HAMÍKŮV KOUTEK

Číslo **259**

Zábavně naučný pdf magazín pro mládež, elektroniku a amatérské radio

Bastlení a telegraf dělá hama HAMem, experimentování dělá z HAMa vynálezce, badatele

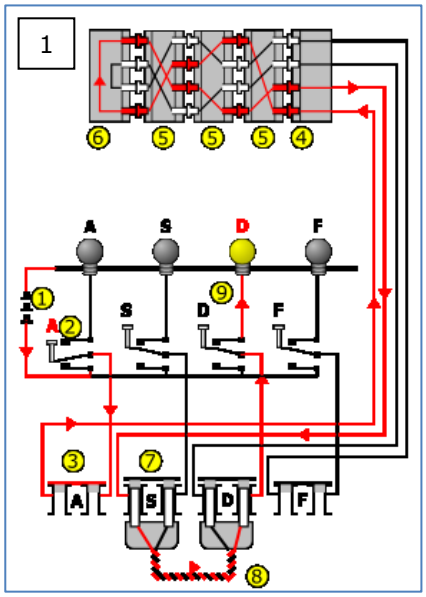
Šifrovací stroj Enigma

Brzy po vynálezu písma lidé cítili potřebu napsat zprávu tak, aby ji kromě adresáta nikdo jiný nemohl přečíst. Jednalo se zejména o vojenské zprávy. Pokud velitel může svým vojskům doručit sdělení tak, aby nepřítel nevěděl, co chystá, je to pro něj velká výhoda.

Již ve starověku se používaly jednoduché způsoby šifrování zpráv, přepravovaných poslem, které neměl číst nikdo nepovolaný. Dělalo se to například tak. že se zaměňovala písmena v abecedě, třeba tak, že se každé písmeno posunulo např. o tři místa. Místo **A** se napsalo **D**, místo **B** se napsalo **E**, místo **C** bylo **F**, atd., až místo **Z** se napsalo **C**. Vznikl nesrozumitelný text. Z dnešního pohledu primitivní šifra. Pro její prolomení si stačí uvědomit, že v lidské řeči je víc samohlásek, než souhlásek. A i souhlásky se vyskytují v různé četnosti. V českém textu například najdeme souhlásky **Q**, **W** a **X** zcela výjimečně, **F** a **G** pak zřídka, atd. Stačí si tedy znaky v šifrované zprávě seřadit podle četnosti a podle toho odhadnout, co by asi mohly znamenat. Po několika pokusech se zpravidla podaří zprávu rozluštit.

Dříve ovšem byla situace jiná. Málokdo vůbec uměl číst, a hledání klíče k rozšifrování zprávy bylo tehdy nad možnosti chápání většiny lidí.

Na podobném principu (záměna písmen), ale mnohem dokonalejším, je šifrování podle knihy. Tento způsob šifrování se používal ještě nedávno, před rozšířením počítačů, a spočívá v tom, že šifrovací i dešifrovací pracoviště je vybaveno stejnou knihou. Nejlépe nějakou běžnou, nenápadnou, dostatečně tlustou, ale ve vydání, které je málo rozšířené. Šifrant najde v knize písmenko, které má zašifrovat, a místo něj napíše (odtelegrafuje) pětimístnou skupinu znaků, která určuje stránku, řádek a pořadí písmene v řádku. Když se v zašifrovávané zprávě vyskytne stejné písmeno, najde ho šifrant na jiném místě v knize a zašifruje jako jinou pětimístnou skupinu. V zašifrovaném textu se tedy nic neopakuje, každá odvysílaná skupina je jiná. Prolomit takovou šifru je velmi těžké. Prakticky jediná možnost je dostat se na pracoviště telegrafisty a prohlédnout vše, co se tam nachází. Nejohmatanější kniha bude pravděpodobně šifrovací. Ale šifrování podle knihy má i značné nevýhody: práce jde velmi pomalu a šifrovaná zpráva je několikanásobně delší, než byla původní. To podstatně prodlužuje dobu vysílání zprávy, a zvyšuje tak nebezpečí zaměření radiostanice nepřítelem.



