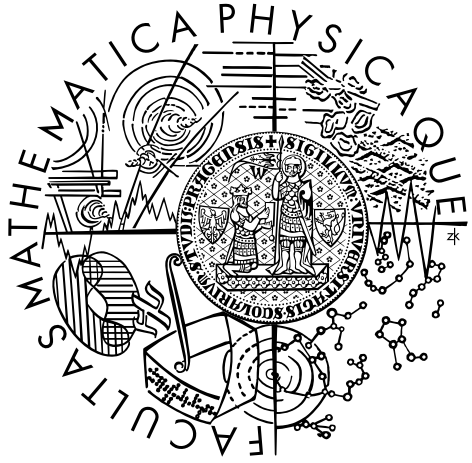
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

DIPLOMOVÁ PRÁCE



Jiřina Hrušová

Kryptografie na střední škole

Katedra didaktiky matematiky

Vedoucí diplomové práce: doc. RNDr. Jiří Tůma, DrSc.

Studijní program: Učitelství pro SŠ, matematika – informatika

Na tomto místě bych chtěla poděkovat především svému vedoucímu diplomové práce doc. RNDr. Jiřímu Tůmovi, DrSc. za velkou trpělivost a podporu, bez které bych tuto práci nedokončila, a Ing. Janu Mizerovskému, zástupci ředitelky SPŠ ST Panská, za maximální ochotu a spolupráci, kterou mi poskytl během realizace testů na této škole. Děkuji mu také za téměř otcovskou lásku, s kterou se o mě staral.

Dále bych chtěla poděkovat všem kolegům v SPŠ ST Panská, kteří se účastnili realizace testů, studentům, kteří ochotně spolupracovali a všem dobrovolníkům, kteří napsali svůj příspěvek na mých stránkách o metodách napovídání.

V neposlední řadě děkuji také Mgr. Petru Klášterecképu a doc. RNDr. Karlu Zvárovi, CSc. za odbornou konzultaci ve statistických metodách.

Prohlašuji, že jsem svou diplomovou práci napsala samostatně a výhradně s použitím citovaných pramenů. Souhlasím se zapůjčováním práce.

V Praze dne 20. dubna 2006 Jiřina Hrušová

Obsah

Kódy, šifry a další pojmy na úvod ... 4
Steganografie a kryptografie ... 5
Historie šifer ... 8
Caesarova šifra ... 8
Le chiffre indéchiffrable ... 8
Knižní šifra ... 11
Vernamova šifra – konečně bezpečí? ... 13
Moderní metody šifrování ... 15
Binární kódování ... 15
Strojové šifrování, šifrování a počítače ... 16
Problém distribuce klíče ... 19
Kvantová kryptografie ... 24
Budoucnost ... 28
Kódování informace a testy ... 29
Kódování množiny znaků ... 29
Multiple-choice testy ... 31
Předání informace ... 31
Teorie informace ... 34
Měření velikosti informace ... 34
Metody měření ... 38
Webový formulář ... 38
Sesbírané metody ... 38
Testování studentů ... 41
Podoba testů ... 41
Realizace ... 42
Výsledky ... 45
Výsledky testů ... 45
Šíření informace ... 47
Závěr ... 50
Literatura ... 52
Dodatky ... 53
Přílohy ... 56

Název práce: Kryptografie na střední škole
Autor: Jiřina Hrušová
Katedra (ústav): Katedra didaktiky matematiky
Vedoucí diplomové práce: doc. RNDr. Jiří Tůma, DrSc., Katedra algebry
E-mail vedoucího: Jiri.Tuma@mff.cuni.cz
Abstrakt:

Diplomová práce pojednává o aplikaci teorie informace na středních školách na multiple-choice testy. Snažila jsem se v ní zmapovat, jak studenti středních škol spolupracují při prověřování znalostí. Úkolem bylo zjistit, jsou-li studenti schopni si informaci o správném řešení předat nebo zkontrolovat a jakým způsobem. Vzhledem k výsledkům testů se jeví možné, že při zkoušení multiple-choice testem si studenti dokáží velice efektivně předávat informace bez vědomí učitele. Multiple-choice testy se tak nejeví jako vhodný prostředek pro získání informace o skutečných vědomostech studentů.

