**Maturitní práce**

Enigma

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Název

**Profilová část maturitní zkoušky**

Studijní obor: Informační Technologie

Třída: ITB4

Školní rok: 2022/2023 Ondřej Műhlhandel

Studijní obor: počítačové systémy

Třída: EPA4

Školní rok: 2014/2015 Jan Novák

Studijní obor: počítačové systémy

Třída: EPA4

Školní rok: 2014/2015 Jan Novák

Studijní obor: počítačové systémy

Třída: EPA4

Školní rok: 2014/2015 Jan Novák

Studijní obor: počítačové systémy

Třída: EPA4

Školní rok: 2014/2015 Jan Novák

Studijní obor: počítačové systémy

Třída: EPA4

Školní rok: 2014/2015 Jan Novák

Studijní obor: počítačové systémy

Třída: EPA4

Školní rok: 2014/2015 Jan Novák

















**Střední průmyslová škola Třebíč**

Manželů Curieových 734, 674 01 Třebíč

**Střední průmyslová škola Třebíč**

Manželů Curieových 734, 674 01 Třebíč

**Střední průmyslová škola Třebíč**

Manželů Curieových 734, 674 01 Třebíč

**Střední průmyslová škola Třebíč**

Manželů Curieových 734, 674 01 Třebíč

**Střední průmyslová škola Třebíč**

Manželů Curieových 734, 674 01 Třebíč

**Střední průmyslová škola Třebíč**

Manželů Curieových 734, 674 01 Třebíč

**Střední průmyslová škola Třebíč**

Manželů Curieových 734, 674 01 Třebíč

**Střední průmyslová škola Třebíč**

Manželů Curieových 734, 674 01 Třebíč

Obsah obrázku text, stůl

Popis byl vytvořen automatickyABSTRAKT

Práce je zaměřena na jedno z nejsofistikovanějších šifrovacích zařízení, které bylo používáno v období 2. světové války, a jehož prolomení ve velké míře určilo výsledek tohoto válečného konfliktu. Bude popsán funkční princip tohoto stroje a realizován počítačový simulátor šifrovacího stroje Enigma. Ve vytvořeném programu bude ukázáno vnitřní fungování tohoto stroje, založeného na principu tří rotorů důmyslně spojených prostřednictvím zkřížených elektrických obvodů. Pomocí moderního programovacího jazyka C# a vývojového prostředí Visual Studio, bude dále demonstrováno, jak jednoduché je emulgovat historické šifrovací zařízení Enigma moderním počítačovým systémem.

KLÍČOVÁ SLOVA

Enigma, Microsoft Visual Studio, C#

ABSTRACT

ddd

KEYWORDS

Enigma, Microsoft Visual Studio, C#

PODĚKOVÁNÍ

Děkuji bla bla bla za bla bla

V Třebíči dne 1. března 2023

podpis autora

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracoval samostatně a uvedl v ní všechny prameny, literaturu a ostatní zdroje, které jsem použil.

V Třebíči dne 1. března 2023

podpis autora

OBSAH

[ÚVOD 6](#_Toc413411010)

[1 Blbxyz 7](#_Toc413411011)

[1.1 Hshs 7](#_Toc413411012)

[ZÁVĚR 8](#_Toc413411013)

[SEZNAM LITERATURY 9](#_Toc413411014)

[SEZNAM ZKRATEK 10](#_Toc413411015)

[SEZNAM PŘÍLOH 11](#_Toc413411016)

SEZNAM OBRÁZKŮ

ÚVOD

V této ročníkové práci bude realizován počítačový simulátor šifrovacího stroje Enigma. Šifrovací stroj Enigma našel své největší uplatnění v době druhé světové války, kdy ho Němci používali k šifrování vojenských, leteckých a námořních zpráv, protože se domnívali, že jeho kód nelze prolomit. V práci bude stručně popsán vznik stroje Enigma i způsob jeho vnitřního fungování, včetně okolností, které nakonec vedly k prolomení šifrování. Způsob vnitřního fungování stroje Enigmy ukáže i počítačový program, vytvořený ve vývojovém prostředí Visual Studio za pomocí programovacího jazyka C#, simulující činnost Enigmy. Celá práce je dokladem toho, jak je jednoduché pomocí moderního programovací jazyka napodobit mechanický systém počítačovým programem, kterým bude šifrovat zprávy stejně sofistikovaným způsobem.

