**Středoškolská technika 2023**

**Setkání a prezentace prací středoškolských studentů na ČVUT**

# Historie šifrování

**Zdeněk Báča**

**První soukromé jazykové gymnázium Hradec Králové**
**Brandlova 875, Hradec Králové**

# Čestné prohlášení

Prohlašuji, že jsem svou práci *„Historie šifrování“* v rámci projektu Středoškolské techniky samostatně a použil jsem pouze prameny a literaturu uvedené v seznamu bibliografických záznamů. Prohlašuji, že tištěná verze a elektronická verze soutěžní práce jsou shodné. Nemám závažný důvod proti zpřístupňování této práce v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších předpisů.

V Hradci Králové dne _____

_____

Zdeněk Báča

# Poděkování

Děkuji všem, kteří jakkoli přispěli radou nebo pomocí k úspěšnému dokončení této práce. Jmenovitě bych chtěl poděkovat vedoucímu práce doc. Ing. Filipu Malému, Ph.D. za poskytnutí jeho odborného vedení a Ing. Josefu Kokešovi Ph.D. za pomoc s vypracováním praktické části. Dále bych chtěl poděkovat každému, kdo jakkoliv pomohl k vypracování této práce a v neposlední řadě i rodině za mnoho praktických rad.

# Anotace

BÁČA, Z. Historie šifrování. Hradec Králové, 2023. Práce soutěže Středoškolská technika. Vedoucí práce doc. Ing. Malý Filip, Ph.D. 53 s.

V dnešní době si většina lidí uvědomuje, že spousta moderních technologií je zabezpečena šifrováním, ale na druhou stranu nemají ponětí ohledně základních kořenů kryptologie. Její kořeny sahají až do starověku, kdy staří Řekové už dokázali pracovat s jednoduchými šiframi a podobnými principy. Ve své práci se autor zaměřil na historii šifrování a historické šifry, o kterých se v daném rozměru zmiňuje v teoretické části. V praktické části se autor zabývá povědomím veřejnosti o šifrování a znalostech šifer, dále provedl rozhovor s odborníkem v daném oboru, konkrétně na katedře informatiky ČVUT. Výsledky práce mohou sloužit jako materiál k obeznámení se o šifrách pro neodbornou veřejnost.

**Klíčová slova:** Historie šifrování, kryptologie, kryptografie, šifry, historické šifry

# Strukturovaná anotace

Klíčová slova: Historie šifrování, kryptologie, kryptografie, šifry, historické šifry

Rozsah práce: 53

Přílohy práce: nejsou

Záměr a cíl práce: Zjištění principů historických šifer, obeznámení čtenářů o historii šifrování, vymyšlení vlastní šifry

Použité metody a techniky: dotazník a rozhovor

Popis výsledků: V mých výsledcích jsem zjistil, že se odpovědi velmi liší a velká část respondentů nezná šifrování a vytvoření vlastní šifry není zas tak složité.

Zhodnocení výsledků: Práci lze použít pro obeznámení laické veřejnosti. Informace a mé poznatky shromážděné v této práci jsou důležité pro pochopení dané problematiky.

Další možnosti řešení, pokračování v práci: Rozšíření práce by bylo možné o podrobnější popsání šifer a jejich fungování a zaměření se více na informace o Alanu Turingovi. V praktické části by se daly doplnit další rozhovory s odborníky z oblasti kryptologie, kryptografie a historiky, aby výsledky vycházely z průzkumu více lidí. Doplnění by mohlo být i dotazníkového řešení o více respondentů s větším věkovým spektrem. V neposlední řadě i zdokonalení vlastní šifry za pomocí moderních metod.

# Obsah

# ÚVOD

Toto téma jsem si zvolil, protože se již od dětství zabývám matematikou a informatikou, konkrétně kryptografií. Šifry nejsou jenom složité zašifrované texty, ale mohou být i jednoduché. Šifry se dají řešit pomocí jednoduchých, ale i složitých matematických výpočtů. Autoři historických šifer byli často slavní historičtí matematici, kteří se v jejich době zabývali všemožnými matematickými problémy. Mým hlavním cílem bylo se vzdělat v této oblasti, ale i obeznámit veřejnost o této tématice a zjistit, jak moc je veřejnost informována o metodách šifrování a známých osobnostech, které se v této oblasti vědy pohybovaly. Zkoušel jsem vymyslet vlastní šifru, která vznikla zkombinováním několika historických šifer a později matematicky zdokonalena, aby byla odolnější k dešifrování. Získané informace v praktické části jsem získal pomocí dotazníků a rozhovoru s odborníkem v oboru kryptografie Ing. Josefem Kokešem Ph.D. Práce může sloužit lidem, kteří se zajímají o informatiku a matematiku a chtějí se dále vzdělávat v tomto tématu. Je vhodná i pro laickou veřejnost, která by si chtěla rozšířit své obzory.

# TEORETICKÁ ČÁST

## 1 Vysvětlení základních pojmů

Nejprve vysvětlím základní pojmy, které jsou nezbytné pro pochopení problematiky.

- Šifra - označení pro šifrovací a dešifrovací funkci
- Klíč - kritérium potřebné k šifrování a dešifrování zprávy
- Zpráva - série symbolů abecedy
- Kryptografie - věda, která se věnuje tvorbě kryptografických systémů
- Steganografie - podobor kryptografie, který se zabývá utajováním komunikace, takže si pozorovatel ani nevšimne, že probíhá výměna informací
- Kryptografická transformace - „libovolné prosté zobrazení množiny celých čísel na množinu celých čísel (při šifrování je otevřený text nejprve převeden na čisla)“ [1]
- Kryptografický systém - algoritmus, který umožní změnu textu do podoby, která je nečitelná pro všechny čtenáře, kteří neznají dešifrovací klíč
- Kryptoanalýza - se věnuje hledání způsobů, jak prolomit šifry a tímto způsobem se dostat i k zašifrovanému obsahu
- Kryptoanalytik - člověk, který se zabývá dešifrováním zpráv bez toho, aby znal klíč
- Kryptologie - věda, která je tvořena spojením kryptografie a kryptoanalýzy
- Otevřený text - text, který ještě není zašifrovaný
- Kryptogram - již zašifrovaný text, který v sobě má šifrovací algoritmus a obsahuje utajenou informaci
- Šifrovací funkce - matematická funkce, která provádí zobrazení z množiny znaků nezašifrovaného textu do množiny textu zašifrovaného, který je určen k dešifrování
- Dešifrovací funkce - převrácená matematická funkce k šifrovací funkci, která provádí dešifrování zašifrovaného textu
- Symetrické šifrování - používá pouze jeden klíč k šifrování textu, ale i k tomu, aby byl text dešifrován
- Transpozice - technika promíchání otevřeného textu

# 2 Historie

Šifrování sahá až do starověku, kde již staří Řekové začínali používat jednoduché šifry, kterými se snažili ukrýt své utajované zprávy před nepřítelem.

## 2.1 Starověká kryptologie

„První pokusy o utajení obsahu zpráv jsou známé již ze starověkého Egypta, Mezopotámie a Indie a doprovázejí tak vznik civilizací. V Egyptě se jednalo o jednoduché „kryptosystémy“, které spočívaly v neobvyklé úpravě písma nebo v přidávání znaků, které byly známy pouze omezenému kruhu osob. Ve starověké Mezopotámii a v Sumeru byly obdobně jako v Egyptě používány různé druhy klínového písma a později i upravené pečetní válečky pro ověřování pravosti zpráv. Ve starověké Indii obsahuje Kámasútra vedle známého návodu k milování celkem 66 dalších umění včetně umění vyznat se v tajných písmech a znacích.

Ve starověkém Řecku byly využívány techniky ukrývání zprávy (steganografie), transpozice a kódování. Zprávu ukrývali tak, že oholili svému poslovi hlavu, napsali vzkaz a když mu vlasy opět narostly, mohl se tajný posel vydat na cestu. Sparťané používali jako transpoziční systém dvě hole přesně stanovené šířky; na prvou hůl (šifrovací) se navinul pás látky, papyru nebo pergamenu, na který se potom napsala zpráva a to směrem dolů po délce hole. Pás s textem se sejmul a posel jej odnesl na místo určení. Tam byl pás navinut na druhou hůl („dvojče“) a zpráva mohla být přečtena. Řecký spisovatel Polybius byl jedním z prvních průkopníku kódování – seřadil písmena do čtverce a jejich řady a sloupce očísloval. Každé písmeno tak bylo reprezentováno dvěma čísly – číslem řady a číslem sloupce. Polybiův čtverec, který umožňuje převod písmen na číslice, se později stal základem mnoha dalších šifrovacích systémů – převod písmen na číslice je zpravidla první operací při šifrování.

Římané kolem roku 0 našeho letopočtu prokazatelně zavedli vojenskou kryptografii – zprávy mezi legiemi nebyly zasílány otevřeně, ale pomocí záměny otevřeného textu za šifrovaný text. Každé písmeno zprávy bylo zaměněno za písmeno, které leželo o tři místa dále v abecedě – používali jednoduchou Cézarovu šifru.“ [2]

## 2.2 Středověká kryptologie

„Kryptologie, systematicky rozvíjena a založená na matematických základech, se zrodila díky vynikajícím arabským matematikům. Roku 855 našeho letopočtu popisuje Abú Bakr Ahmad ve své práci různé substituční šifrovací systémy. Jedna z popisovaných substitučních abeced se v arabském světě dokonce beze změny používala ještě v roce 1775. Arabové byli také první, kteří objevili a popsali metody kryptoanalýzy.

Na práce arabských matematiků a kryptologů navázala středověká Evropa. Jejím významným představitelem byl benediktinský opat Johanes Trittheim, ten kolem roku 1500 napsal významnou evropskou knihu o šifrování, ve které se zabýval převážně substitučními systémy. Panovnické rody, které běžně šifry ke komunikaci

používaly, se zalekly Trittheima a označili ho za čaroděje, což znamenalo jeho konec. V 16. století se objevili i první slavní kryptoanalytici. Jeden z největších byl v té době Francois Viete, který luštil zašifrované depeše španělského krále pro francouzského panovníka Jindřicha IV. Navarrovského. Spolehnutí se na nekvalitní systém stálo skotskou královnu Marii Stuartovnu život, neboť dopisy, ve kterých dala souhlas k připravenému povstání a zavraždění anglické královny Alžběty, posloužil jako důkaz při soudním líčení. Úspěšná kryptoanalýza pak začíná stále více ovlivňovat dějiny. Poznání, že tehdejšími jednoduchými substitučními a transpozičními šiframi utajované šifrované texty lze na základě statistických metod luštit, vedlo ke zdokonalování kryptografických systémů. Snahou bylo zahladit dodatečné informace, které by byly v šifrovaném textu obsaženy, a tím zabránit analýze šifrovaného textu tehdejšími dostupnými prostředky.“[2]

## 2.3 Kryptologie dvacátého století

„První světová válka přivedla na svět první masové použití šifrování v polních podmínkách. Podnětem k rozvoji kryptologie nebyla jen válka jako taková, ale i rozšíření bezdrátového telegrafu. Ten dával možnost snadného odposlechu, a bylo proto potřeba zavést jednoduché a bezpečné systémy šifrování. Dále se prokázala užasná síla kryptoanalytiků. Samotný vstup USA do války byl důsledkem vyluštění obsahu šifrovaného telegrafu – dnes známého jako tzv. Zimemermannův telegram. První světová válka vychovala i prvního z velikánu kryptologie dvacátého století – Williama Frederica Friedmana. Jeho čtyřsvazkové dílo „Základy kryptoanalýzy“ z roku 1923 se stalo opravdovou biblí všech kryptologů prvé poloviny dvacátého století. Obsah této knihy zásadně ovlivnil rozvoj kryptologie ve všech státech světa mezi dvěma světovými válkami a dá se říct, že se znalosti právě díky tomuto dílu „na všech frontách“ vyrovnaly. Tato kniha by pravděpodobně asi nikdy nebyla vydána, kdyby Friedman neměl existenční problémy a nemusel se živit psaním. Američané se totiž dopustili obrovské chyby a nepředvídatelnosti, která je stála těžce získaný náskok – zrušili kryptoanalytické oddělení a členy tohoto oddělení propustili! Americký ministr zahraničí Henry Stimson zrušení kryptoanalytického oddělení komentoval dnes již proslulou větou „Gentlemani si navzájem dopisy nečtou “.

Postupně kryptologii doprovází rozvoj techniky reprezentovaný v tomto období mechanickými šifrovacími stroji. Ve 30. letech bylo v Německu sestrojeno snad nejzámější šifrovací zařízení všech dob – legendární mechanický šifrovací stroj Enigma, jehož příběh ožil i na plátnech kin. I ostatní státy připravující se na další válku vydávaly značné částky na tvorbu šifrovacích zařízení.

Druhá světová válka prověřila kvalitu přichystatných šifrovacích zařízení. Zajímavé je, že většinu tehdy používaných šifrovacích systémů se podařilo druhé straně prolomit a příslušné zprávy z těchto kanálů využívat. Utajení před veřejností i nepřítelem bylo dokonalé. V zájmu neprozrazení, že ve Bentchley Parku „hrabství Buckinghamshire, Anglie“ luští zprávy z Enigmy, úmyslně nezabránil W. Churchill

rozbombardování Coventry a postavil tak dlouhodobé strategické využívání zpráv z těchto zdrojů nad životy tisíců lidí z tohoto anglického města. Pro luštění šifer sestrojil Alan Turing jeden z prvních počítačů na světě Colossus a další vývoj kryptologie začal být určován vývojem informační technologie, zejména vztahem k aktuálnímu a předpokládanému výpočetnímu výkonu.