Klíčová slova:

teorie informace, kódování, šifrování, multiple-choice testy

Title: Cryptography in high school
Author: Jiřina Hrušová
Department: Department of Mathematics Education
Supervisor: doc. RNDr. Jiří Tůma, DrSc., Department of Algebra
Supervisor's e-mail address: Jiri.Tuma@mff.cuni.cz
Abstract:

This thesis deals with application of information theory to multiple-choice testing in high school. It attempts to map out the ways and the degree of cooperation among students when their knowledge is being examined. Our task was to find out whether students are able to distribute the information about the right solution or check it among themselves and in what ways. Our results show that it is possible that students information distribution channels may be exceedingly effective in multiple-choice testing. Thus, multiple-choice testing does not appear to be an appropriate instrument if truthful information about the students knowledge is to be obtained.

Keywords:

information theory, coding, encryption, multiple-choice tests

Úvod

Tématem diplomové práce je aplikace teorie informace na středních školách v testech s výběrem jediné správné odpovědi. Vzhledem k malému množství informace obsažené v odpovědích na otázky se studentům naskýtá příležitost k jednoduché komunikaci bez vědomí učitele a k předání si nebo ověření svých odpovědí. Snažila jsem se zmapovat, jak studenti středních škol spolupracují při prověřování znalostí. Po krátkém uvedení studentů do problematiky teorie informace, kódování a šifrování, jsem se zaměřila na testování, zda jsou schopni správně aplikovat nové znalosti k dosažení lepších studijních výsledků. Realizace probíhala na střední škole SPŠ ST Panská, Praha. Prvotním úkolem bylo zjistit, jsou-li studenti schopni si informaci o správném řešení předat nebo zkontrolovat a jakým způsobem. Dále jsem zjišťovala, zda používají nějaké šifrovací a kódovací metody a jakým způsobem je aplikují. Podklady byly také sesbírány průzkumem mezi jinými studeny, učiteli a přáteli, kteří byli ochotni popsat metody a postupy, s kterými se prakticky nebo zprostředkovaně setkali.

Při hledání odpovědi na domněnku, zda studenti zlepší své studijní výsledky, se naskytla otázka, jakým způsobem se informace šíří po třídě a dostane-li se mezi všechny studenty? Nebo bude zachycena pozorným učitelem? Také na tuto otázku jsem se snažila najít odpověď.

Kapitola 1
Kódy, šifry a další pojmy na úvod

Na úvod je třeba si vyjasnit základní pojmy. **Kryptografie** je věda, která se věnuje návrhu nových šifrovacích systémů. Zkoumáním šifrovacích systému, zjišťováním síly šifer a jejich luštěním se zabývají kryptoanalytici a oboru, který zastupují říkáme **kryptoanalýza**. Oba obory pak souhrnně nazýváme **kryptologie**. Zprávě, jejíž obsah chceme utajit, říkáme **otevřená zpráva** či otevřený text. Po zašifrování ji nazýváme **šifrovou zprávou** nebo také šifrovým textem a procesu převádění otevřené zprávy na zprávu šifrovou říkáme **šifrování**. Při šifrování často pracujeme pouze s anglickou abecedou, která obsahuje 26 písmen, bez interpunkčních znamének, rozlišení velikosti písma a národních znaků. Při šifrování v češtině bychom tak zprávu 'Příliš žluťoučký kůň úpěl ďábelské ódy.' převedli na 'priliszlutouckykunpeldabelskeody'. Taková omezení se zavádí proto, aby se z textu odstranilo co nejvíce informace o struktuře otevřeného textu a jazyku, v kterém byl napsán, protože by tyto postranní informace případnému luštiteli usnadnily dešifrování. Na druhou stranu, odstranění diakritiky či mezer může vést ke špatnému pochopení textu a to především u krátkých zpráv, jak si lze všimnout na příkladu OSVOBODITNEOBESIT, který můžeme interpretovat jako OSVOBODIT, NE OBĚSIT nebo také jako OSVOBODIT NE, OBĚSIT.

Dalšími pojmy, mezi kterými je potřeba rozlišovat, jsou kódy a šifry. Co je kód a co je šifra?

Kódy jsou většinou veřejně známé a používají se jako určitý standard, který má usnadnit komunikaci. Kódovou abecedou může být stejná abeceda nebo zcela nové značky – 0 a 1, tečka a čárka, ♡, ⋆ a ‡ atp. Kód je potom sestaven ze znaků kódové abecedy a musí být různý pro každý znak otevřené abecedy.