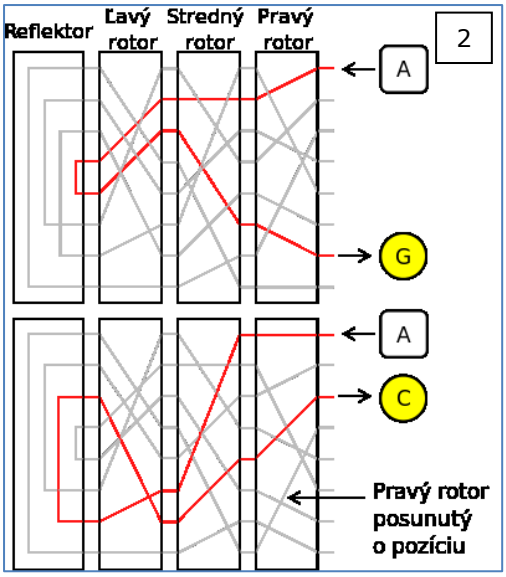
Vše změnil vynález přenosného elektromechanického šifrovacího stroje s otočnými kotouči. Stroj prošel dlouhým vývojem, než byl prakticky využitelný. Šifrovací stroj tohoto typu si nechal patentovat Holanďan Hugo Alexander Koch již před více než sto lety. Stroj chtěl vyrábět a prodávat pro šifrování obchodních zpráv, ale nebyl úspěšný. Patent později koupil německý inženýr Arthur Scherbins, který ho začal vyrábět pod názvem **Enigma** (z řečtiny, záhada, tajenka, hádanka). Ale ani ten nedokázal prodávat stroje ve velkém, zájem o ně byl malý. Až do začátku 30. let, kdy se o stroj začal zajímat **Wehrmacht.** Po zdokonalení a důkladném testování bylo rozhodnuto, že se Enigma bude používat v celé německé armádě. Věřilo se totiž, že šifra je neprolomitelná.

Enigma měla klávesnici jako psací stroj. Stisknutím některé klávesy sepnul kontakt pod ní a přes rozvodný panel a kontakty v šifrovacích kotoučích se rozsvítila žárovka, prosvětlující zašifrované písmeno **(Obr. 1).** V zařízení je ještě umístěn tzv. reflektor, který obrací tok proudu a posílá signál ještě jednou přes všechny šifrovací kotouče, ale v jiné pozici. To zajišťuje symetrii šifrování, Enigma se při stejném nastavení dá použít pro zašifrování i rozšifrování textu. Po každém stisku klávesy se šifrovací kotouče

Obr. 1 Schéma zapojení Enigmy ukazující, jak proud teče od stisknutí tlačítka klávesnice k rozsvícené lampě. Klávesa *A* je zakódována do *D* lampy. D dává po dekódování A.
1 baterie, 2 klávesnice, 3 zdířka na rozvodné desce bez zasunutého kabelu pro změnu mapování klávesnice, 4 vstupní kolo, 5 šifrovací kotouče, 6 reflektor, 7 zdířka na rozvodné desce se zasunutým kabelem 8 pro změnu mapování klávesnice, 9 žárovka označující zakódované písmeno.

pootočily o jednu pozici. Někdy jen pravý, někdy dva a někdy všechny, podle algoritmu, který byl určen mechanickými zářezy přímo na kotoučích. Tím bylo zaručeno, že při každém následujícím stisku stejné klávesy bude pokaždé stejné písmeno zašifrované jinak **(Obr. 2).**

Enigma se vyráběla v mnoha různých variantách, a i během války se upravovala s cílem zvýšit odolnost proti prolomení. Počet šifrovacích kotoučů u varianty pro **Kriegsmarine** (říšské válečné námořnictvo) byl zvýšen ze tří na čtyři, protože pro spojení s loděmi na moři a hlavně s ponorkami je nutné použít dlouhé



vlny a velké výkony a takové spojení lze snadno odposlouchat na velké vzdálenosti. Proto válečné námořnictvo používalo dokonalejší šifrování. U novějších verzí Enigmy bylo možné reflektor osadit v několika polohách, přidalo se nenulovatelné mechanické počítadlo stisků kláves, které by odhalilo případné neautorizované použití stroje a počet kotoučů se zvětšil až na osm různých, z nichž se osazovaly do stroje vždy vybrané tři nebo čtyři. Aby bylo šifrování a dešifrování úspěšné, musely být oba stroje na začátku nastavené přesně stejně. To znamená stejné šifrovací kotouče ve stejné výchozí poloze na jednotlivých pozicích, stejné nastavení reflektoru a stejné prodrátování na rozvodné desce. Celkový počet všech možných kombinací byl tedy úctyhodný a u nejvybavenější verze Enigmy dosahoval přibližně stejného počtu kombinací, jako umožňuje třistašedesátibitové kódování. Proto se mělo za to, že kód Enigmy je neprolomitelný.