# Teoretická část

## Kryptografie

Kryptografie je synonymem pro šifrování. Používá se již po řadu tisíciletí pro skrývání významu informací před osobami, kterým nejsou adresovány. Kryptografie prožívá velký rozmach díky moderním telekomunikačním technologiím, u kterých je nezbytné klást velký důraz na zabezpečení dat. Každý z nás se s ní setkává prakticky každý den přihlásí-li se k e-mailu nebo do internetového bankovnictví. (1)

V historii kryptografie jedno z nejvýznamnějších zařízení používaných k šifrování zpráv představuje stroj Enigma, kterému se dostalo největšího využití německou armádou v průběhu druhé světové války. Dokonce ještě v 50. letech 20. století se tento šifrovací stroj používal v mnoha zemích a západní zpravodajské služby si tak mohly běžně číst tajné šifrované zprávy ze všech oblastí. (2) Britové si dokonce z Enigmy vytvořily vlastní šifrovací stroj nazvaný Typex, ve kterém odstranily slabiny Enigmy (písmeno se někdy mohlo stát sebou samým) a jejich přístroj tak byl mnohem bezpečnější. (3)

## Enigma

Enigma – nejslavnější šifrovací zařízení všech dob, ve své době velmi sofistikovaný přístroj, který zajišťoval přepis tajných informací do téměř nerozluštitelné šifry. Přístroj nebyl využíván pouze armádou, ale i v běžném životě. Měl kompaktní velikost, byl snadno přenosný, a tedy použitelný kdykoli a kdekoli. Enigma transformovala obyčejný text na šifrovaný text, který vypadal jako úplně náhodné znaky, libovolné písmeno se mohlo v textu objevit jako písmeno nebo i číslice. Šifrování bylo navíc prováděno pomocí tzv. krkového systému, tzn. že při každém stisknutí kláves se rotory Enigmy posunuly o krok a změnily šifrování. Vojenské Enigmy měly navíc ještě vylepšení, které dále ztěžovalo možnost prolomení šifry. (4)

### Princip Enigmy

První rotorový šifrovací stroj vynalezl ještě během první světové války německý elektromechanik Arthur Scherbius. Jeho zařízení připomínalo psací stroj, který měl navíc propojitelné nastavitelné rotory. (2) Text, který bylo třeba zašifrovat se převáděl po jednotlivých písmenech. Každému písmenu zprávy odpovídalo nové písmeno vytvořené Enigmou. A průlom v šifrování spočíval v tom, že stejná písmena zadaná do Enigmy byla v šifře odlišná. Tedy např. slovo „ANANAS“ bude ve zprávě zašifrované pomocí Enigmy znít „BQZSOX“. A při každém dalším pokusu bude výsledná šifra slova ANANAS opět zcela jiná.

Pro šifrování používala Enigma rotory. Uvnitř každého rotoru byly zkřížené elektrické obvody. Při zadání prvního písmene se otočil první rotor (rychlý rotor). Celkový možný počet otočení jednoho rotoru byl 26. Když se první rotor celý otočil, otočil se také druhý rotor (střední rotor) o jedno místo. A pak se první rotor otáčel dál. Až se otočil i celý druhý rotor, otočil se poprvé i třetí rotor (pomalý rotor) o jedno místo. Systém si lze zjednodušeně představit jako hodiny s hodinovou, minutovou a vteřinovou ručičkou. Po zmáčknutí klávesy s příslušným písmenem se rozsvítila žárovka u písmene, které bylo třeba zapsat do šifry místo něj. Základem byl obyčejný elektrický obvod tvořený baterií a žárovkou, uvnitř kterého byly pohyblivé části. Když se vedení otočilo, zdroj se připojil k jiné žárovce. To byla základní myšlenka Enigmy.

Při šifrování se používaly právě 3 rotory, ty byly vyjímatelné a vzájemně zaměnitelné. Ten, kdo Enigmu nastavoval, si mohl vybrat z 5 rotorů. Pro výběr 3 rotorů existuje tedy celkem 5 x 4 x 3, tj. 60 různých možností výběru. Každý rotor měl 26 různých pozic, tzn. že lze použít 26 různých pozic umístění, tj. 26 x 26 x 26, tj. celkem existuje 17 576 různých variant nastavení rotorů.