Veřejnost se sice dozvěděla některé dílčí informace hned po válce, ale řada zpráv se objevovala až v průběhu desítek let po skončení války po otevření archivů. K tomu bylo několik důvodů – především i po válce řada států ještě používala své kryptografické systémy, o nichž se nevědělo, že v průběhu války byly prolomeny, nebo naopak byly tyto systémy úspěšné a vlády nechtěly zveřejněním informací o nich oslabit možnost jejich využití. Příkladem může být úspěšný systém, který využíval Indiánskou Kódovou řeč, kterou Indiáni předávali ve své mateřštině, tak se Japoncům nepodařilo rozluštit. Američané tento způsob s úspěchem použili ještě v 50. letech ve válce v Severní Koreji a dokonce i v 60. letech ve Vietnamu. Veřejnost byla o úspěchu těchto Indiánů informována až koncem šedesátých let a úplná kódovaná kniha byla uvolněna k publikování v roce 1999.

V době studené války byla kryptologie chápána jako tajná zbraň a informace o ní byly záměrně potlačovány. Na civilních školách se nevyučovala. Instituce, které se použitím a vývojem šifrovacích technik zabývaly, si vybíraly do svých služeb nejschopnější matematiky už během studia a po nástupu do svých služeb je teprve seznamovaly s dosaženými výsledky, které patřily mezi nejutajovanější informace. Tento sytém přispěl k tomu, že v šedesátých a sedmdesátých letech byl náskok těchto agentur „zejména NSA a KGB“ až desítky let před světovou odbornou veřejností“[2]

## 2.4 Moderní kryptologie

„Dalším významným mezníkem bylo nalezení postupu kryptografie s veřejným klíčem. Brzy po zveřejnění teoretického schématu asymetrické kryptografie (1978) se objevuje první šifrovací systém založený na myšlence využití kryptografie z veřejného klíče. Vžil se pro něj název RSA (zkratka prvních písmen autorů šifry Rivest, Shamir a Adelmann). Tento systém se po malých úpravách (proudloužení klíče, stanovení pravidel používání a využití výhod systému při elektronickém podepisování a úpravě klíčů) používá dodnes.

Přes zjevné principiální výhody při používání RSA na přelomu 70. a 80. let se ještě moc neprosazují. Výpočetní složitost k šifrování i dešifrování je obrovská a tehdejší slabé počítače pracovaly velmi pomalu. Kryptografie s veřejným klíčem slouží jen k distribuci klíčů pro symetrické šifrování (hybridní kryptosystémy – pomocí asymetrického šifrovacího systému se přenese relativně krátký klíč pro symetrický systém, a tím se dále šifruje). Od 70. let kryptologie dynamicky vstupuje do civilní sféry. V 80. letech jsou postupně vyvíjeny z tehdejšího hlediska relativně bezpečné symetrické kryptosystémy a snaha pro jejich standardizaci vedla k dokončení vývoje DES ( Data Encryption standard). DES byl v roce 1977 v USA předán za veřejný

standard pro ochranu citlivých údajů v civilním sektoru, nikoli však pro ochranu informací utajovaných ve státní administrativě, diplomacii, špionáži a vojenství. Způsob ochrany tajných informací v USA není zveřejněn. Kryptografové dlouhá léta živě diskutují o bezpečnosti DES, protože již z tehdejšího pohledu a technických možností nedostatečné délce klíče a o struktuře S–boxů. V roce 1994 publikoval J. Weiner zprávu s popisem zařízení, které vyzkouší všechny klíče DES do 7 hodin. Cenu nového zařízení odhaduje na jeden milion dolarů. V roce 1995 se na veřejnost dostává informace, že NSA (National Security Agency, Národní úřad pro bezpečnost, USA) vlastní počítač, který je schopen zprávu šifrovanou pomocí DES vyluštit do 15 minut. DES měl být nahrazen jiným standardem. Prozatímně jej NIST ( National Institute of Standards and Technology) nahrazovala implementací 3DES. Kryptologické veřejnosti bylo jasné, že řešení není optimální (zpomalení šifrování a dešifrování na 1/3 ), a proto v roce 1997 NIST vypisuje v USA veřejnou soutěž na vytvoření nového komerčního standardu pro symetrické šifrování – AES ( Advanced Encryption Standard)

V 90. letech se na poli asymetrické kryptografie objevuje nové řešení – kromě šifrování je možné elektronicky podepisovat dokumenty. Postupně vznikla teorie i praxe elektronických podpisů včetně zakládání certifikačních autority. Koncem roku 1999 přijala evropská komise směrnici o elektronických podpisech. Zároveň probíhal proces schvalování zákona o elektronickém podpisu i v České republice. V lednu 1999 byl dosažen další symbolický kryptoanalitický cíl – bylo faktorizováno číslo délky 512 bitů (155 – ciferné dekadické číslo) jako součást potencionálního útoku např. na šifru RSA.

Dále jsou systematicky vyvíjeny metody kryptoanalýzy (diferenční kryptoanalýza, lineární kryptoanalýza aj.) Jsou zdokonalovány metody útoku hrubou silou (včetně metod faktorizace čísel na prvočísla nebo obecněji na součinitele). Je rozvíjena teorie kryptologie, vychází „bible kryptologů“B. Schneiera, jsou rozvíjeny a uplatňování kryptografické protokoly (jeden ze základu bezpečnosti aplikace kryptografie). Významný je rozvoj alternativních počítačů – v roce 2001 je již hlášena úspěšná faktorizace součinu malých prvočísel (15=15*3) pomocí kvantového počítače.

Průlomem v kryptologii je povolení vývozu silných šifer z USA, kde do roku 1999 platil (jako součást boje proti kriminalitě a terorismu) zákaz vývozu šifer s klíčem delším než 40 bitů. Impulsem mohlo být prohlášení německé vlády v létě roku 1999, ve kterém jasně prohlašuje, že na dobu dvou let ruší všechny restrikce v používání silné kryptografie a dává celému světu najevo, že chce zaujmout rozhodující pozici v evropském trhu s kryptologii. Tlak amerických firem, které přicházely o miliony dolarů kvůli zákazu vývozu silných šifer, nakonec slaví úspěch. V listopadu roku 1999 dochází k prvnímu uvolnění vývozních restrikcí a další uvolnění následuje v lednu roku 2000. Povolení se nevztahuje na teroristické státy – byl vytvořen seznam 44 důvěryhodných států (v Evropě Maďarsko, Polsko, Chorvatsko, Belgie, Rakousko, Dánsko, Finsko, Francie, Irsko, Itálie, Lucembursko, Monako, Holandsko, Norsko, Portugalsko, Řecko, GB,SRN, Španělsko, Švédsko a Česká republika).

Byl zjednodušen vývoz 56 bitového DES a povolen je vývoj šifer pro americké firmy, jako jsou pojišťovny, bankovní instituce, zdravotnictví a online obchod. S konečnou platností je tak uvolněn export šifrovacích algoritmů ze Spojených států (včetně zdrojových textů a kódů). Uplatňuje se také nový přístup – technologie sdílení klíčů (angl. key escrow), systém obnovy klíčů (angl. key recovery) a klíč v komunikačních zařízeních (angl. operation action).

Nastala doba, kde softwarové a hardwarové firmy mohou tvořit na základě standardu a norem bezpečné aplikace. Pokud firmy vyřeší bezpečné a uživatelsky jednoduché uchování klíčů, pak se nebude muset uživatel bát, že produkty, které nějak prokáží svoji shodu s těmito celosvětovými standardy (na základě validace, certifikace apod.) nejsou spolehlivé. Bezpečné kryptografické produkty (společně s právními akty – zákony, vyhláškami) zřejmě povedou k nebývalému rozšíření šifrování.

Zatímco aplikovaná kryptologie byla dříve výsadou tajných služeb, armády a diplomacie, nyní se stává během posledních let věcí veřejnou a současně i výnosným obchodem“[2]

# 3 Alan Turing

Alan Turing, celým jménem Alan Mathison Turing, se proslavil jako kryptoanalytik a zakladatel moderní informatiky, přičemž byl dále matematik a logik. Klíčovým se stal hlavně během druhé světové války, kdy měl velké zásluhy v dešifrování nacistických kódů pomocí Enigmy.

## 3.1 Život před druhou světovou válkou

Narodil se 23. června roku 1912 v Londýně a zemřel 7. června roku 1954 ve Wilmslowu ve svých čtyřiceti jedna letech. Krátce po jeho narození rodiče opustili Anglii a vrátili se zpátky do Indie. Turing s nimi však nejel, zůstal v rodné Velké Británii a v průběhu jeho dětství byl vychováván jeho příbuznými nebo chůvami. Jeho dospívání probíhalo jako u jeho vrstevníků, neprokazoval nadprůměrnou inteligenci a byl průměrným žákem. Na střední škole se seznámil s Christopherem Morconem, se kterým prováděli vlastní pokusy a bavili se o vědeckých novinách. V tomto a pozdějším věku začal Turing projevovat sklony k vědě a jejímu zkoumání navzdory smrti jeho přítele v roce 1930.[3]

Po studiu na střední škole nastoupil Turing na King's College v Cambridge, kde studoval během let 1931 a 1936. Jeho hlavním oborem byla matematika a roku 1935 byl zvolen členem univerzitní koleje na základě disertace o centrální limitní větvi, kterou napsal. Jeho další vědecké zásluhy jsou obsaženy v článku „On Computable Numbers, with an Application to the Entscheidungsproblem". Toto byl první článek, ve kterém byl zaveden pojem „Turingův stroj". Ve zkratce se jedná o teoretický model obecného výpočetního stroje. Tento stroj zajistil základy informatiky a dokázal, že problém zastavení Turingova stroje není rozhodnutelný. Po studiu v Cambridge nastoupil na druhou vysokou školu, na univerzitu v Princetonu. Zde byl pod vedením Alonza Churcheho a získal doktorát. [3]

## 3.2 Působení v období druhé světové války

Do povědomí lidí se dostal právě během válečného období. Byl jedním z nejdůležitějších vědců, co luštili tajné německé kódy, které byly kódované převážně dvěma stroji, Enigmou a Tunnou. Tato dešifrace probíhala na panském sídle Blechtley Parku asi osmdesát kilometrů od Londýna, kam nastoupil 4.9.1939. Jejich práce se zúročila a Angličané díky tomu byli po větší část války v převaze díky dispozici nepřátelské komunikace. Avšak Turing vynalezl spoustu přístrojů, je mu neprávem připisováno i sestrojení počítače Colossus roku 1943, jehož hlavní funkcí bylo zachycování německých rádiových depeší.

Enigma byla přenosný šifrovací stroj či mechanismus využíván pro šifrování a dešifrování tajných údajů. Prolomit ji se nejprve podařilo polským kryptogramům pod vedením Rejewského a Turing pracoval na zlepšení, aby se mohla používat intenzivněji. Rejewského výzkum byl založený na zkoumání jednoho písmene, kdy

problémem byla pravděpodobnost. Zvýšením používaných kabelů v propojovací desce pravděpodobnost, že testované písmeno je správné, rapidně klesala. Turing popsal návrh na zlepšení teoreticky, ale nikdy jej prakticky nezrealizoval.

Turing prostudoval velké množství starých rozšifrovaných zpráv, protože předpokládal, že pomocí znalostí ze starých depeší, dokáže předpovědět alespoň z části některé šifrované zprávy. Přišel na to, že Němci využívali opakující se fráze. Například každý den ve stejný čas Němci posílali informace o počasí, forma byla striktně daná bez jakýkoli výjimek. Britští kryptoanalytici se snažili uhodnout použitou frázi a porovnávali ji se zachycenou šifrovou zprávou. Pokud došlo k propojení takové části otevřeného textu a šifrového textu, nazývali to tahák. Turing významně pomohl k dešifraci zpráv a hledání denních klíčů se značně zrychlilo. Do konce války bylo pomocí jeho stroje rozšifrováno velké množství zachycených německých depeší. Druhá světová válka skončila tím pádem velkým úspěchem britských kryptoanalytiků.[3]

## 3.3 Život po válce

Od roku 1948 pracoval na univerzitě v Manchassteru, kde napsal několik prací a dále se zabýval svým výzkumem. Jeho myšlenky z období druhé světové války byly dále využity při rekonstrukci prvních počítačů řízených programem uloženým ve vnitřní paměti zařízení. Významným je tzv. Turingům test, což je pokus, který tvrdí, že stroj můžeme považovat za inteligentní, když nejsme schopni odlišit jeho výstup (např. odpovědi) od výstupu člověka.

O jeho osobním životě se toho ví málo. Byl zasnoubený pár měsíců s Joan Clarke, věnovala se matematice a kryptoanalýze, ale poté, co přiznal, že je homosexuál, ho odmítla. V lednu roku 1952 se seznámil Turing s nezaměstnaným Arnoldem Murrayem, kterého pozval k sobě domů a následující den, 23.1. 1952, byl jeho dům vykraden. Murray řekl, že zlodějem byl jeho známý, a Turing tento přestupek nahlásil na policii, což se mu stalo osudným.