Jako příklad uveďme Morseovu abecedu: Jednotlivým písmenům abecedy (popřípadě i číslicím) A = {A, B, ..., Z, 0, 1,..., 9} jsou přiděleny kódy z množiny B = {·, −, |} v podobě posloupností teček, čárek a mezer (které budeme značit |) tak, jak je uvedeno v tabulce Tab. 1. V příkladu pod tabulkou pro jednodušší orientaci oddělujeme jednotlivá slova || a větu |||. V praxi se používá pouze | pro oddělení kódů jednotlivých písmen, ostatní interpunkční značky (mezera mezi slovy, či konec věty) se doplňují podle kontextu. Morseova abeceda se používala při telegrafické komunikaci. Tečka odpovídala krátkému pípnutí, čárka dlouhému pípnutí a mezera krátké pomlce, která znamenala konec vysílání kódu jednoho písmene.

Otevřený text: Takto vypada zprava v morseove abecede.

Text v Mors. abecedě: −| · −| − · − | − | − − − || · · · −| − · − −| · − − ·| · −| − · · | · −||
− − · · | · − − ·| · − · | · −| · · · −| · −|| · · · −||
− − | − − − | · − · | · · · | · | − − − | · · · −| · ||
· − | − · · ·| · | − · − ·| · | − · · | · |||

Otevřená abeceda	Morseova abeceda	Otevřená abeceda	Morseova abeceda
A	· –	N	– ·
B	– · · ·	O	– – –
C	– · – – ·	P	· – – ·
D	– · ·	Q	– – · –
E	·	R	· – ·
F	· · – ·	S	· · ·
G	– – ·	T	–
H	· · · ·	U	· · –
CH	– – – –	V	· · · –
I	· ·	W	· – –
J	· – – –	X	– · · –
K	– · –	Y	– · – –
L	· – · ·	Z	– – · ·
M	– –		

Tab. 1: Morseova abeceda.

Šifry, narozdíl od kódů, se používají pro utajení *obsahu* zprávy, která je posílána. Jejich smyslem není zjednodušit komunikaci, ale zabránit tomu, aby se informace v zaslané zprávě dostala do nepovolaných rukou. Každou šifru lze popsat pomocí nějakého pravidla – algoritmu. Pravidla pro šifrování a dešifrování jsou veřejně známá a může je použít každý, kdo má klíč. Síla šifry tedy spočívá ve správném zvolení klíče, který zná pouze odesílatel a příjemce, kterému je zpráva určená. Při posuzování kvality nového šifrovacího systému se pak předpokládá, že případný luštitel zná systém, kterým byla zpráva zašifrována, ale nezná klíč.

1.1 Steganografie a kryptografie

Starší metodou utajení zpráv, s níž se setkáváme již v dobách starověku, je **steganografie**. Tehdy ještě lidé neznali lepší způsob utajení, než bylo důmyslné ukrytí zprávy, aniž by byl její text nějakým způsobem šifrován. Tak vzniklo také pojmenování metody, z řeckých slov *steganos* – 'schovaný' a *graphein* – 'psát'. Její nevýhodou je použitelnost pouze do té doby, než ostatní objeví, kam byla zpráva ukryta.

Uveďme si několik příkladů úspěšného použití steganografie. První skupinu tvoří zprávy, jež byly *důmyslně ukryty* na nejneočekávanějších místech.

V antickém Řecku měl posel doručit tajnou zprávu. Poslovi oholili hlavu, text zprávy na ni napsali a počkali, až jeho vlasy zprávu bezpečně skryjí. Pak se posel mohl vydat na cestu. Když dojel na místo určení, příjemce mu hlavu opět oholil a text zprávy přečetl.

Staří Číňané zalili zprávu napsanou na hedvábí do malé voskové kuličky, kterou posel polkl.

Další podskupinu steganografie tvoří tzv. *neviditelné inkousty*. Zprávy napsané neviditelným inkoustem se zobrazí až po vykonání procedury zviditelnění, který odpovídá chemickým vlastnostem inkoustu. Nejznámějším neviditelným inkoustem používaným dětmi při hrách je obyčejná citrónová šťáva, kterou napíší text zprávy (například pomocí štětce) na papír. Pro přečtení zprávy pak stačí papír nahřát (například nad svíčkou) a stopa vytažená inkoustem zhnědne.