Ale nebylo tomu tak. Už začátkem 30. let se v polské Poznani podařilo pod vedením **Mariana Rejewského** prolomit kód jednoduché civilní Enigmy. Když byla Enigma pro Wehrmacht zdokonalena, nebylo již možné zprávy číst. Ale

Obr. 2 Šifrování dvou písmen pomocí Enigmy: proud je veden do sestavy rotorů, přes reflektor a zpět znovu skrz rotory. Pozn.: šedé čáry představují další možné elektrické okruhy uvnitř každého z rotorů, které jsou napevno zapojeny uvnitř rotorů. Písmeno A se zakóduje jinak s každým následným stisknutím, poprvé na G, podruhé na C, atd. Je to proto, že pravý rotor se po stisku klávesy pootočí a signál je veden pokaždé jiným obvodem.

základ dešifrovacího algoritmu byl na světě a podařilo se ho před obsazením Polska nacisty předat do Anglie. Zde **v Bletchley Parku** vzniklo velké dešifrovací oddělení, které mělo za úkol prolomit německou šifru. Zaměstnávalo nejen nejlepší kryptology, lingvisty a matematiky, ale i křížovkáře, hádankáře, šachisty a jiné odborníky, kterým je vlastní logické myšlení. Skupinu vedl geniální matematik **Alan Turing.** Pro účely prolomení kódu navrhl a sestrojil elektromechanický počítač, který nazval **Bomba.** A podařilo se to, co Němci považovali za nemožné – **kód Enigmy byl prolomen** a spojenci mohli číst tajné německé radiogramy. To určitě urychlilo pád nacistického Německa, zkrátilo válku a zachránilo mnoho lidských životů. K úspěchu pomohla především mravenčí práce celého týmu, ale i trochu štěstí: Podařilo se získat funkční Enigmu ze zajaté ponorky. Tím zjistili, že zašifrovaný znak je vždy jiný, než původní. Tedy např. **A** se nikdy nezašifruje jako **A**, ale vždy jako jiný znak. A také pomohla německá důkladnost a smysl pro pořádek. Zjistili, že Němci mají **v hlavičce každého telegramu po celý den stejných prvních 6 znaků.** O půlnoci se hlavička změnila na jinou, ale zase do půlnoci se 6 znaků opakovalo. Zjevně se tedy jednalo o kód k nastavení šifrovacích kotoučů. Kotouče byly tři, a Němci ve své důkladnosti šifrovací klíč opakovali. První a čtvrté písmeno šifrované hlavičky tedy znamenalo stejné nezašifrované písmeno, druhé bylo totéž, co páté a třetí totéž, co šesté. A téměř každý telegram v závěru obsahoval **zašifrovaný pozdrav Heil Hitler.** Z těchto maličkostí spojenci dokázali vytěžit maximum a dílo se podařilo. Když si Němci uvědomili možné riziko z opakování hlavičky po celý den a měnili šifrovací klíč po každém druhém telegramu, bylo již pozdě. Spojenci šifru již prolomili, aniž Němci cokoliv tušili. **Informace o prolomení kódu byla přísně tajná** nejenom po dobu války, ale i mnoho let po ní. Enigma se totiž používala ještě po válce v rozvojových zemích i v Sovětském Svazu, protože se věřilo, že je neprůstřelná. A pro Západ byla velmi zajímavá možnost číst tajné obchodní a diplomatické zprávy ostatních zemí.

V 70. letech minulého století už Enigmu profesionálně nikdo nepoužíval a tajné informace o ní byly odtajněny. Z Enigmy se stala legenda. Bylo o ní napsáno mnoho knih, natočeno několik filmů. Odhaduje se, že šifrovacích strojů Enigma v různých verzích bylo vyrobeno na **100 000 kusů,** přesto se jich zachovalo málo. Jsou k vidění v muzeích v Anglii, Polsku a USA **(Obr. 3, 4 a 5).** Některé skončily i v soukromých sbírkách, počet není znám. Občas se Enigma objeví někde v aukci, vydražená cena originálu dosahuje částky i **20 000 $.**

Obr. 3 Armádní Enigma se třemi rotory, z londýnského Imperial War Museum.

Proto není neobvyklá ani stavba novodobých replik. Buď kopírují více nebo méně zdařile původní elektromechanický šifrovací stroj, nebo jen jeho funkci moderními elektronickými prostředky. Existuje několik programů pro PC, které emulují Enigmu, existují i nová hardwarová elektronická zařízení, která fungují jako Enigma a často i podobně vypadají.