Během vyšetřování se přiznal, že s Murrayem měl sexuální vztah, kvůli čemu byl obviněn ze sexuálního deliktu a čelil soudnímu procesu. Ztratil veškerý přístup k utajovaným informacím a možnost cestovat do USA. Turing dostal na výběr mezi vězením a probací (podmíněním prominutím trestu), s níž se vázalo podstoupení hormonální léčby. Rozhodl se podstoupit léčbu, kdy přijímal estrogeny, a trvala přes rok. Po této době se Turing otrávil kyanidem draselným, který byl napuštěný v jablku. Oficiálně se jednalo o sebevraždu a byly odmítnuty spekulace o náhodě nebo o vraždě.[3]

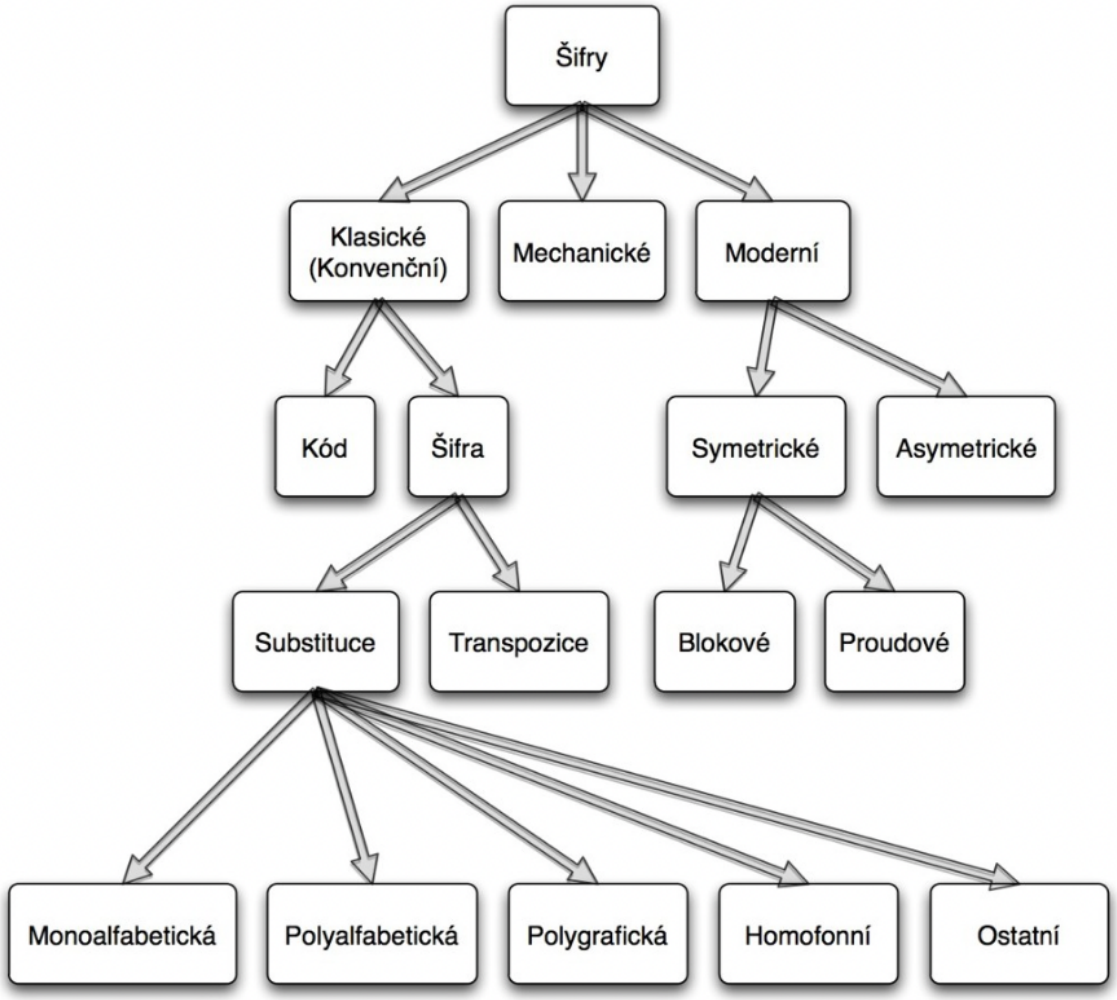
## 3.4 Enigma

Význam slova enigma pochází ze starořeckého slova hádanka. Pokud většina lidí uslyší slovo enigma, vybaví se jim šifrovací stroj, který je spojován s šifrovanou

korespondencí německé armády v průběhu druhé světové války. Z historického hlediska byla sice šifra toho přenosného šifrovacího zařízení prolomena polskými kryptoanalytiky, nicméně pro zásadní obrat v průběhu druhé světové války byl výsledek vědeckého bádání britského týmu pod vedením profesora Alana Turinga, díky kterému bylo možné číst zasílané utajované německé zprávy a následně moci reagovat na vojenskou strategii používanou v průběhu druhé světové války fašistickými jednotkami. Dalo by se říci, že enigma, ač pro běžného člověka bez znalosti historie na první pohled vypadá jako obyčejný psací stroj s několika úpravami a elektrickým připojením, tedy v té době pokrokový elektrický psací stroj, byl jeden ze zásadních nástrojů šifrovací techniky. Již z dob této doby je v rámci vojenské strategie zažité heslo bez spojení není velení a bez velení se nedá vyhrát válka. Jinými slovy, díky tomu, že byl prolomen kód enigmy bylo možné využívat informací získaných z rozkazů německých velitelů k odpovídající reakci a následnému vítěznému tažení a porážce Německa. To, že byl šifrovací stroj enigma legendou se dá usoudit i z toho, že byl po druhé světové válce používán několika civilními organizacemi k šifrování vnitroorganizačních dokumentů s tím, že se jedná o jedno z těžko prolomitelných zařízení ve světovém měřítku. Ikdyž bylo od té doby vyvinuto mnoho šifrovacích zařízení a strojů, asi už nikdy žádný z novodobých šifrovacích zařízení používaných v kryptografické bezpečnosti na bázi počítačových programů, žádný z nich nedosáhne tak velké publicity, jako se dostalo šifrovacímu stroji Enigma.[4]

# 4 Primární dělění šifer

V této kapitole ukazuji primární dělení šifer a v další kapitole se jim věnuji podrobněji.




Obrázek 1: Dělení šifer [5]

Z obrázku výše lze vyčíst, jak se dělí šifry. Historické šifry jsou převážne na levé straně.

# 5 Substituční šifrování

Substituční šifra je šifrovací systém, ve kterém je každé písmeno zprávy nahrazeno jiným znakem, ale zachovává si své místo v utajované zprávě. [4]

## 5.1 Systémy monoalfabetické

„Systémy monoalfabetické mají jednu důležitou vlastnost. Zachovají jednoznačný vztah mezi znaky původní zprávy (otevřené zprávy, tajné zprávy apod.) a znaky šifrované zprávy. Tento vztah a toto přiřazení se obvykle označuje jako kódová kniha daného šifrovacího systému a je vlastně klíčem k řešení šifry.

Jeden z nejstarších systémů pochází z Indie. Místo písmen se psala písmena, která podobně znějí. Např. v češtině by věta „Včera se náš oddíl pokusil ustoupit.“ by mohla znít třeba: „Fšera ze ňaf ottiv pokufyl huftoupyt.“ Tyto systémy založené na homofonnosti (stejnoznělosti) hlásek již dnes nemají valné použití.“[1]

### 5.1.1 Cézarovská šifra

Cézarova šifra je velmi jednoduchá šifra používaná Juliem Cézarem ve vojenské komunikaci.

**Princip** „Šifra může pracovat nad libovolnou abecedou, ale obvykle předpokládáme, že pracuje nad anglickou abecedou o 26 písmenech ab ... yz. Klasická Cézarova šifra vypadala tak, že se každé písmeno z otevřeného textu „posunulo“ o tři písmena dále. Takže místo písmena „a“ se napsalo písmeno „d“, místo písmena „b“ se napsalo písmeno „e“ atp. Pokud už jsme došli na konec abecedy, začali bychom od začátku — takže písmeno „z“ bychom zašifrovali na písmeno „c“. Celý posun ukazuje následující tabulka:“ [6]

| Vstup | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Výstup | **d** | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w |

Obrázek 2: Cézarovská šifra [6]

**Zobecnění Caesarovy šifry** „Zatímco Caesar údajně vždy používal posun právě o tři písmena, my můžeme Caesarovu šifru zobecnit na posun o libovolný počet písmen. Jako klíč šifry se pak používá to písmeno, na které se zobrazí písmeno „a“. Takže původní Caesarova šifra představuje posun o tři písmena, což odpovídá písmenu „d“, protože „a“ se zobrazí na „d“. V ukázkových tabulkách je klíč zvýrazněn tučně. Dále si můžete vygenerovat tabulku dle odpovídajícího klíče:“ [6]

| Vstup | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Výstup | **d** | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w |

Obrázek 3: Cézarova šifra [6]

**Šifrování** „probíhá stejně, nalezneme písmeno v horním řádku a napíšeme místo něj písmeno z odpovídajícího spodního řádku“[6]

**Dešifrování** „probíhá opačným směrem — nalezneme písmeno ve spodním řádku a napíšeme místo něj písmeno z horního řádku.“[6]

**Příklad** „máme šifrový text „klwrw“ a budeme dešifrovat podle klíče w. Vygenerujeme si tabulku s klíčem „w“ a ve spodním řádku nalezneme písmena „klwrw“. V horních řádku přečteme původní text: „Opava“.“[6]

## 5.2 Systémy polyalfabetické

„Všechny monoalfabetické šifry zachovávají původní četnosti výskytu znaků a tím napomáhají snadnějšímu rozluštění. Tento nedostatek se snaží odstranit polyalfabetické šifry, které tvoří konečná (nebo nekonečna) posloupnost monoalfabetických šifer. Současně se však snažíme, abychom nemuseli předávat ve příliš mnoho informací nutných pro dešifrování textu.“[1]

### 5.2.1 Vigenerova šifra

**Princip šifrování a dešifrování** „Postup šifrování můžeme vysvětlit pomocí Cézarovy šifry. Klíčem Vigenèrovy šifry je libovolné slovo skládající se z písmen anglické abecedy, tj. a—z. Klíčem tak může být například slovo „bcf“. Šifrování pak probíhá tak, že si napíšeme otevřený text a hned pod něj klíč, který budeme opakovat tak dlouho, aby měl stejnou délku jako otevřený text. Pro otevřený text „dobryvecer“ by to vypadalo takto:

| Otevřený text: | d | o | b | r | y | v | e | c | e | r |
|---|---|---|---|---|---|---|---|---|---|---|
| Klíč: | b | c | f | b | c | f | b | c | f | b |

Obrázek 4: Vigenèrova šifra [6]

Nyní bychom všechna písmena z otevřeného textu zašifrovali pomocí Cézarovy šifry s příslušným klíčem, tj. s klíčem ve stejném sloupečku. Cézarova šifra je posunovací šifra, klíč udává, o kolik písmen máme písmeno otevřeného textu posunout,

měřeno od písmene „a“. Písmeno „b“ například značí posun o jedno písmeno v abecedě „doprava“. Písmeno „d“ značí posun o tři písmena doprava. Slovo „ahoj“ bychom Cézarovou šifrou a s klíčem „b“ zašifrovali na „bipk“.

Zatímco v Cézarově šifře šifrujeme celý text jedním písmenem, ve Vigenèrově šifře typicky šifrujeme více písmeny. Šifrování textu „dobryvecer“ s klíčem „bcf“ by tak dopadlo takto:

| Otevřený text: | d | o | b | r | y | v | e | c | e | r |
|---|---|---|---|---|---|---|---|---|---|---|
| Klíč: | b | c | f | b | c | f | b | c | f | b |
| Šifrový text: | e | q | g | s | a | a | f | e | j | s |

Obrázek 5: Vigenèrova šifra příklad [6]

První písmeno „d“ jsme šifrovali s klíčem „b“, tedy posun o jedno písmeno, a proto je výsledkem písmeno „e“. Písmeno „o“ jsme šifrovali s klíčem „c“, tedy posun o dvě písmena a výsledkem je písmeno „q“. Atd.

Dešifrujeme úplně stejným způsobem a pouze místo toho, abychom posouvali písmena „doprava“, je posouváme „doleva“.“[6]

**Vigenèrův čtverec** „Celý postup šifrování a dešifrování lze také vysvětlit na Vigenèrově čtverci, což je pomůcka, kterou můžeme během šifrování použít. Vigenèrův čtverec je tabulka, která má 26 řádků a 26 sloupců. V každém řádku je vepsána abeceda, přičemž v každém řádku je vždy posunuta o jedno písmeno:

Pokud máme takovýto Vigenèrův čtverec, šifrování by probíhalo následovně: vzali bychom písmeno z otevřeného textu a našli bychom řádek s tímto písmenem. Pak bychom vzali písmeno z klíče a našli bychom sloupeček. Písmeno ze šifrového textu by pak bylo písmeno z odpovídajícího řádku a sloupce.

V předchozím příkladě jsme šifrovali „dobryden“ s klíčem „bcf“. Najdeme tak řádek, který začíná „d“ a sloupeček, který začíná „b“. V průsečíku tohoto řádku a sloupce je písmeno „e“, výsledné písmeno šifrového textu.

Při dešifrování bychom postupovali obráceně. Pokud bychom chtěli dešifrovat písmeno „e“ za použití klíče „b“, tak bychom našli sloupec „b“, v němž bychom našli řádek, který obsahuje písmeno „e“ a písmeno, které je na začátku tohoto řádku by bylo písmeno z otevřeného textu.“[6]

| | **a** | **b** | **c** | **d** | **e** | **f** | **g** | **h** | **i** | **j** | **k** | **l** | **m** | **n** | **o** | **p** | **q** | **r** | **s** | **t** | **u** | **v** | **w** | **x** | **y** | **z** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **a** | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| **b** | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a |
| **c** | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b |
| **d** | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c |
| **e** | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d |
| **f** | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e |
| **g** | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f |
| **h** | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g |
| **i** | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h |
| **j** | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i |
| **k** | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j |
| **l** | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k |
| **m** | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l |
| **n** | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m |
| **o** | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n |
| **p** | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o |
| **q** | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p |
| **r** | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q |
| **s** | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r |
| **t** | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s |
| **u** | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t |
| **v** | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u |
| **w** | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v |
| **x** | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w |
| **y** | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x |
| **z** | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y |

Obrázek 6: Vigenèrův čtverec [6]

# 6 Symetrické šifrování

„Symetrická šifra, někdy též nazývaná konvenční, je takový šifrovací algoritmus, který používá k šifrování i dešifrování jediný klíč. Tím se liší od algoritmů s veřejným klíčem, které mají dvojici klíčů – tajný a veřejný. Podstatnou výhodou symetrických šifer je jejich nízká výpočetní náročnost.

Algoritmy pro šifrování s veřejným klíčem můžou být i stotisíckrát pomalejší. Na druhou stranu velkou nevýhodou je nutnost sdílení tajného klíče, takže se odesílatel a příjemce tajné zprávy musí předem domluvit na tajném klíči.

