herring mezi Římem a Tuniskem poprvé zavedena funkce Klartextfunktion (a po nějaké době kvůli problémům s dešifrováním opět zrušena). Žádné z těchto opatření však britské kryptoanalytiky nezastavilo více než na měsíc, především proto, že neodstraňovaly slabinu v podobě společného pohybu kol ψ. Metody luštění tudíž proti těmto opatřením byly v principu imunní.

Po invazi do Normandie 6. června 1944 došlo k očekávanému okamžitému zpřísnění pravidel provozu, zejména ke zkrácení platnosti vzorků všech kol na jeden den. Rovněž byly na některých linkách instalovány nové přístroje Lorenz SZ42B a opět byla dočasně zavedena Klartextfunktion, což opět na nějakou dobu přerušilo luštění zpráv.

S postupem spojeneckých vojsk zanikaly některé spoje a síť se celkově dezorganizovala, centrála v Královci byla zrušena a berlínský uzel se nakonec přesunul až k Salcburku. Bletchley Park byl stále méně vytížený a mohl si dokonce dovolit pracovat na starých nevyluštěných zprávách.

Poslední zpráva šifrovaná přístrojem Lorenz SZ byla poslána v den německé kapitulace 8. května 1945.

5. Konkrétní úspěchy

Informace z depeší rozluštěných v Bletchley Parku, s krycím jménem BONIFACE a později ULTRA, poskytovaly spojencům neocenitelnou strategickou výhodu. Díky rozumnému nakládání s informacemi, tak aby nepřítel neměl důvod domnívat se, že jeho šifry jsou prolomeny, tento zdroj nevyschl po celou válku (velkou měrou také díky neopodstatněné sebedůvěře v oblasti kryptografie na německé straně).

Velký význam mělo čtení komunikace šifrované přístrojem Enigma, které mimo jiné významně přispělo k porážce německého námořnictva s jeho obávanými ponorkami. Rovněž přístup k nejcitlivějším zprávám o strategických plánech celých armád, zprostředkovaný luštěním zpráv šifrovaných systémem Lorenz, se však osvědčil hned v několika případech.

Během dobývání Apeninského poloostrova byl na začátku roku 1944 postup spojeneckých vojsk zastaven na Gustavově linii bránící Řím, kde došlo k první bitvě o Monte Cassino. S úmyslem obejít tuto linii a buď přinutit její obránce bojovat na dvou frontách, nebo je odříznout, byl přijat plán na vylodění čtyřiceti tisíc mužů u Anzia cca. 40 km jižně od Říma, který byl realizován 22. ledna. Německá strana do oblasti stáhla dostupné jednotky a chystala na invazní síly zaútočit armádou o síle tří divizí a 270 tanků. Bletchley Parku se ovšem 28. ledna podařilo rozluštit zprávu generála Kesselringa, velitele německých sil v Itálii, který měl přímé dálnopisné spojení s berlínským ústředím, zabezpečené přístroji Lorenz SZ (tato linka byla Brity označovaná Bream). Zpráva obsahovala detailní plány protiútoku. Během následujících týdnů získali spojenečtí kryptoanalytici mnoho dalších informací, včetně povelu k zahájení útoku 15. února (tentokrát z komunikace Luftwaffe). Spojenecká vojska tak byla připravena a Kesselring 19. února tuto největší protiofenzivu italského tažení odvolal s konstatováním, že „spojenci správně identifikovali hlavní záměry jeho útoku [6]“.

Vylodění ve Francii 6. června předcházela masivní spojenecká klamavá kampaň, která měla Němce přesvědčit o tom, že k hlavní invazi dojde v oblasti Calais a že pokud se vůbec bude něco dít i v Normandii, půjde jen o pokus o odvedení pozornosti. Za tímto účelem byly na doverském pobřeží vybudovány kulisy obrovské invazní armády včetně nafukovacích tanků a iluzi podporovala lživá hlášení dvojitých agentů. Efektivitu těchto opatření a vůbec naděje na úspěch invaze potvrzovaly zprávy o počtu, síle a pozici německých divizí, vysílané na lince zvané Jellyfish mezi Berlínem a velitelem západních armád generálem von Rundstedtem v Paříži.

V průběhu celé války byly vyluštěny zprávy šifrované přístroji Lorenz SZ v celkové délce cca. 63 431 000 znaků.

6. Po válce

Samotná existence kryptoanalytického střediska v Bletchley Parku zůstala před veřejností utajena až konce 70. let 20. století. Ihned po skončení války nařídil W. Churchill zničit

veškeré důkazy o operaci ULTRA. Pracovníci Bletchley byli zavázáni mlčenlivostí a většina počítačů Colossus a jiných přístrojů byla rozebrána, výkresy spáleny.

Dva ze série modernějších Colossů byly dále používány v nové organizaci Government Communication Headquarters (GCHQ), nástupkyni GC&CS, a vyřazeny a rozebrány byly údajně až v letech 1959, resp. 1960.

Sídlo v Bletchley Parku se v roce 1991 málem stalo obětí developerů. Dnes slouží jako muzeum britských luštitelských úspěchů během druhé světové války, provozované organizací Bletchley Park Trust. V poslední době se však potýká s finančními problémy.