Enigma používaná armádou měla ještě další „vylepšení“, které zmenšovalo možnost prolomení šifrování. V přední části Enigmy byla umístěna konektorová deska, kterou tvořilo 10 kabelů, přičemž každý z nich spojoval dvě písmena do páru. Když se tato dvě písmena spojila, prohodila se. Jednalo se o vyšší stupeň šifrování určený pouze pro německou armádu. Takové propojení má nekonečné množství kombinací. Celkem je možno vytvořit z 26 různých písmen 150 biliónů 738 miliard 274 miliónů 937 tisíc a 250 kombinací. Z jednoduchého výpočtu pak vyplývá, že Enigma mohla být nastavena celkem 158 trilióny 962 biliardy 555 bilióny 217 miliardami 826 milióny a 360 tisíci různými způsoby.

Když bylo na Enigmě zmáčknuto jedno písmeno, signál prošel nejprve přes konektory v konektorové desce, pak skrz první rotor, skrz druhý rotor, skrz třetí rotor, na konci se to otočilo a signál procházel zpět v opačném pořadí, tj. skrz třetí rotor, skrz druhý a skrz první rotor. Nakonec opět prošel skrz konektory a rozsvítil žárovku u některého z písmen

U každého ze tří právě používaných rotorů bylo okénko s číslem od 01 do 26, Jejich kombinace vytvářela číselný kód. Po zadání kombinace čísel, která byla na Enigmě nastavena před začátkem šifrování, zpětným zadání šifry do přístroje mohl příjemce zprávu dešifrovat.

Příjemce zprávy tedy musel znát výchozí nastavení Enigmy. To si Němci sdělovali v písemné formě na listech papírů. Nastavení přístrojů bylo vytvářeno vždy na 1 měsíc dopředu a bylo psáno rozpustným inkoustem, takže pro znehodnocení stačilo malé množství tekutiny. Němci se oprávněně domnívali, že je jejich šifra neprolomitelná. (5)

### Rozluštění Enigmy

Podstatou Enigmy bylo, že každé písmeno, bylo-li opakovaně voleno, pokaždé se zašifrovalo v jiné písmeno. Dvě písmena v šifře za sebou nikdy mohla být stejná. Ale písmeno se nikdy nemohlo stát sebou samým, a to byla slabina Enigmy, která napomohla k jejímu prolomení.

Jako první měli Enigmu k dispozici Poláci. Tým vědců okolo matematika Mariana Rejewského už v roce 1932 napsal rovnici, která matematicky rekonstruovala zapojení rotorů v Enigmě. Jejich dešifrovací zařízení neslo název bomba a dokázali s jeho pomocí do roku 1938 dešifrovat až 75 % zachycených zpráv. Od konce roku 1938 však Němci začali přidávat k Enigmě další rotory, což dešifrování zpráv velmi zkomplikovalo (4).

Po vypuknutí 2. světové války se centrum snah o prolomení Enigmy přesunulo do Velké Británie. Vládní škola pro kódy a šifry (Government Code and Ciper School) se v srpnu 1939 přemístila do rozsáhlého komplexu Bletchley Park severně od Londýny. Poláci se o své poznatky se Spojenci podělili a podíleli se na dalším výzkumu. (2)

Němci každé ráno v 6:00 hodin posílali zprávu o aktuálním počasí. Tato zpráva měla standardizovaný formát, pouze se lišilo počasí. Tyto ranní šifrované zprávy tak obsahovaly každý den určité stejné fráze, které se kryptologové snažili odhalit a jejich pomocí pak šifrování prolomit, s využitím poznatku, že žádné písmeno není sebou samým. (5) Na prolomení Enigmy pracoval zejména britský kryptolog Alan Turing, považovaný za zakladatele informatiky. Spolu s dalším kryptologem Gordonem Welchmanem sestavili obrovský přístroj nazvaný Bombe. Ten dokázal prolomit šifru asi za 20 minut. Byl sestrojen v roce 1940 a vážil asi 1 tunu. (4)

Každé ráno musela být šifra znovu prolomena, protože přesně o půlnoci se měnilo nastavení každé Enigmy. Kryptologové museli především zjistit zapojení konektorů v konektorové desce, a právě toto dokázal přístroj Bombe, který používal metodu eliminace, na konci které zůstalo to, co nebylo špatně. Poté se výsledné zapojení vyzkoušelo, zda skutečně funguje. (3)

Až do února 1942 se spojenců dařilo úspěšně dešifrovat zprávy z Enigmy. Pak Němci přidali do námořní Enigmy čtvrtý rotor a nový systém se nedařilo prolomit až do října 1942. Spojencům se však podařilo ve Středomoří dostat na německou ponorku U-559 a než se potopila, získali z ní kódové knihy k Enigmě. Informace z číselníků, instrukcí a seznamů klíčů Enigmy pak napomohly k úspěšnému dešifrování německých zpráv po celý zbytek války. (2) Tento zlomový okamžik nakonec pomohl i k vítězství Spojenců ve válce.