Symetrické šifry se často používají společně s asymetrickými. Obvyklé použití je takové, že otevřený text se zašifruje symetrickou šifrou s náhodně vygenerovaným klíčem. Tento symetrický klíč se zašifruje veřejným klíčem asymetrické šifry, takže dešifrovat data může pouze majitel tajného klíče dané asymetrické šifry.“ [7]

## 6.1 Bloková šifra

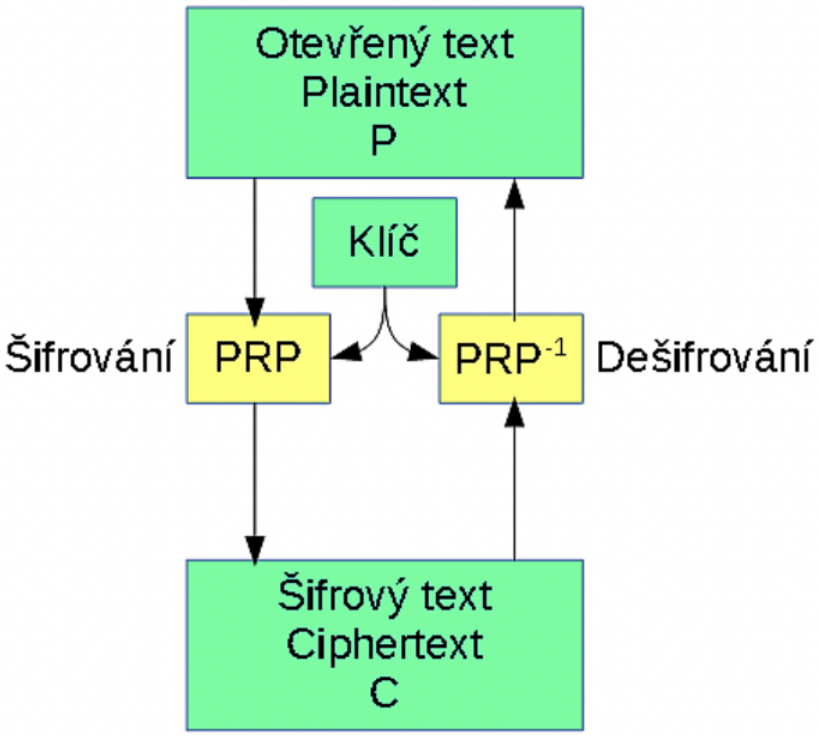
„Bloková šifra jednoznačně patří mezi nejčastěji používaná primitiva. Jejím cílem je při zadaném klíči změnit pro všechny čitelnou zprávu (otevřený text, plaintext) do tvaru nečitelného pro všechny (kromě vlastníků klíče). Tento nečitelný tvar se označuje jako šifrový text (ciphertext). Proces převodu otevřeného textu na šifrový nazýváme šifrováním, opačný proces dešifrováním.

Z pohledu teorie blokovou šifru reprezentujeme tzv. pseudonáhodnou permutací (pseudorandom permutation, PRP). Srozumitelně řečeno to znamená, že:

převádí celá čísla z určitého rozsahu na jiná ve stejném rozsahu, mapuje způsobem jedna ku jedné, čímž je garantována existence obrácené permutace pro dešifrování, je náhodná, takže ani ze znalosti mnoha párů otevřeného a šifrového textu nejsme schopni dopočítat další takové páry či dokonce odvodit klíč. PRP obvykle pracují s čísly v intervalu ¡0; 2n - 1¿, tedy převádí libovolná n-bitová data na jiná. Hodnota n se také označuje jako velikost bloku. Šifrování a dešifrování si můžeme názorně ukázat na tomto schématu níže.

Zde můžeme oprávněně namítnout, že kromě otevřeného textu do blokové šifry musíme dodat i tzv. klíč, který je v tomto případě tvořen (pseudo)náhodnou posloupností k bitů (např. 128, 192 či 256 pro AES) a že se bloková šifra stává PRP až v okamžiku, kdy jí nějaký klíč přiřadíme. To je pravda. Na klíč můžeme také nahlížet jako na jakýsi index, jímž určíme, kterou z PRP definovaných algoritmů blokové šifry budeme používat.

V praxi máme problémy zejména s požadavkem (pseudo)náhodnosti. Jak můžeme o nějaké permutaci obecně dokázat, že je (pseudo)náhodná? V zásadě nijak. Můžeme samozřejmě provést různé statistické testy, kterými ověříme, že se pseudonáhodně chová, ale to nám nedává žádné teoretické garance. Dokud se nám daný algoritmus nepodaří prolomit (dešifrovat bez znalosti klíče), předpokládáme, že se chová jako pseudonáhodná permutace, o které víme, že je pro účely šifrování bezpečná.




Obrázek 7: Schéma blokové šifry [8]

Jednou z vlastností související s (pseudo)náhodností, kterou by každá bloková šifra měla disponovat je IND-CPA. Ta nám říká, že pokud nám útočník dá dva jím vybrané otevřené texty, my je oba zašifrujeme pro něj neznámým klíčem a vrátíme mu náhodný z nich, není schopen s rozumnou pravděpodobností (výrazně odlišnou od 50 % ) poznat, ke které zprávě přísluší. Podobných vlastností existuje celá řada a díky nim dokážeme říci zajímavé věci o složitějších schématech sestavených z primitiv jako je právě bloková šifra.“ [8]

# 7 Neprolomitelná šifra

Na světě je pouze pár neprolomitelnýcgh šifer. Obykle bývají neprolomitelné pouze z důvodu jejich složitosti a toho, že jejich klíč bývá velice dlouhý a častokrát i delší než šifrovaný text samotný. Jejich nevýhodou bývá častokrát přenos klíče z důvodu jeho velikosti.

## 7.1 Vernamova šifra

„Vernamova šifra nebo také jednorázová tabulková šifra (anglicky one-time pad) je jednoduchý šifrovací postup patentovaný v roce 1917 Gilbertem Vernamem. Spočívá v posunu každého znaku zprávy o náhodně zvolený počet míst v abecedě. To se prakticky rovná náhradě zcela náhodným písmenem a na tomto faktu je založen důkaz, že Vernamova šifra je v principu nerozluštitelná.“[9]

**Podmínky spolehlivosti** „Porušení kterékoli z následujících podmínek má za následek oslabení šifry, takže by již nebyla nerozluštitelná.

- Klíč je tak dlouhý jako přenášená zpráva. Jiné šifrovací systémy používají kratší klíče, což znamená, že počet možných klíčů je menší než počet možných zpráv. Kratší klíč v principu umožňuje útok hrubou silou.
- Klíč je dokonale náhodný. Nepřipadají v úvahu počítačové generátory pseudonáhodných čísel, neboť jejich činnost lze předvídat. Nejvhodnější je užití fyzikálních metod, například tepelného šumu či ještě lépe kvantových procesů, jejichž základní vlastností je náhodnost.
- Klíč nelze použít opakovaně. Tato podmínka je vlastně důsledkem předchozí, protože opakovaný klíč není náhodný. Dostane-li útočník do ruky dvě zprávy zašifrované týmž klíčem, má často velmi snadnou cestu k rozluštění.

Popsané zacházení s klíčem je v praxi velice obtížné. Dlouhý náhodný klíč si člověk nedokáže zapamatovat, musí být zaznamenán. Jeho generování není jednoduché. Musí být zajištěno, že klíč zná pouze odesilatel a příjemce zprávy a nikdo jiný. Komunikující strany se tedy musí předem dohodnout na dlouhém klíči nějakým bezpečným způsobem a hned po odeslání první zprávy klíč zničit. Stojíme tak před problémem slepice a vejce: Abychom mohli bezpečně odeslat třeba 2 MB tajných dat, musíme předem bezpečně odeslat 2 MB dat (klíč). Vernamova šifra se tak i přes svou sílu používala jen výjimečně, například pro krytí horké linky mezi Moskvou a Washingtonem za studené války. Také někteří špioni tuto šifru využívali. Dnešní historici mají několik zpráv zašifrovaných tímto způsobem a nemají k dispozici klíč. Tajný text v tom případě zůstane skryt navěky.“ [9]

# PRAKTICKÁ ČÁST

# 8 ÚVOD K PRAKTICKÉ ČÁSTI

Praktickou část jsem začal zpracovávat po většinovém dokončení teoretické části. Rozhodl jsem se, že praktickou část rozdělím na dvě části a to na rozhovor s odborníkem a na dotazník, kterým zjistím povědomí veřejnosti o šifrování, kryptografii a Alanovi Turingovi.

# 9 METODIKA

Informace do teoretické i praktické části jsem začínal sbírat na začátku září, kdy jsem hledal šifrování v literatuře, v české i v anglické, protože publikace v anglickém jazyce jsou obsáhlejší než české zdroje. Velice mi pomohl rozhovor s odborníkem, protože mi podal neuvěřitelné množství užitečných informací a poznatků, které mi pomohly lépe pochopit šifrování a jeho využití.

V dotazníku jsem celkově získal 70 respondentů ve všech věkových kategoriích s tím, že nejvíc jich bylo ve věku do 20 let. Pomocí grafů jsem zjišťoval, kolik toho lidé vědí o kryptografii a Alanu Turingovi, či ho vůbec znají a co si myslí o využití kryptování. Dotazník jsem rozeslal po střední škole v Hradci Králové a zaměstnancům firmy zaměřené na sport.

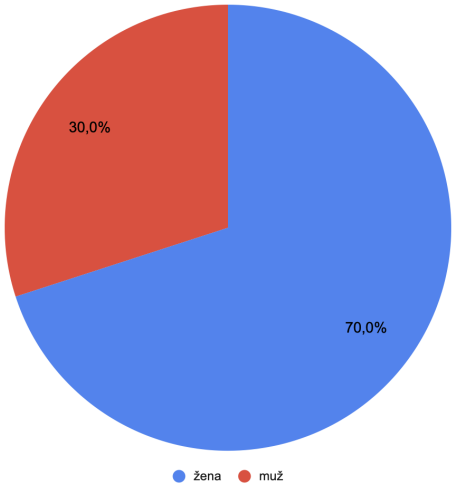
Dále jsem provedl rozhovor s odborníkem Ing. Josefem Kokešem Ph.D., který mi pomohl lépe pochopit princip šifrování a jak se používá v běžném životě.

V neposlední řadě jsem se věnoval vymyšlení vlastní šifry. Při tvoření šifry jsem vycházel z poznatků z teoretické části. Při tvoření šifry jsem se inspiroval jednoduchými šiframi a po zkombinování několika z nich jsem vytvořil svoji vlastní. K vymýšlení jsem používal převážně papír, tužku a knihu s těmito pomůckami se povedlo vymyslet a později zdokonalit šifru.

# 10 DOTAZNÍK

Dotazník vyplnilo celkově 70 respondentů. Zaměřoval jsem se na otázky ohledně obeznámení veřejnosti s pojmem kryptografie a kryptologie, o jejím vzniku a zda respondenti znají nějakou šifru. V neposlední době i na otázky ohledně vlastních zkušenostech se šifrováním. Dále jsem se ptal na to, zda znají Alana Turinga a šifru Enigmu. Dotazníky byly rozeslány do několika škol. Zjišťované informace jsou patrné z následujícího vyhodnocení, dotazník je součástí přílohy této práce.

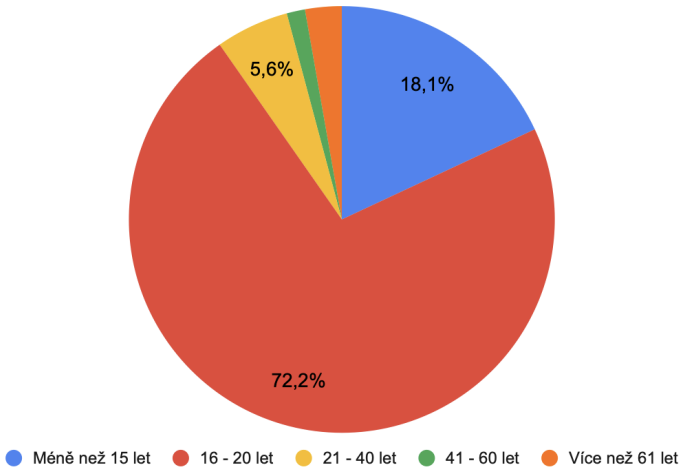
V první otázce bylo zjišťováno pohlaví respondentů




Obrázek 8: Pohlaví respondentů

Graf ukazuje, že dotazovaných bylo více žen (69,4 % ) než mužů (30,6 %).

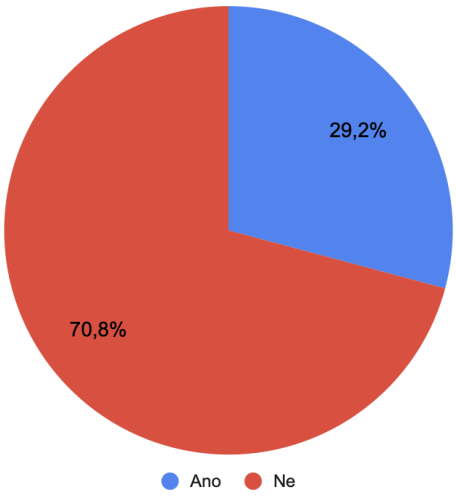
V druhé otázce jsem se zaměřil na věk respondentů




Obrázek 9: Věk respondentů

Z druhého grafu vyplývá věkové rozložení všech dotazovaných. Nejvíce respondentů se pohybovalo ve věkovém rozpětí 16 - 20 let (72,2 %), další početnou skupinou bylo rozpětí méně než 15 let (18,1 %). Nejméně dotazovaných bylo v nejvyšší věkové skupině, více než 61 let (1,4 %), ve střední věkové skupině 41 - 60 let (2,8 %) a dále 21 - 40 let (5,6 %) V třetí otázce jsem se zaměřil na pohlaví respondentů.

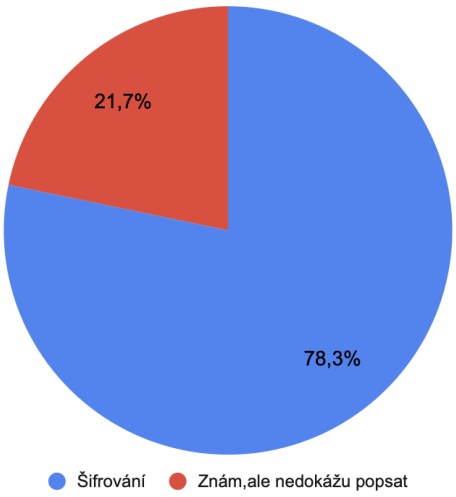
Ve třetí otázce jsem zjišťoval, kolik respondentů zná pojem kryptografie




Obrázek 10: Respondenti a povědomí o pojmu kryptografie

Přes 70,8 % respondentů nezná pojem kryptografie a pouze 29,2 % všech dotazovaných ho znalo.