Již z 1. století n. l. pochází návod, jak použít jako neviditelný inkoust mléko pryšce. Zaznamenal jej Plinius Starší. Inkoust je po zaschnutí průhledný a po zahřátí též zhnědne.

Ve středověku italský vědec Giovanni Porta popsal sloučeninu, pomocí které lze ukrýt zprávu do vajíčka. Může se nám to zdát neuvěřitelné, ale ve skutečnosti se jedná o jednoduchou chemickou reakci: Čirou sloučeninou, vyrobenou z jedné unce kamence a pinty octa, se na skořápku vejce napíše text zprávy, sloučenina skořápku prostoupí a stopu inkoustu zanechá v bílku. Vejce se zprávou posel doručí adresátovi, ten vejce uvaří, oloupe a text, který uvízl čitelný ve ztuhlém bílku, si přečte.

Možná si říkáte, že steganografie dnes již nemá použití, ale není tomu tak. Poslední skupinu, která také spadá do steganografie, představuje *vložení tajné zprávy do jiné* – neškodně vypadající.

Známý je například způsob předání tajné zprávy v tzv. **mikrotečce**, který používali Němci za druhé světové války. S pomocí fotografických metod zmenšili text celé zprávy do jediné malé, nenápadné tečky za větou – mikrotečky. Text, který mikrotečky obsahoval, mohl být naprosto libovolný a otevřený všem, protože utajená zpráva byla pouze v tečkách za větami. Tato metoda byla Němcům velmi užitečná do doby, než si někdo všiml, že papír, na kterém se zprávy předávají, se podezřele leskne.

Skrýt jednu zprávu do druhé lze jednoduše tak, že text tajné zprávy tvoří například druhé písmeno každého slova zprávy veřejné. Veřejná zpráva může být jakákoliv – například v podobě novinového inzerátu. Takto si například domlouvali dostaveníčka milenci v 19. století.

Také skrytí jednoho digitálního obrázku do druhého je moderním způsobem využití steganografie. Digitální obrázky jsou v počítači uloženy pomocí 1 a 0 do tzv. bitů. Způsoby uložení obrázků po jednotlivých bitech záleží na použitém formátu. Všechny používané formáty jsou dobře známé a lze je nalézt například na Internetu. Obrázky v jistých formátech obsahují bity, které jsou „méně důležité“ a ty lze použít pro vložení bitů druhého obrázku. Při vykreslení se pak otevřený obrázek zobrazí beze změn, ale vhodným zpracováním můžete odhalit i druhý – ukrytý.

Tím bychom opustili příklady steganografie a podívali se na další metody. Jak je patrné z předchozích odstavců, nevýhoda steganografie spočívá v jejím jednorázovém použití. Jakmile totiž zprávu zachytíte a zjistíte, jak je ukryta, je vše prozrazeno. Můžete snadno prověřit všechna místa a způsoby, které jsou známé jako místo ukrytí – tj. oholit hlavu každému poslovi, uvařit všechna získaná vejce, či zvětšovat tečky za větami v listinách, které jsou převáženy. Takový závěr se může jevit dosti absurdní, ale pouhá možnost prověřit a odhalit takto ukryté zprávy činí steganografii pro dnešní použití

nedůvěryhodnou. Zvláště známe-li dokonalejší metody ochrany – a ty právě popisuje kryptografie.

Kryptografie se začala rozvíjet nedlouho po steganografii. Její myšlenkou nebylo utajit existenci zprávy, jak tomu bylo u steganografie, ale utajit její obsah (*kryptos* – 'skrytý', *graphein* – 'psát', nebo-li 'psát skrytě'). To znamená, že i když se zpráva dostane do nepravých rukou, nedokáže její obsah nikdo přečíst, nezná-li správný klíč k jejímu rozluštění.

Na závěr poznamenejme, že výhody obou metod – steganografie a kryptografie – se dají navzájem zkombinovat: Zašifrování zprávy a její následné ukrytí jen zvyšuje šance, že bude bez odhalení doručena na místo určení. Kryptografii se budeme věnovat podrobněji v kapitole, která následuje.