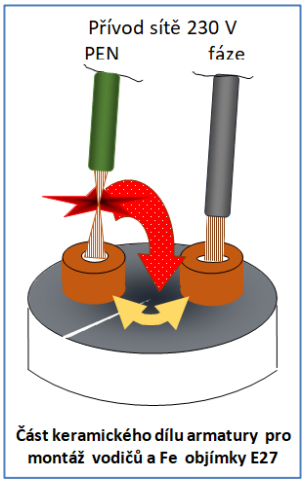
Obr. 4 Enigma z muzea v Jersey. Z celkem pěti šifrovacích kotoučů se do stroje vložily vždy tři ve správných pozicích.

Jednu takovou **elektronickou repliku Enigmy** má i redakce Hamík **(Obr. 6),** bližší popis je na *https://meinenigma.com/* . Zařízení se dodává v podobě stavebnice, která obsahuje desky plošných spojů i všechny mechanické a elektrické součástky. Po sestavení vznikne šifrovací stroj, který má, jako skutečná Enigma, klávesnici, šifrovací kotouče s možností individuálního nastavení, nastavitelný reflektor, pole s 26 LED pro zobrazení zašifrovaného písmene i rozvodnou desku se šňůrami. Funguje však na elektronickém principu, je řízena mikroprocesorem. Díky tomu má i další funkce, které původní Enigma neměla: umí zašifrovaný znak nejen zobrazit rozsvícením příslušné LED, ale i vyslovit nebo odvysílat morseovkou. Lze ji pomocí USB portu připojit na PC. Je to velmi zajímavá hračka, kterou budou mít možnost si vyzkoušet čtenáři Hamíka na Setkání radioamatérů **v Holicích** poslední víkend v srpnu, nebo na Maker Fairu 17. a 18. září **v Pražské tržnici.** Vladimír Štemberg

Obr. 1 až 5 pochází z webu *cs.wikipedia.org* .

Obr. 5 Enigma z ponorky U 534 se čtyřmi šifrovacími kotouči. Muzeum Birkenhead.

Obr. 6 MeinEnigma – elektronická replika Enigmy v redakci Hamík.



Část keramického dílu armatury pro montáž vodičů a Fe objímky E27

ZUB ČASU po 55 letech dopaden a usvědčen!

Poslední HRYZ – a nastala tma ----

Konec licny (žíly) PEN byl ve výrobě při kompletaci žárovkové objímky E 27 smáčen v agresivní pájecí kapalině. Se vzdušnou vlhkostí byla měděná vlákna chemicky narušena, postupně se měnila v šedou krystalickou látku. Z původních 24 vláken zůstalo nakonec jediné – také ale narušené. A v tomto místě jej elektrický proud 200 mA stačil zahřát až na teplotu tavení.

V tom okamžiku se v místě přerušení vytvořil el. oblouk (jako při svařování). ◄ Roztavená měď se odpařila do okolí – a na keramickém výlisku „nosiči objímky" tak vytvořila vodivý zkratový „můstek". Než oblouk „zhasl"; ještě zareagoval bytový 16A jistič.

Odpařená měď zřejmě „částečně svařila" již několik přerušených vláken a PEN se opět propojil se svorkou v keramice. V dalším okamžiku se spojení žíly se svorkou – vzniklým zkratem - zcela a trvale přerušilo. Josef Novák, OK2BK