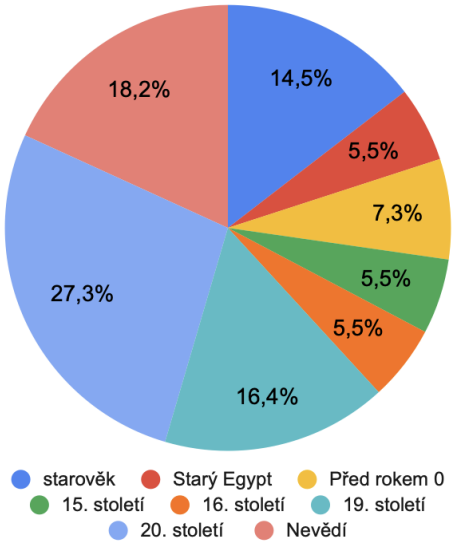
Ve čtvrté otázce jsem zjišťoval, zda respondenti dokáží vysvětlit pojem kryptogafie.




Obrázek 11: Respondenti a vysvětlení pojmu kryptografie

Tato otázka byla pouze pro respondenty, kteří na předchozí otázku odpověděli kladně. Většina respondentů (78,3 %) vědělo, že kryptografie je šifrování a dalších 21,7 % znalo pojem kryptografie, ale nedokázali ho popsat.

V páté otázce jsem zjišťoval, kdy si myslí respondenti, že vznikla kryptografie

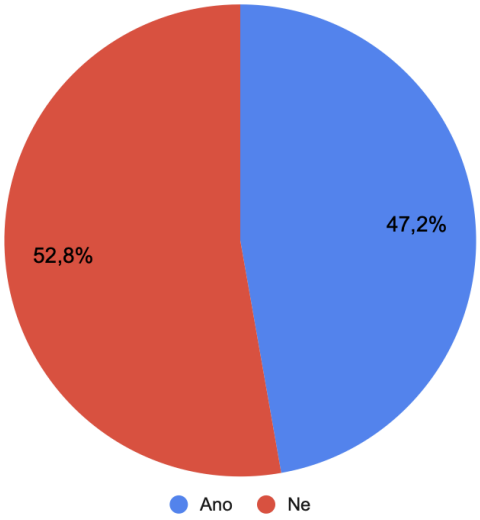



Obrázek 12: Respondenti a vznik kryptografie

Z grafu nám vychází, že nejvyšší procento respondentů 27,3 % si myslí, že kryptografie vznikla ve 20. století. Další početnou skupinou jsou respondenti, kteří nevědí, kdy kryptografie vznikla 18,2 %, dále tu jsou ti respondenti, kteří se domnívají, že kryptografie vznikla v 19. století 16,4 %. Poslední početnější skupinou jsou respondenti, kteří odpověděli, že kryptografie vznikla ve starověku 14,5 %. V neposlední

řadě tu jsou méně početné skupiny a to jsou ti respondenti, co si myslí, že kryptografie vznikla před rokem 0 (7,3 %),v 16 století(5,5 %), v 15. století(5,5 %) a ve starém Egyptě (5,5 %).

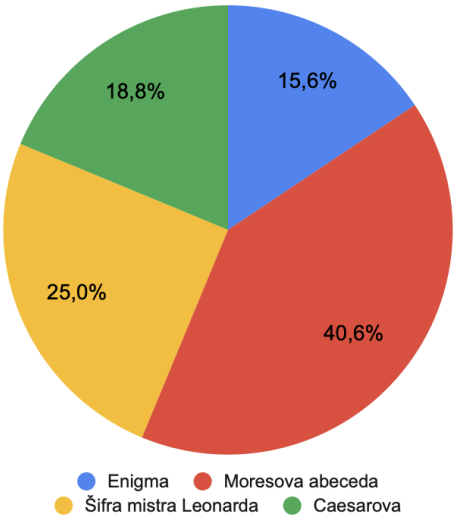
V šesté otázce jsem zjišťoval, zda respondenti znají nějakou šifru.




Obrázek 13: Respondenti a znalost šifer

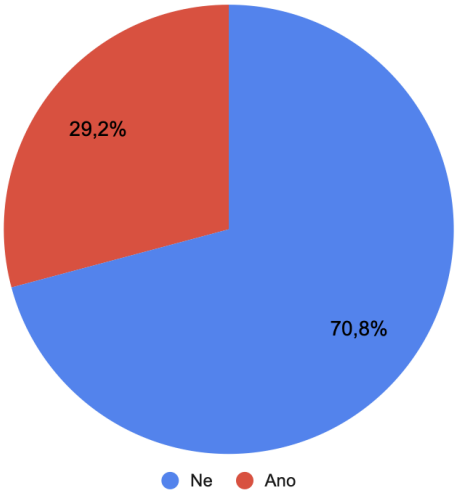
Z grafu lze vyčíst, že většina respondentů nezná žádnou šifru (52,8 %) a 47,2 % zná nějakou šifru.

Ve sedmé otázce jsem zjišťoval, jaké šifry znají respondenti.




Obrázek 14: Respondenti a znalost druhů šifer

Z grafu lze vyčíst, že nejvyšší procento respondentů zná Morseovu abecedu (40,6 %), další početná skupina zná Šifru mistra Leonarda (25 %). Dále tu je Cézarova šifra a tu uvedlo 25 % respondentů, poslední byla uváděna Enigma (15,6 %)

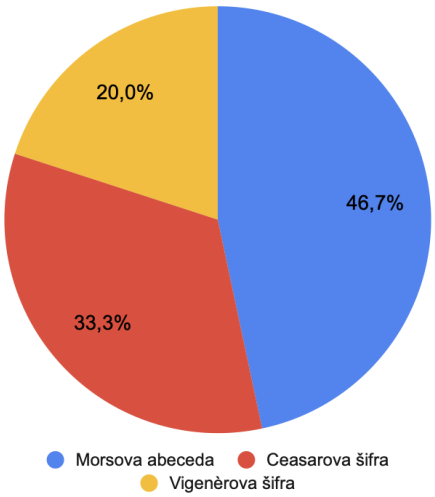



Obrázek 15: Respondenti a zkoušení šifrování

V osmé otázce jsem zjišťoval, zda respondenti zkoušeli někdy šifrovat.

Z grafu lze vyčíst, že drtivá většina (70,8 %) respondentů nikdy nezkoušelo šifrování a pouze 29,2 % zkoušela šifrování.

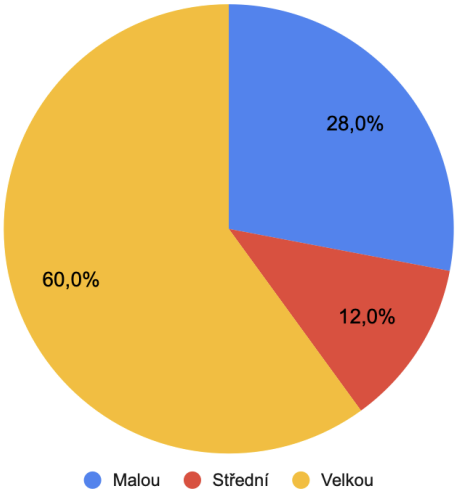
V deváté otázce jsem zjišťoval, jakou metodu respondenti použili při šifrování.




Obrázek 16: Respondenti a použití šifer

Tato otázka byla pouze pro respondenty, kteří na předchozí otázku odpověděli kladně, že zkoušeli někdy šifrovat. Z grafu lze vyčíst, že nejvíce respondentů odpovědělo Morseovu abecedu (46,7 %), dále odpovídali Cézarovu šifru (33,3 %) a Vigenèrova šifru (20 %).

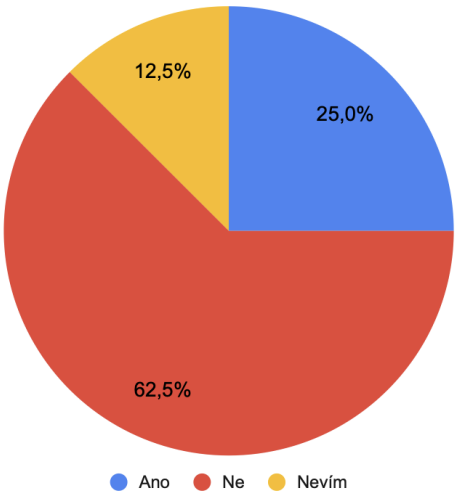
V desáté otázce jsem zjišťoval, jak velkou roli podle nich hraje kryptografie v oblasti vědy.




Obrázek 17: Respondenti a použití šifer

Z grafu lze vyčíst, že 60 % respondentů si myslí, že velkou, 28 % malou a pouze 12 % střední.

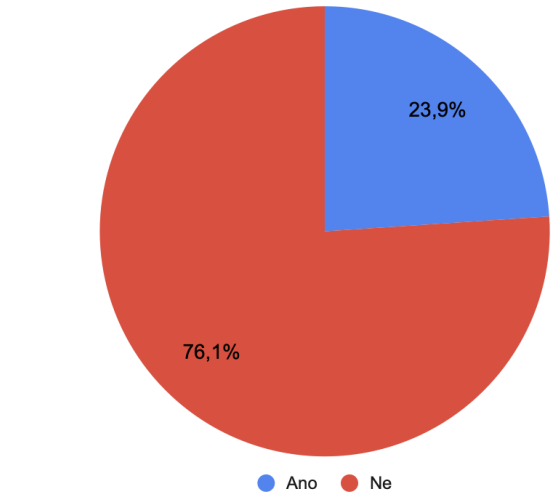
V jedenácté otázce jsem zjišťoval, zda by respondenty zajímal předmět kryptografie.




Obrázek 18: Respondenti a zájem o předmět kryptografie

Z grafu lze vyčíst, že 62,5 % respondentů by nemělo zájem o předmět kryptografie, 25 % ano a 12,5 % neví.

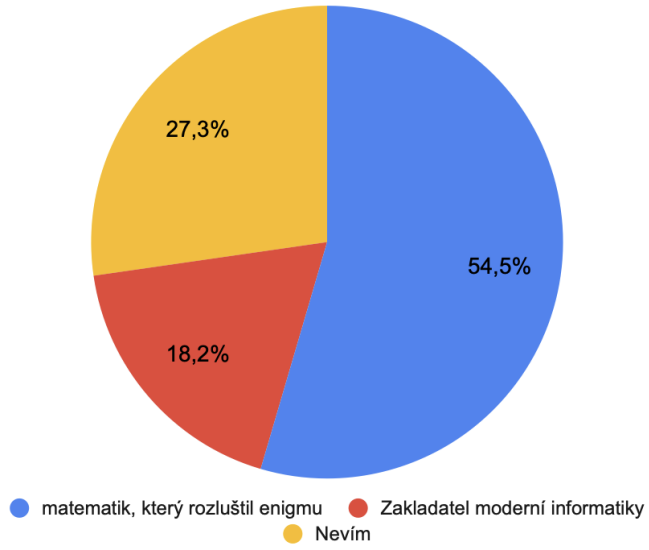
Ve dvanácté otázce jsem zjišťoval, zda respondenti znají Alana Turinga.




Obrázek 19: Znalost Alana Turinga

Z grafu lze vyčíst, že většina respondentů (76,1 %) nezná Alana Turinga a zbylá část (23,9 %) zná.

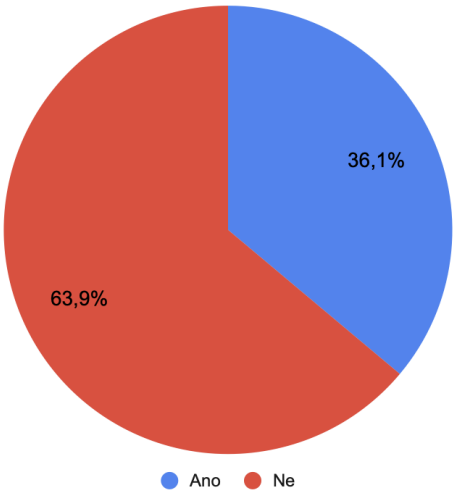
Ve třináctém otázce jsem zjišťoval, zda respondenti vědí, kdo byl Alan Turing.




Obrázek 20: Znalost Alana Turinga a toho co dokázal

Tato otázka byla pouze pro respondenty, kteří na předchozí otázku odpověděli kladně, že znají Alana Turinga. Z grafu lze vyčíst, že 54,5 % respondentů odpovědělo, že to byl matematik, který rozluštil Enigmu, 27,3 % neví a 18,2 % odpovědělo, že to byl zakladatel moderní informatiky.

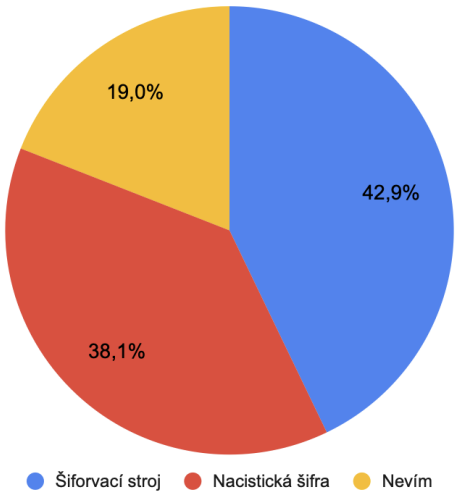
Ve čtrnácté otázce jsem zjišťoval, zda respondenti znají pojem Enigma.




Obrázek 21: Znalost Enigmy

Z grafu lze vyčíst, že 63,9 % respondentů nezná pojem Enigma a zbylá část 36,1 % zná.