V roce 2000 byla zveřejněna oficiální Hlavní zpráva o TUNNY (General Report on Tunny), již v roce 1945 napsali pracovníci Bletchley Parku I. J. Good, D. Michie a G. A. Timms.

Tony Sale, jeden ze členů Bletchley Park Trustu, se od roku 1993 pokoušel zrekonstruovat počítač Colossus Mk II. Na konci roku 2007 byl projekt úspěšně dokončen a Colossus změřil síly s moderními počítači v luštění zpráv zašifrovaných systémem Lorenz SZ42. Elektronkovému stroji trvalo luštění tři a půl hodiny; vítězi soutěže a jeho modernímu notebooku méně než minutu.

7. Závěr

Rozbití systému Lorenz bylo možné především díky vážným prohřeškům proti kryptografickým pravidlům na německé straně. Nedostatečná opatření proti posílání zpráv šifrovaných stejným klíčem při používání Vernamovy šifry a užívání slabých klíčů ve svém důsledku vedly k prozrazení šifrovacího algoritmu. Přitom samotný algoritmus vytváření pseudonáhodné posloupnosti se ukázal jako chatrný a jeho bezpečnost do velké míry závisela právě na jeho utajení.

Velkou roli sehrálo rovněž hrubé podcenění technických možností protivníka. Jak řekl jeden ze členů Newmanry, Jack Good: „Jedno z největších tajemství války bylo, že normální dálnopisná papírová páska může běžet rychlostí 30 mil v hodině aniž by se přetrhla [6].“

Literatura

[1] Good, J.; Michie, D.; Timms, G. A. *General Report on Tunny*.
URL: < http://www.alanturing.net/tunny_report/ >
< http://www.ellsbury.com/tunny/tunny-000.htm >
< http://www.codesandciphers.org.uk/documents/newman/newman.pdf >

[2] Bauer, F. L. *Decrypted Secrets: Methods and maxims of Cryptology*. Springer, Berlin, 2007

[3] Tutte, W. T. Fish and I. *Coding Theory and Cryptography*. Springer, Berlin, 2000

[4] Michie, D. Colossus and the Breaking of the Wartime „Fish“ Codes. *Cryptologia*, 2002, roč. 26, č. 1, s. 17-58.

[5] Sale, T. *The Updated Virtual Tunny machine*.
URL: < http://www.codesandciphers.org.uk/tunny/tunny.htm >

[6] *Bletchley Park – 60 years ago*
URL: < http://www.bletchleypark.org.uk/content/archive/ >

[7] Veselý, P. *Luštění německého šifrovacího stroje Lorenz*. Bakalářská práce, MFF UK Praha 2008

D. Hašovací funkce COMP-128

Petr Sušil, MFF UK Praha, (susil.petr@gmail.com)

GSM autentizace …..

E. O čem jsme psali v říjnu 2000 – 2007

Crypto-World 10/1999

Crypto-World 10/2000

Příloha : ZoEP.htm
Dnešní užitečnou přílohou je plné znění zákona č.227/2000 Sb.- "Zákon o elektronickém podpisu a o změně některých dalších zákonů (Zákon o elektronickém podpisu)", který nabyl účinnosti 1.10.2000.

Crypto-World 10/2001

Příloha : Vyhláška 366/2001 Sb. (366_2001.pdf)
(prováděcí vyhláška ÚOOÚ k Zákonu o elektronickém podpisu č.227/2000 ve tvaru předaném k vyhlášení ve Sbírce zákonů)

Crypto-World 10/2002

Crypto-World 10/2003

Crypto-World 10/2004

Příloha : J.Pinkava - Hashovací funkce v roce 2004 , hash_2004.pdf

Crypto-World 10/2005

Příloha : Další informace k článku V.Klímy - prilohy.zip (53 kB)
(Obsahuje: Žádost a podpisy odborníků, Návrh Šámal, Návrh Smejkal, Návrh VK_IURE, překlad části úmluvy, průvodní dopis vk_iure, link psp, stenozáznam jednání PSP, tisk zpráva ČTK)

Crypto-World 10/2006

Příloha: doprovodné materiály k Soutěži v luštění 2006 - vystava.pdf , epilog.pdf

Crypto-World 10/2007

F. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.
Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí sešity GCUCMP, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály:
http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci elektronický formulář na http://crypto-world.info. Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání kódů ke stažení sešitu.
Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info. Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byly kódy zasílány.

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška
Stálí přispěvatelé:	Pavel Vondruška
	Jaroslav Pinkava
Jazyková úprava:	Jakub Vrána
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS	Vlastimil Klíma
(výběr příspěvků,	Jaroslav Pinkava
komentáře a	Tomáš Rosa
vkládání na web)	Pavel Vondruška
Webmaster	Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	Jaroslav.Pinkava@zoner.cz ,	http://crypto-world.info/pinkava/
Tomáš Rosa	t_rosa@volny.cz ,	http://crypto.hyperlink.cz/
Pavel Vondruška	pavel.vondruska@crypto-world.info ,	http://crypto-world.info/vondruska/index.php
Pavel Vondruška,jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info
Jakub Vrána	jakub@vrana.cz ,	http://www.vrana.cz/