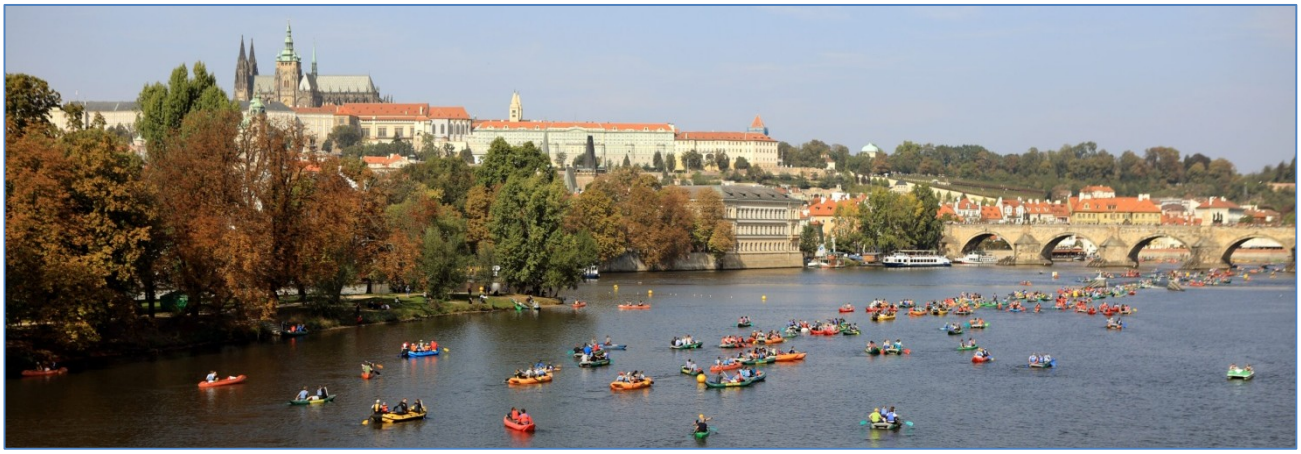
Skautské středoevropské Jamboree

Ahoj přátelé radioamatéři, 2.-12. srpna 2022 proběhne v Praze mezinárodní setkání skautů a skautek **CEJ 2022**

https://cej2022.cz/about-the-event-en/cs/o-akci-cz/

Náš skautský radioklub **OK1RAJ** bude zajišťovat spojovací službu a pomáhat s telekomunikační infrastrukturou organizátorů na akci. V rámci doprovodného programu budeme provozovat "rádiostan", odkud povede provoz příležitostná stanice **OL22CEJ** a bude účastníkům představovat činnost radioamatérů. **Budou si moci vyzkoušet radiový orientační běh, výrobu jednoduché elektronické stavebnice a komunikaci v morseově abecedě.**

Pokud by někdo z vás měl zájem zapojit se do činnosti našeho rádiostanu na této akci pro mládež, může mě prosím kontaktovat. Třeba si jen přijít zavysílat na den či noc. Předpokládáme provoz dvou (tří?) stanic na KV pásmech **všemi druhy provozu.** Michal Rybka, OK1M, tel. 732 212 091, *https://ok1m.cz/?page_id=13*



Milí čtenáři, vydávání Hamíkova Koutku prochází zajímavými peripetiemi. Zpočátku jsem vydával jedno číslo na jedné stránce jednou měsíčně. Postupně jsem vydávání rozšířil až na čtyři stránky týdně. U čísla 250 jsem si prošel malou personální krizí, kdy jsem zvažoval, mám-li vůbec ve vydávání HK pokračovat. Vy, moji milí čtenáři jste mě ale přesvědčovali, abych to určitě nevzdával a třeba si jen ulevil vydáváním jednou za dva týdny. Což jsem tedy učinil.

Jenže, abych pravdu napsal, dva týdny jsou pro mě moc dlouhá doba. Číslo mám většinou hotové již během prvního týdne a pak už jen smutně čekám na slíbený termín vydání. **Takže v dalším období zkusím HK vydávat nepravidelně - týdně nebo dvoutýdně, podle toho jak budu dostávat zajímavé články od vás, mých milých čtenářů.**

Snad mě z toho brzy neklepne. Držte mi palce. A posílejte dál své příspěvky. -DPX-

Výsledky Minitestíku z HK 258 Vzhledem k tomu, že v HK 258 bylo vyhlášeno, aby odpovědi byly posílány nejpozději druhý pátek, počkáme s vyhlášením výsledků Minitestíku z HK 258 na další číslo HK.

Náš Minitestík Malá legrácka: Jak se dá dokázat, že polovina ze třinácti je osm? Námět: Stanislaw Kowal.
Odpovídejte nejpozději v pátek do 18. hodiny, výhradně na *dpx@seznam.cz*

Zdibec moudra na závěr Jan Přeučil

Umění života spočívá v tom, uvědomovat si krásu všedního dne.

HAM je mezinárodně používaný pojem pro radioamatéra Toto číslo vyšlo 2. července 2022
HAMÍK je tedy mladý, začínající, budoucí radioamatér Vychází nepravidelně - týdně nebo dvoutýdně, v sobotu v 00:00 h

HAMÍKŮV KOUTEK je přílohou Bulletinu Českého radioklubu,
je určen pro vedoucí a členy elektro - radio – robo kroužků, jejich učitele, rodinné kluby, rodiče, prarodiče a všechny příznivce práce s mládeží; vzniká ve spolupráci s ČRK, ČAV a OK QRP klubem

Všechna předchozí čísla HK, adresy kroužků, stavební návody a mnoho dalšího najdete na *https://www.hamik.cz/*
© Petr Prause, OK1DPX, redakce HAMÍK, Čechovská 59, 261 01 Příbram, tel. 728 861 496, *dpx@seznam.cz*