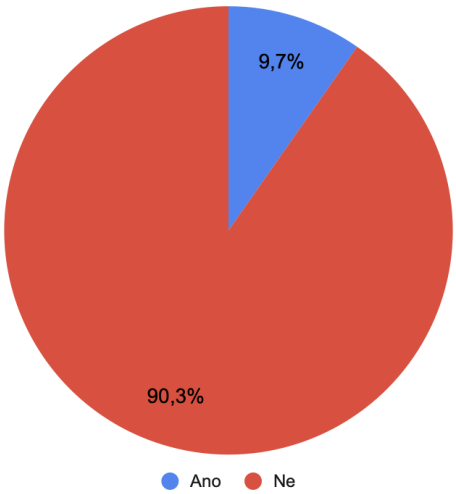
V patnácté otázce jsem zjišťoval, zda respondenti vědí, co byl pojem Enigma.




Obrázek 22: Znalost funkce Enigmy

Tato otázka byla pouze pro respondenty, kteří na předchozí otázku odpověděli kladně, že vědí, co to je Enigma. Z grafu lze vyčíst, že 42,9 % respondentů odpovědělo, že to byl šifrovací stroj, 38,1 % nacistická šifra a 19 % neví.

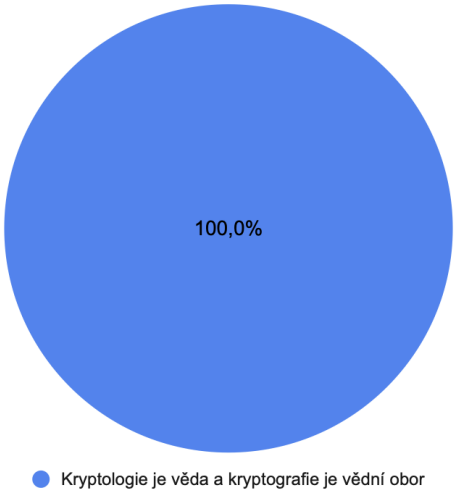
V šestnácté otázce jsem zjišťoval, zda respondenti vědí, jaký je rozdíl mezi kryptologií a kryptografií.




Obrázek 23: Rozdíl mezi kryptografií a kryptologií

Z grafu lze vyčíst, že drtivá většina respondentů (90,3 %)neví, jaký je rozdíl mezi kryprologií a kryptografií a zbylá část (9,7 %) tento rozdíl zná.

V sedmnácté otázce jsem zjišťoval, zda respondenti znají konkrétní rozdíl mezi kryptologií a kryptografií.




Obrázek 24: Konkrétní rozdíl mezi kryptografií a kryptologií

Tato otázka byla pouze pro respondenty, kteří na předchozí otázku odpověděli kladně, že znají konkrétní rozdíl mezi kryptografií a kryptologií. Z grafu lze vyčíst, že všichni respondenti znali rozdíl mezi kryptografií a kryptologií.

# 11 Rozhovor s odborníkem v oboru kryptografie z katedry informační bezpečnosti na Fakultě informačních technologií ČVUT

Rozhovor jsem prováděl s odborníkem, který se věnuje kryptologii a kryptografii. Vyučuje ji na vysoké škole a věnuje se jí i v pracovním životě.

1. Mohl byste mi prosím říci něco málo o Vaší práci, studiu?

   *„Vystudoval jsem na fakultě informačních technologií ČVUT obor počítačová bezpečnost a pokračoval dále v doktorském studiu se zaměřením na kryptologii. Nyní jsem těsně před dokončením, zbývá obhajoba dizertační práce. Moje hlavní profesní zaměření je vývojář aplikací, bezpečnosti a kryptologii se věnuji ze zájmu, mimo svou hlavní profesi. Mám zde však i praktické zkušenosti, šířit se o nich nechci.“*

2. Co Vás přivedlo k tomu, abyste se věnoval problematice kryptografie?

   *„V druhé polovině 90. let jsem připojil svůj počítač do internetu a velmi rychle mě zaujala problematika zabezpečení počítačů k němu připojených. Z toho se postupně vyvinul zájem o jejich bezpečnost jako takovou a jedním ze způsobů, jak jí dosáhnout, bylo šifrování. No a šifrování je jednou z věcí, kterou kryptologie dělá.“*

3. Co je to šifrování?

   *„Šifrování je postup, který nám umožňuje upravit data a informace do takové podoby, aby jejich obsah dokázal přečíst pouze ten, kdo je k tomu oprávněn, přestože šifrovanou podobu má volně k dispozici. “*

4. Kde šifrování začalo?

   *„Jako každá ”správná vědní disciplína”i kryptografie může dohledat své kořeny do staré antiky. Už staří Římané (skutečně! Máme to doloženo.) používali při přenosu citlivých informací techniky, které dnes nazýváme kryptografií, byť pochopitelně z dnešního pohledu poměrně slabou.“*

5. Na jakém principu funguje šifrování?

   *„Základním principem šifrování je, že data, jejichž obsah chceme utajit, a tajný klíč, jsou vloženy do šifrovacího algoritmu, který je určitým, přesně definovaným způsobem, ”promíchá”a vyprodukuje na jejich základě výstup, který je nerozlišitelný od náhodných dat. Pouze za pomoci příslušného dešifrovacího klíče jde takový výstup následně dešifrovat do původní podoby. “*

6. Jakým způsobem se dešifrovalo dřív?

*„Dvě základní kryptografické techniky z historie se nazývají substituce (nahrazování písmen, skupin písmen nebo celých slov jinými symboly) a transpozice (změna pořadí písmen, skupin nebo slov ve zprávě). Obě se používají i v moderních šifrách. Základní rozdíl najdeme zaprvé v rozsahu takových úprav (dnešními slovy, historické klíče byly velmi malé, při znalosti šifry stačilo vyzkoušet jen několik málo možných klíčů, než útočník dokázal zprávu rozluštit) a zadruhé v naprosto zásadním požadavku na utajení algoritmu šifry (jak přesně pro daný klíč probíhá substituce i transpozice). “*

7. Jakým způsobem se dešifruje teď?

   *„Moderní algoritmy jsou v první řadě mnohem rozsáhlejší, aby odolávaly i výpočetní síle počítačů - a to nejen těch dnešních, ale i těch z představitelné budoucnosti, např. za tisíc let. Jsou postaveny na dobře prozkoumaných a ověřených matematických základech a procházejí velmi důkladným testováním vědců z celého světa. To je umožněno tou vůbec nejzásadnější změnou ve filozofii návrhu šifer proti historickým šifrám - šifra musí být veřejná, její bezpečnost nesmí být založena na utajení algoritmu; všechny utajované šifry jsou automaticky vnímány přinejlepším jako podezřelé.“*

8. Používají se nějaké šifry z minulosti i teď?

   *„Záleží, z jak dávné minulosti myslíte a k jakému účelu je chcete použít. Středověké šifry můžeme najít jako součást některých her např. na dětských táborech nebo jako úkolů v geocachingu či tzv. capture-the-flag úlohách, pro ”vážné”utajení informace se ovšem nehodí. Totéž platí pro drtivou většinu šifer nejméně do konce druhé světové války. Ale jsou výjimky - např. Vernamova šifra (1919, ale byla popsána už v 19. století) je i z dnešního pohledu neprolomitelná bez znalosti klíče, dokonce ”více neprolomitelná”než moderní šifry: U moderních šifer je představitelné, že někdo dostane geniální nápad a vyřeší dosud neřešitelný problém, nebo že vývoj v technice umožní zvýšit výkon počítačů do takové míry, že šifru prolomíme hrubou silou. Vernamovu šifru prolomit nelze, jedině nějak získat její klíč (ukrást, získat od držitele úplatkem nebo mučením, aj.).“*

9. Šifruje se stále ještě ručně nebo jen pomocí počítačů?

   *„Drtivá většina šifrování dnes probíhá pomocí počítačů prostě proto, že člověku by trvalo příliš dlouho, než by rozumně silné šifrování dokázal ručně udělat. Někteří to přesto zkoušejí, ale tato snaha je vesměs odsouzena k neúspěchu. Existují nicméně i návrhy silných šifer, které počítač nepotřebují, např. šifra Solitaire (autorem je Bruce Schneier), a které mohou mít uplatnění ve specifických situacích - pokud je například vlastnictví počítače samo o sobě podezřelé nebo dokonce rovnou trestné.“*

10. Lze dešifrovat složité šifry i bez počítače?

*„Záleží v první řadě, co myslíte složitou šifrou. Známe složité šifry, které bezpečné nejsou a dají se prolomit i ručně, a dále každá silná šifra (silná šifra není totéž co složitá) může být prolomena - někdy i ručně, pokud je nesprávně použita. Například Vernamova šifra, kterou jsem zmiňoval výše, je absolutně bezpečná, ale jen je-li použita správně; porušíme-li kterýkoliv z jejích tří předpokladů, stane se prolomitelnou, a to zcela triviálně a zvládneme to i ručně.“*

11. Jak se kryptovalo v minulosti, když neexistovala výpočetní technika?

    *„Používaly se různé pomůcky, které šifrování usnadňovaly, např. speciální mřížky s otvory, které určovaly, do kterého okénka v čtvercové matici se má písmenko při transpozici zapsat. “*

12. Jak to bylo doopravdy s Enigmou?

    *„Popravdě řečeno, nevím. Uvádí se, že Poláci zjistili řadu vlastností Enigmy, na které pak navázali Britové, ale nedokázali ji prolomit celou. Jak to bylo skutečně by Vám asi řekl spíš historik. “*

13. Je podle Vašeho názoru možné využít některé metody nebo přístroje z minulé doby pro kryptování i v dnešní době nebo je už vše postaveno pouze na počítačích?

    *„Možné to je, ale nevidím pro to dobrý smysl. Vizte také odpověď 8 a 9.“*

14. Existuje v historii další příklad kryptování jako byla Enigma, o kterém by věděla široká veřejnost?

    *„Myslíte z pohledu toho, že dnes (skoro 80 let po jejím slavném prolomení ve 2. světové válce a 100 let po jejím vzniku) ví o Enigmě mnoho "běžných lidí"(mimo obor) název a část jejího příběhu? Pak je odpověď "NE", už jen proto, že k událostem svou velikostí a významem srovnatelných s 2. světovou válkou nedochází zase tak často a když už nastanou, tak se v nich šifrování třeba vůbec neuplatní, takže si jeho prolomení nemůže získat takový zájem). Počkejte dalších 80 let a můžeme se podívat, jak moderní šifry obstály.“*

15. Bylo v oblasti kryptování nějaké období, kdy z Vašeho pohledu nebyl žádný zásadnější objev, který by tuto vědu posunul dále, je vůbec možné se v současné době v oblasti kryptování ještě někam posouvat?

    *„Tak například téměř celý středověk byl v tomto ohledu bez zásadnější změny. Dokonce i 20. století se v tomto ohledu vyznačovalo spíše skokovými změnami než tím, že by se neustále dělo něco nového a průlomového. Dnešní vývoj je velmi rozsáhlý a pro člověka z oboru fascinující, ale také obtížně uchopitelný pro kohokoliv mimo obor - složitost dnešních algoritmů a zejména problémů, na nichž jsou založeny, to vylučuje. Obrovské otevřené pole působnosti je např. v*

*oblasti kvantových kryptografických algoritmů, kde toho k řešení zbývá opravdu mnoho.“*

16. Na základě Vašich zkušeností je větší pravděpodobnost zlepšení systému (nebo objevení nového postupu) spíše dlouhodobá systematická činnost nebo náhodný objev při „rutinní“ práci?

    *„Vymyslet nový a lepší algoritmus klidně může být i věc náhody a intuice. Ale to ještě nic neznamená - ani sebegeniálnější takový intuitivní algoritmus nikdo, kdo se v oboru orientuje, nebude používat, dokud nebudou jeho vlastnosti prověřeny velmi důkladným a rozsáhlým testováním. A možná ani potom, pokud tento algoritmus nebude vykazovat zcela zásadní zlepšení proti algoritmům dosud používaným - rozhodně nebude stačit "dvojnásobné zrychlení".“*

17. Kde se aktuálně šifruje nejvíce?

    *„V absolutních číslech bych asi řekl "na internetu"- pokaždé, když použijete protokol HTTPS (dle statistik je výchozí pro 80 % všech webových serverů, prohlížeče ho mají jako výchozí všechny, které vznikly v posledních několika letech), tak používáte šifrování. Každá načtená stránka na internetu má nejméně jedno šifrování pro požadavek na stránku, jedno šifrování pro odpověď na tento požadavek a desítky až stovky dalších požadavků na komponenty stránky (obrázky, skripty, atd.), krát dvě (ke každému požadavku odpověď).“*

18. Existuje nějaká neprolomitelná šifra?

    *„Pokud myslíte absolutně, bez jakéhokoliv "ale", tak ano, např. Vernamova šifra. Pokud myslíte prakticky, tedy např. ve smyslu "neznáme žádnou technologii, která by i v mnohaletém výhledu (miliony nebo miliardy let) měla šanci šifru prolomit", tak ano, např. AES.“*

19. Je veřejnost dostatečně informována ohledně kryptografie?

    *„Ano. Jsou k dispozici jak papírové knihy, tak spousta materiálů na internetu. Kdo chce materiály k některé z běžně používaných šifer najít, tak tu možnost jednoznačně má. “*

20. Jaké jsou nejčastější mylné představy o Vašem zaměstnání?

    *„Představa bezpečnostního specialisty, jak ji známe z filmů, je úplně mimo.“*

21. Existuje nějaká forma kryptování, kterou lidé přijímají jako normální?

    *„Ano, každá, o které nevědí. Takže například automatické šifrování hovorů prováděných mobilním telefonem, automatické šifrování komunikace mezi prohlížečem internetu a internetovým serverem, nebo šifrování používané pro ochranu her proti kopírování.“*

22. Co si myslíte o základech kryptografie v hodinách informatiky na základních a středních školách?

    *„Nedokážu odpovědět, nemám nejmenší tušení, jestli a jak se o kryptografii vyučuje na základních nebo středních školách dnes. V době, kdy jsem je navštěvoval já, o této problematice nezaznělo ani slovo. A nejsem přesvědčen o tom, že by bylo účelné to mít jinak - běžný občan podle mě nemá žádný důvod být o kryptografii detailně informován, je zodpovědností kryptologů, aby kryptografii navrhli správně, a úkolem tvůrců programů i zařízení, aby ji implementovali tak, aby o ní uživatel vědět nemusel. Smysl by měla výuka o tom, jak bezpečně přemýšlet a chovat se, ale k tomu není potřeba kryptografie.“*

23. Jaká je uplatnitelnost studentů po absolvování oboru kryptografie případně jejich umístění na trhu práce mimo systém školství?