### Programovací jazyk C#

C# je označení pro je vysokoúrovňový objektově orientovaný programovací jazyk vyvinutý firmou Microsoft zároveň s platformou .NET Framework. Microsoft založil C# na jazycích C++ a Java, syntaxi čerpá z jazyka C. Tento program lze využít k tvorbě databázových programů, webových aplikací a stránek, webových služeb, formulářových aplikací ve Windows, softwaru pro mobilní zařízení (PDA a mobilní telefony) atd. Nejnovější verze C# byla uvedena v listopadu 2022 pod označením C# 11. (6)

### Microsoft Visual Studio 2022

Microsoft Visual Studio je vývojové prostředí (IDE) od Microsoftu. Může být použito pro vývoj konzolových aplikací a aplikací s grafickým rozhraním spolu s aplikacemi Windows Forms, webovými stránkami, webovými aplikacemi a webovými službami jak ve strojovém kódu, tak v řízeném kódu na platformách Microsoft Windows, Windows Mobile, Windows CE, .NET, .NET Compact Framework a Microsoft Silverlight. (7) Aktuálně je na trhu Visual Studio 2022. Tato verze je oproti předchozím velmi inovativní, protože při dokončování kódu využívá umělou inteligenci. V reálném čase spolupracuje se sdílenými relacemi kódování. (8)

# Blbxyz

dddddd

## Hshs

ddddvvvdeerf

ZÁVĚR

dd

SEZNAM LITERATURY

1. ***ttps://it-slovnik.cz/pojem/kryptografie. 20.2.202***

# Citovaná literatura

1. *Co je to Kryptografie?* [online]. [cit. 2023-02-20]. Dostupné z: https://it-slovnik.cz/pojem/kryptografie

2.MICHÁLEK, Tomáš. 100+1 ZAHRANIČNÍCH ZAJÍMAVOSTÍ. *Prolomení kódu Enigma pomohlo zkrátit druhou světovou válku o dva roky* [online]. 22.9.2018. [cit. 2023-02-20]. Dostupné z: https://www.stoplusjednicka.cz/prolomeni-kodu-enigma-pomohlo-zkratit-druhou-svetovou-valku-o-dva-roky.

3. Flaw in the Enigma Code - Numberphile. In: YouTube [online]. 14.1.2013 [cit. 2023-02-20]. Dostupné z: https://youtu.be/V4V2bpZlqx8. Kanál uživatele Numberphile.

**4. *SANDRA. Od CAESARA až po ENIGMU = : História šifrovania alebo KRYPTOGRAFIE = Historie šifrování nebo KRYPTOGRAFIE. Slovensko: Dejepis Inak, 2022. online zdroj :.***

5. 158,962,555,217,826,360,000 (Enigma Machine) - Numberphile. In: YouTube [online]. 10.1.2013 [cit. 2023-02-20]. Dostupné z: https://youtu.be/G2\_Q9FoD-oQ. Kanál uživatele Numberphile.

6. C Sharp. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation. 11.2.2023 [cit. 2023-02-20]. Dostupné z: https://cs.wikipedia.org/wiki/C\_Sharp.

7. Microsoft Visual Studio. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation. 31.1.2023 [cit. 2023-02-20]. Dostupné z: https://cs.wikipedia.org/wiki/Microsoft\_Visual\_Studio.

8. *Piště kód rychleji. Pracujte efektivněji.: Vytvářejte budoucnost s Visual Studio 202* [online]. [cit. 2023-02-20]. Dostupné z: https://visualstudio.microsoft.com/cs/vs/

SEZNAM ZKRATEK

JSA - Jazyk Symbolových adres

SEZNAM PŘÍLOH

[A Schémata 12](#_Toc413409041)

[A.1 Schéma zapojení XYZ 12](#_Toc413409042)

[B Desky plošného spoje 13](#_Toc413409043)

[B.1 Deska XYZ1 13](#_Toc413409044)

[B.2 Osazení XYZ1 13](#_Toc413409045)

1. Schémata
   1. Schéma zapojení XYZ
2. Desky plošného spoje
   1. Deska XYZ1
   2. Osazení XYZ1