    *„Přímo kryptografie by až tak moc poptávaná ani být neměla - měly by se používat zejména ověřené algoritmy, vyvíjet vlastní ”na koleni”je krajně nežádoucí. Navíc si nejsem jistý, jestli je vůbec někde (i mimo ČR) kryptografie vyučována přímo jako samostatný obor. Běžně se ovšem vyskytuje jako součást oboru zaměřeného na bezpečnost a tam je uplatnění obrovské a stále rostoucí. Informace dnes nacházíme všude a potřebu je chránit taktéž. Z rozhovorů se studenty mých předmětů mohu říci, že neznám ani jednoho, který by neměl uplatnění ještě před dokončením studia, leda že by ho sám odmítl. “*

24. Co si myslíte, že by bylo možné udělat pro zlepšení kryptografie ze strany vzdělávání (školství) nebo ze strany vládních organizací či vlády?

    *„Částečně vizte předchozí otázky. Z mého pohledu, čím méně bude vláda o něčem z oboru rozhodovat, tím lépe. Máme NÚKIB, který vydává doporučení, to mi přijde jako zcela dostačující - aspoň se o to starají odborníci, kteří oblasti rozumí. Nechtěl bych se dočkat toho, že o tom budou rozhodovat ministři formou vládních nařízení nebo poslanci formou zákonů.“*

25. S jakým problémem v oblasti kryptování se v současné době potýkáte?

    *„Aktuálně hlavně s tím, že sice máme silné algoritmy, ale nesprávně je používáme. Hledám příčiny těchto nesprávných použití a způsoby, jak je odstranit. “*

26. Myslíte si, že oblasti kryptování se dostává dostatek kreditu a respektu vzhledem k jiným oblastem vědy?

    *„Asi záleží, jak kde. Ale řekl bych, že ano - pokud někde mezi ne-odborníky řeknu, že se zabývám kryptologií, dostane se mi stejné směsi obdivu a politování, jako kdybych se přihlásil k čemukoliv jinému, co zní tajemně a složitě, třeba neurochirurgii, průzkumu planet mimo sluneční soustavu nebo šamanským rituálům. “*

27. Myslíte si, že ve Vašem oboru mají stejnou pozici muži i ženy nebo má ke kryptování větší dispozice jedna z těchto skupin?

    *„Nevšiml jsem si nikdy, že by kdokoliv řešil pohlaví kryptologů. Muži se vyskytují častěji, ale jestli je to dané objektivními faktory nebo diskriminací, to nedokážu posoudit. “*

28. Říká Vám něco systém ADAM?

    *„Ne.“*

29. Existuje nějaký druh kryptování který jste si nevyzkoušel, ale chtěl byste?

    *„Těžko říct. Nenapadá mě nic, co bych si nemohl vyzkoušet, kdybych dost chtěl. Mohou do toho vstupovat omezení, že den má jen 24 hodin a z nich část potřebuji spát, ale pokud se vyskytne něco, co opravdu hodně chci zkusit, tak podle mě vždy existuje způsob, jak to udělat. Z této definice pak vyplývá, že co jsem nezkusil, to jsem asi nechtěl dost hodně. “*

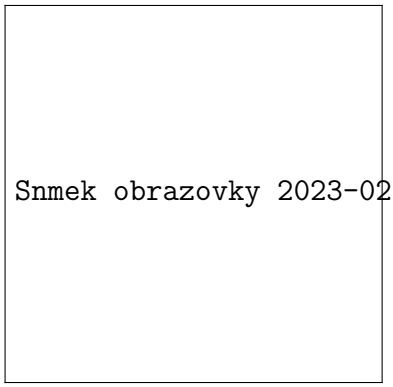
# 12 Vlastní šifra a její princip

Šifra funguje na principu, že se šifrátor a příjemce předem domluví na textech (nejlépe literární dílo), z kterých se čerpá. Každý týden v měsíci je jiné předem domluvené dílo.

Každé písmeno má své souřadnice, které se zadávají do šifrovacího čtverce (čtverec 3x3 s 5 zadělanými políčky). Šifrovací čtverec má šifrátor i příjemce.

**Šifrovací čtverec** Šifrovací čtverec se nasazuje na kryptogram a zobrazí správná platná čisla, která nám zobrazí souřadnice v textu dle pravidla:

1. Číslo = strana, kde se nachází cílové písmeno
2. Číslo = řádek od začátku strany
3. Číslo = pořadí slova v řádku
4. Číslo = písmeno slova




Obrázek 25: Šifrovací čtverec

**Postup při šifrování**

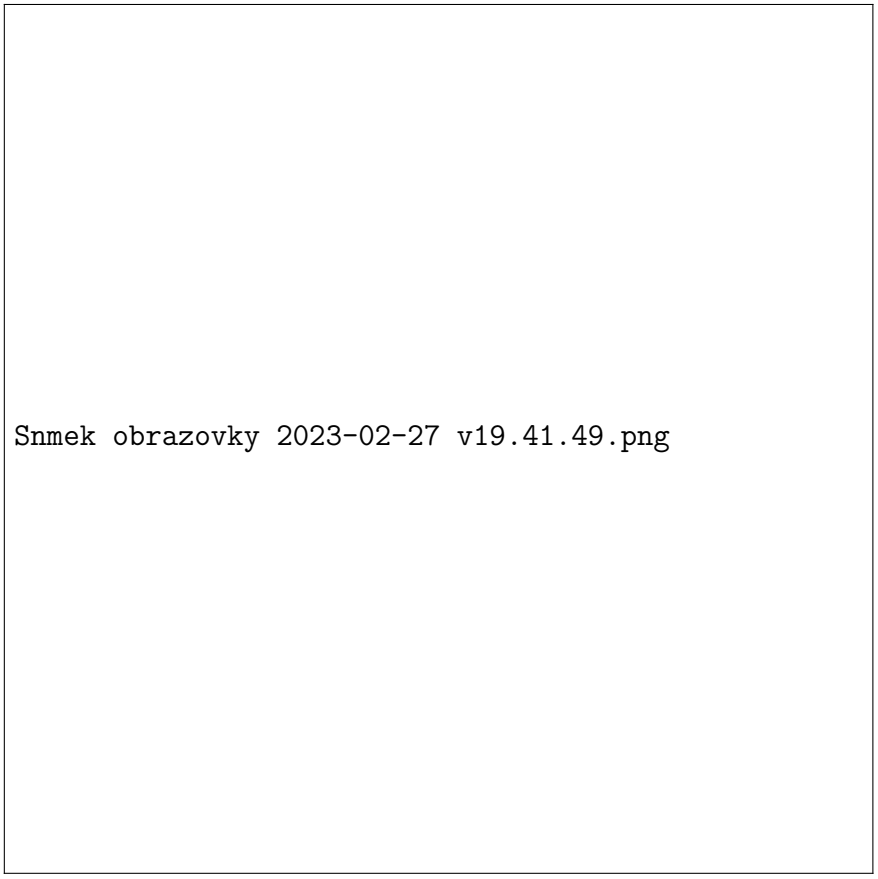
1. Najit písmeno v knize
2. Zapsání jeho souřadnic na příslušná místa v šifrovacím čtverci
3. Náhodně vyplnit zbylá políčka
4. Složit celé slovo
5. Odeslat

**Postup při dešifrování**

1. Nasazení šifrovacího čtverce na první kryptogram
2. Najití písmena dle souřadnic v knize
3. Dešifrování celého slova

## 12.1 Příklad

Modelová situace: Aktuálně je první týden v měsíci a já budu k šifrování používat dle domluvy text 1.




Obrázek 26: Text 1

**Šifrování**

- Otevřený text: HELLO
- Klíč: Text 1
- Kryptogram:

**Dešifrování**

1. Kryptogram: viz Kryptogram 1
2. Klíč: dle domluvy Text 1
3. Kryptogram po nasazení šifrovacího čtverce
4. Zobrazily se nám souřadnice písmen v dokumentu, takže si je napíšeme a vznikne nám slovo H E L L O
5. Otevřený text: HELLO

# 13 Vyhodnocení a shrnutí výsledků

V této kapitole shrnu všechny své sesbírané poznatky a zpracuji je.

## 13.1 Celkové shrnutí výsledků analýzy dotazníkového šetření

Na dotazník odpovědělo celkově 70 respondentů, kde převažovaly zejména ženy, kterých bylo až 70 %. Nejvíce dotazovaných bylo věkové skupiny 16-20 let a nejméně dotazníků jsem získal od osob v rozmezí 41-60 let.

Ohledně otázky, zda respondenti mají povědomí o pojmu kryptografie, zvolilo přesně 70,8 % odpověď „ano“. Z těchto procent dokázalo vysvětlit pojem kryptografie 78,3 % dotázaných. Odpovědi, které se týkaly vzniku kryptografie, se velmi lišily. Nejvíce převahovala odpověď, že tento obor vznikl ve dvacátém století, dalšími častými odpověďmi byly starý Egypt, starověk a v neposlední řadě devatenácté století.

V šesté otázce jsem se otázal, zda dotazovaný zná nějakou šifru. Ukázalo se, že více než půlka (konkrétně 52,8 %) ji zná. Více než 40 % nadále zmínilo, že jsou obeznámeni s Morseovou abecedou, dále 25 % se šifrou mistra Leonarda, ale také byla zmiňována i Cézarova šifra či Enigma. Více než 70 % respondentů už zkoušelo šifrovat, přičemž nejvíce dotazovaných použilo Morseovu abecedu a Cézarovu šifru.

Když jsem se ptal na kryptografii a její roli v oblasti vědy, přesně 60 % dotazovaných zodpovědělo, že je velmi důležitá, naopak skoro třetina uvedla, že má pouze malou roli. 62,5 % respondentů se zmínilo, že by neměli zájem o předmět kryptografie. Pouze čtvrtina by uvítala tento obor v hodinách ve škole.

Nadále jsem se tázal na Alana Turinga, kde 76,1 % uvedlo, že někdy slyšeli toto jméno, avšak pouze 54,5 % z těchto procent věděli, kdo byl tento matematik a o co se zasloužil. V další otázce jsem navázal pojmem Enigma, kdy 63,9 % respondentů jsou obeznámeni s tímto pojmem, ale pouze 38 % dokázalo správně odpovědět na otázku, co je to Enigma.

V neposlední řadě jsem zjišťoval rozdíl mezi kryptografií a kryptologií. Bohužel tento pojem odlišuje pouze 9,7 % mých respondentů, kteří v následující otázce všichni věděli, že kryptologie je věda a kryptografie je vědní obor.

## 13.2 Celkové shrnutí výsledků vyplývajících z rozhovoru s odborníkem

Dotazovaný vystudoval na fakultě informačních technologií ČVUT obor počítačová bezpečnost, kde se v dalším studiu zaměřil na kryptologii. Jeho hlavním zaměřením je vývojář aplikací, bezpečnosti a kryptologii se věnuje ze zájmu. Uvedl ale, že s ní má i praktické zkušenosti.

Jeho hlavním podnětem pro studium této vědy byla špatná zabezpečenost počítačů k internetu, které si všiml, jakmile připojil svůj počítač do internetu.

Šifrování mi v rozhovoru popsal jako postup, který nám dovoluje upravit data a informace do podoby, aby obsah přečetl pouze ten, kdo je oprávněn, přestože šifrovanou podobu má volně k dispozici každý.

Šifrování začalo už ve staré antice, stejně jako ostatní správné vědní disciplíny. Podle doložených podkladů dokázali už staří Římané používat techniky k přenosu citlivých informací. Dnes je toto nazýváno kryptografií, i když je v dnešní době používána stejně, ale s větší složitostí.

Základní šifrování je jednoduchá věc v podstatě, utajená data změníme natolik, aby je dokázala přečíst pouze osoba, co zná tajný šifrovací klíč.

Dříve se šifrovalo pomocí substituce. Docházelo k náhradě písmen, skupin písmem nebo celých slov symboly. Toto se přenechalo i do dnešní doby pouze s odlišností náročnosti úprav, co jsou provedeny

Hlavní rozdíl v dešifraci teď a dříve je v náročnosti. Matematika se více rozvinula a přinesla další možnosti. Důležitou změnou je i filozofie, díky které jsou šifry veřejné a to vede k menší podezřelosti. Určité šifry se používají doposud, ale jedná se spíše o herní záležitosti. Existují avšak také těžší šifry např. Vernamova. Většina šifrování probíhá na počítačích, i když jednodušší šifry se dají konstruovat a prolomit ručně. V minulosti bez výpočetní techniky se využívaly např. speciální mřížky s otvory. Tyto nástroje nyní už nejsou efektivní.

Jednou z mála známých šifer mezi širokou veřejností je Enigma. O dalších šifrách však tato skupina není dostatečně informována.

Zejména ve středověku a 20. století nedošlo k zásadnějším objevům v oblasti kryptování. V posledních letech došlo k rozvoji kryptografie a nyní se může její zlepšení stát náhodným objevem a nikoli rutinní prací. Nejvíce šifrování probíhá „na internetu“, jedná se až o 80 % a vyskytuje se na světě několik neprolomitelných šifer.

Často se vyskytují mylné představy o zaměstnání odborníka v oboru zatímco podle něj je veřejnost informovaná dostatečně. Lidé přijímají za normální šifry, ty o kterých nevědí, podle jejich názoru např. šifrování hovorů prováděných mobilním telefonem.

Důležitější je výuka ohledně bezpečnosti a chování se na internetu než kryptografie. Tento obor bývá žádaný a uplatnění je veliké. Zlepšení kryptografie ze strany školství není nutné a lidé by si měli vybírat sami, co budou studovat.

## 13.3 Celkové shrnutí vlastní šifry

Pokusil jsem se vytvořit i vlastní šifru, abych na vlastní kůži mohl vyzkoušet jaké to je a jak je těžké vytvořit takovou šifru, která ještě nebyla vymyšlena a využita. Díky mému pokusu o samostatné vytvoření šifry jsem zjistil, že vymyslet při nejmenší jednoduchou šifru není vůbec jednoduchá a rychlá věc. Vymyslel jsem pouze jed-

noduchou šifru na prostém způsobu, jejíž dešifrování by komukoli, kdo se v oblasti šifer pohybuje, netrvalo asi příliš dlouho. Z toho vyplývá, že kryptografie je velmi složitý obor, který je avšak důležitý pro lidstvo.

# DISKUZE

Cíle, které jsem si na začátku své práce určil, se mi povedly splnit v celém rozsahu. Zjistil jsem mnoho nových informací z oblasti kryptologie a kryptografie. Šifry tu jsou s námi již několik tisíc let a z mého pohledu by každý člověk měl mít o šifrách aspoň nějaké povědomí. Historické šifry jsou často vytvářeny pomocí jednoduchých matematických principů, které se dají často jednoduše prolomit, ale v té době odolávaly. Dále jsem prováděl rozhovor s odborníkem na kryptologii a kryptografii, díky kterému jsem zjistil mnoho cenných informací, které mi pomohly k úspěšnému dokončení mé práce. Má šifra sice patří mezi jednodušší a lépe prolomitelné, ale chtěl jsem ukázat na příkladu, jak vznikají šifry a že jednoduchou šifru může vymyslet každý. Určitě by se dala zdokonalit a více promyslet.

Práce má přínos zejména pro laickou veřejnost a kohokoliv, kdo má zájem o prohloubení znalostí z oblasti historie šifrování. Ve své práci popisuji historické šifry a jejich principy, které jsou velice propracované. Dále jsem se věnoval i jedné z největších osobností matematiky a moderní informatiky, Alanu Turingovi, kterému se za druhé světové války povedlo prolomit kód Enigmy.

Práci mohu porovnávat s dalšími pracemi, které již byly vytvořené a jsou volně přístupné na internetu. Mé výsledky se víceméně shodovaly s ostatními pracemi až na malé odchylky, které mohly být pravděpodobně způsobeny nedostatkem respondentů v dotazníkovém šetření. Z mého dotazníkového šetření jsem zjistil, že největší povědomí o šifrování mají respondenti ve věku od 21 do 40 let. Přičemž ostatní práce tvrdí, že největší povědomí mají osoby ve věku mezi 40 a 60 lety. Důvodem tohoto rozdílu by mohlo být to, že jsem měl nedostatek osob ve věku od 40 do 60 let.

Rozšíření práce by bylo možné o podrobnější popsání šifer a jejich fungování a zaměření se více na informace o Alanu Turingovi. V praktické části by se daly doplnit další rozhovory s odborníky v oblasti kryptologie, kryptografie a historie, aby výsledky vycházely z průzkumu více lidí. Doplněno by mohlo být i dotazníkové šetření o více respondentů s větším věkovým spektrem. Dále by se mohlo více popularizovat šifrování na školách nebo v jiných edukativních institucí, aby byla veřejnost více obeznámena o šifrování.

# ZÁVĚR

Mezi výsledky mé práce patří zjištění obeznámení veřejnosti ohledně historie šifrování a otázek spojených s touto vědou, která je tu již od začátku matematických dějin. Dále provedený rozhovor s odborníkem v oblasti informatiky, který zodpověděl mé otázky ohledně jeho názorů na danou problematiku a jednoduše vysvětlil základní pojmy týkající se mé práce.

Výzkum ukázal nedostatečnou informovanost veřejnosti, která by se dala dále zlepšovat pomocí propagace a popularizace. Ve školách by se v hodinách informatiky mělo více věnovat historii šifrování a dalším informacím spojených s tímto tématem. Ukázalo se, že pouze 52,8 % dotazovaných osob je obeznámeno s konkrétními šiframi ze svého života. Naopak třicet čtyři osob odpovědělo, že sami zkoušeli kryptovat. Ve spojitosti s vyšší informovaností veřejnosti se vyjádřila více než půlka dotazovaných, že nemají zájem o hlubší výuku kryptografie na školách. Vytvoření vlastní jednoduché šifry není náročné a lze vymyslet bez nutnosti použití drahého vybavení.

Práce se může využít jako jeden z podkladů pro informování veřejnosti o šifrování či pro osoby, které se zajímají o informatiku a chtěli by se více dozvědět o dané problematice a historii šifrování. Nedostatečné obeznámení veřejnosti by se dalo zlepšit pomocí různých přednášek, především ve školách.

# LITERATURA


[1] FARANA, R. *Šifrování: pro radost i poučení.* Brno: Mravenec, 1994. ISBN: 80-85978-00-8.

[2] ZELENKA, J. *Ochrana dat: kryptologie.* Hradec Králové: Gaudeamus, 2003. ISBN: 80-7041-737-4.

[3] GLACZOVÁ, B. *REJEWSKÉHO A TURINGOVA BOMBA*. [online], cit. 2007. URL: `https://1url.cz/orIDG`.

[4] SINGH,S, Dita ECKHARDTOVÁ a Petr KOUBSKÝ. *Kniha kódů a šifer: tajná komunikace od starého Egypta po kvantovou kryptografii.* Praha: Argo, 2009. ISBN: 978-80-7363-268-7.

[5] ZELINKA, I. *Kryptologie.* [online], cit. 2011. URL: `http://arg.vsb.cz/Data/Vyuka/PVB12.pdf`.

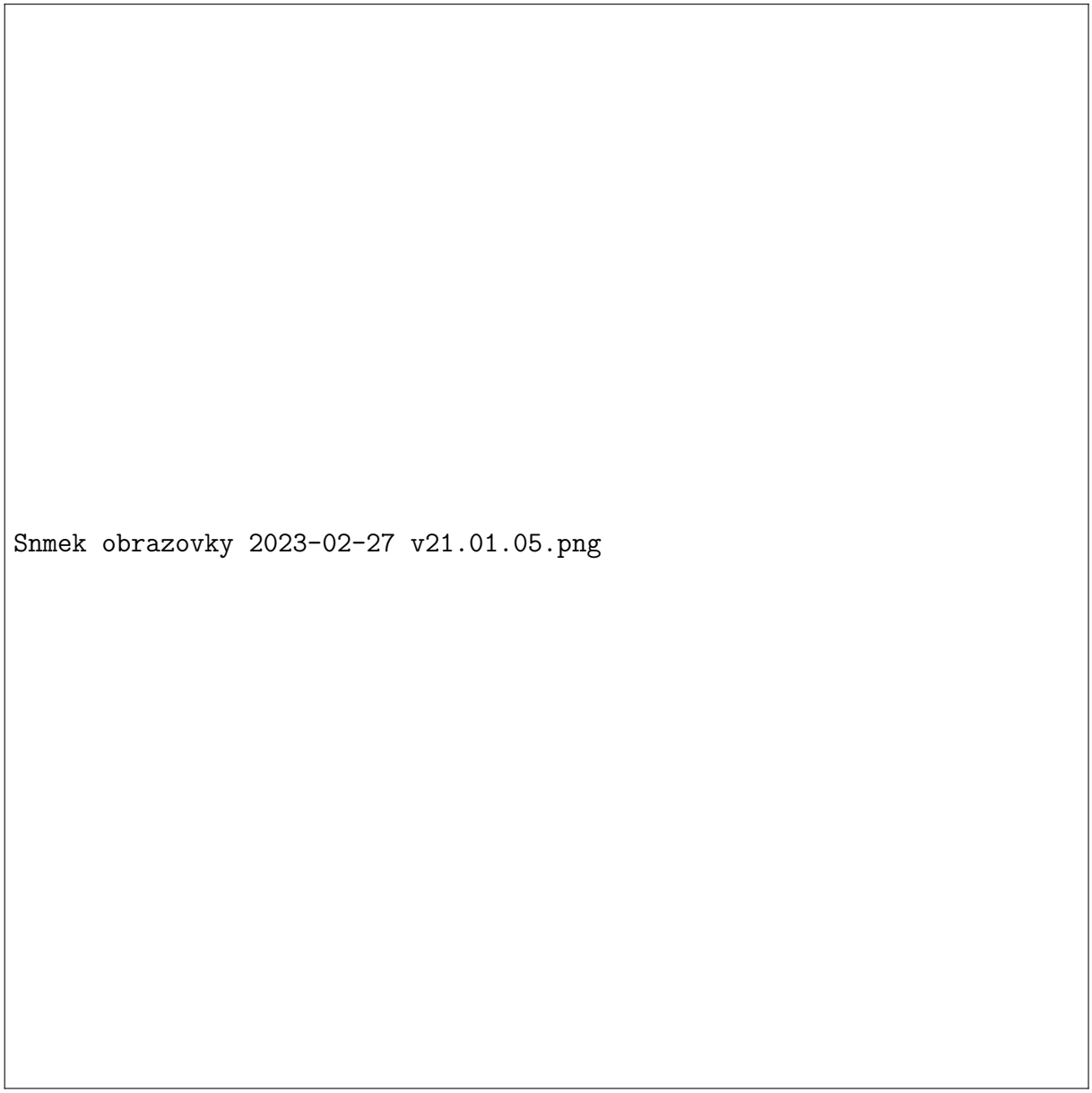
[6] MATEMATIKA polopatě. *Caesarova šifra.* [online], cit. 2006-2022. URL: `https://www.matweb.cz/caesarova-sifra/`.

[7] HVĚZDÁRNA Fr.Pešty. *Moderní symetrické šifry.* [online], cit. 4.11.2016. URL: `https://www.hvezdarna-fp.eu/news/moderni-symetricke-sifry/`.

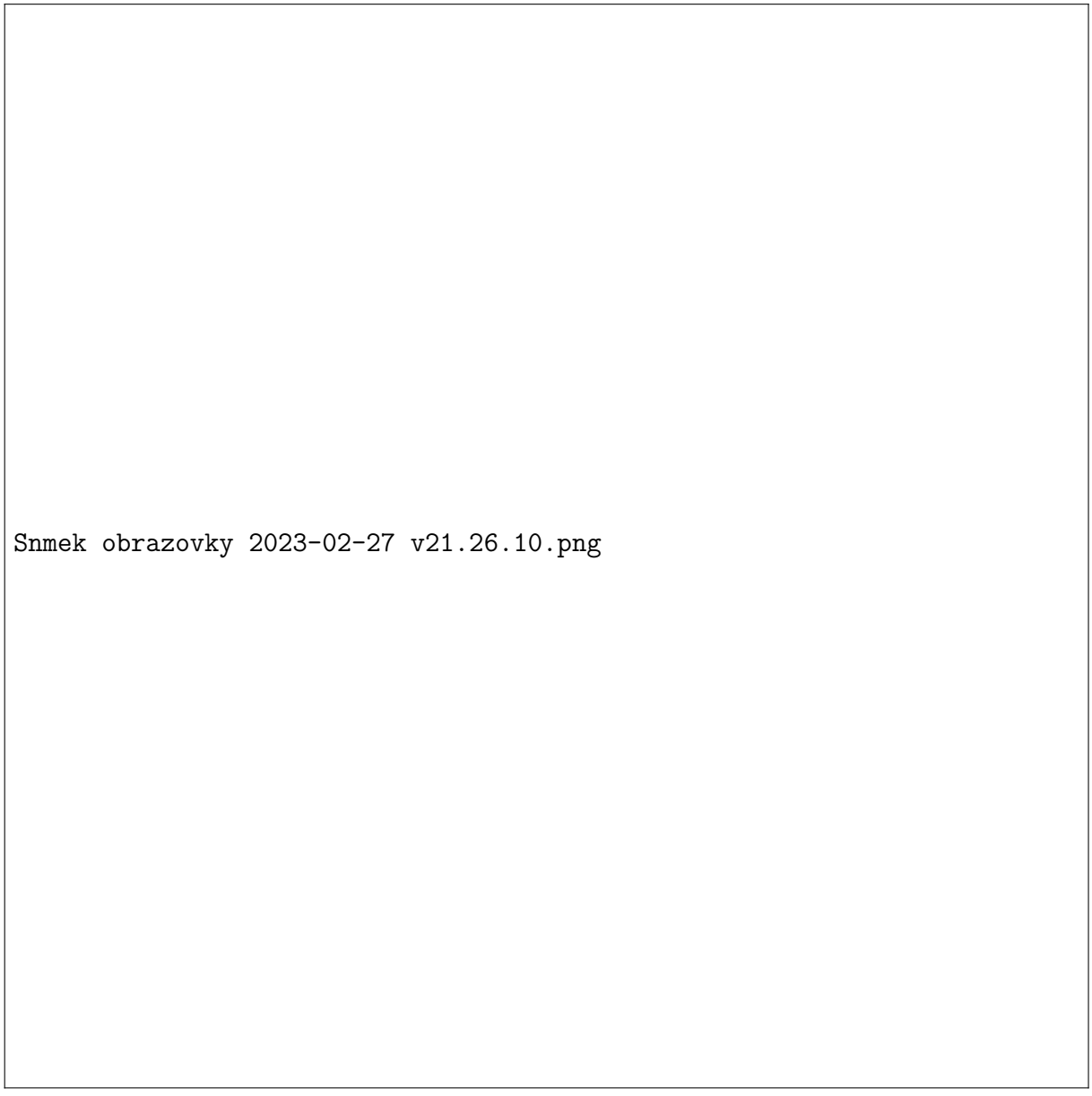
[8] DRÁB, M. *Lekce 1 - Úvod do šifrování a blokové šifry.* [online], cit. 2022. URL: `https://www.itnetwork.cz/algoritmy/kryptografie/uvod-do-%5Clinebreak%20sifrovani-a-blokove-sifry`.

[9] KARLOS. *Vernamova šifra.* [online], cit. 2011. URL: `https://www.rozpad.cz/viewtopic.php?t=780`.

# SEZNAM OBRÁZKŮ




Obrázek 27: Kryptogram 1




Obrázek 28: Kryptogram 1 po nasazení dešifrovacího čtverce