Kapitola 2
Historie šifer

V této kapitole projdeme historií kryptografie od jejích počátků až po dnešní dny. Budeme si přitom všímat šifrovacích metod, kterých bylo v té které době používáno. Metody luštění jednotlivých šifer budeme uvádět jen u některých zajímavých případů.

2.1 Caesarova šifra

V době starověku při tajné komunikaci převažovala steganografie. Až později, z doby Julia Caesara, pochází první zdokumentované použití šifry v díle Zápisky o válce galské. Julius Caesar byl známý tím, že při posílání zpráv používal různé šifry. Jedna z jeho nejoblíbenějších dnes na jeho počest nese jeho jméno: Caesarova šifra. Jedná se o jednoduchý trik – každé písmeno abecedy nahradíme písmenem posunutým o tři místa doprava. Písmeno A se tak přepíše na D, B na E atd. a až dojdeme na konec šifrové abecedy, začneme znovu od písmene A – tedy X se přepíše na A, Y na B a Z na C. Obdrží-li adresát zprávu šifrovanou Caesarovou šifrou, stačí mu pouze písmenka zprávy posunout o tři pozice zpět (tedy doleva) a získá původní text.

Příklad 2.1:
Otevřená abeceda: `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`
Šifrová abeceda: `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`

Zašifrování textu '*veni, vidi, vici.*' Caesarovou šifrou.
Otevřený text: `v e n i,v i d i,v i c i.`
Šifrový text: `Y H Q L,Y L G L,Y L F L.`

2.2 Le chiffre indéchiffrable

„Nerozluštitelná šifra“, tak je dodnes titulována Vigenèrova šifra, ačkoliv její nerozluštitelnost prolomil v 19. století Charles Babbage. Byla nejspolehlivější šifrou po celý středověk, navržená tak, aby odolala novým důmyslnějším metodám prolomení šifer. V době před Vigenèrovou šifrou byla oblíbená šifrovací metoda, kterou dnes nazýváme **jednoduchá záměna**. Jedná se o nahrazení písmen abecedy jinými znaky nebo náhodnou záměnu písmen abecedy. Jednotlivá písmena tak mají pevně přidělený šifrovací znak. Ukázka jednoduché záměny je v příkladu 2.2.

Nejsilnějším nástrojem kryptoanalytiků v té době byla tzv. **frekvenční analýza**, která prolomila bezpečnost právě jednoduché záměny. Jedná se o metodu luštění zachycené zprávy, která využívá struktury daného jazyka – konkrétně toho, že každé písmeno abecedy se v textu vyskytuje různě často. Luštění probíhá tak, že se ke každému písmenu nebo znaku zprávy spočítá poměr výskytů znaku ku délce celé zprávy (délka je počet znaků zprávy). Výsledné číslo udává frekvenci znaku ve zprávě. Je-li zpráva *dostatečně dlouhá*, bude v šifrové zprávě zachycena frekvence písmen běžných textů v daném jazyce. Při luštění pak porovnáváme frekvence znaků použitých v šifrové zprávě s frekvencemi písmen jazyka, ve kterém předpokládáme, že je zpráva napsána.

Frekvence těchto písmen se dají snadno získat analýzou daného jazyka (novinových článků, literatury, dopisů atp.).

Pro ilustraci jsou frekvence několika jazyků uvedeny v dodatcích Tab. 8. Za povšimnutí stojí, že v českých textech se nejčastěji vyskytuje písmeno **e**, stejně jako je tomu v textech anglických.

Jak postupovat při kryptoanalýze pomocí frekvenční analýzy?
Prvním krokem je vytvoření tabulky frekvencí jednotlivých znaků zprávy. Máte-li informaci o tom, v jakém jazyce byla zpráva napsána – například angličtina, naleznete v tabulce tohoto jazyka znak s nejvyšší frekvencí a ve zprávě tento znak zkusíte nahradit nalezeným písmenem – v angličtině jde o písmeno E. Pokud znáte dobře daný jazyk – anglicky, nahrazením prvního písmene můžete rozeznat kontext dalších pasáží zprávy a budete tak schopni nahradit další znaky šifrové zprávy písmeny. Pokud ne, zkusíte použít další písmeno podle tabulky frekvencí. Tato metoda vyžaduje trpělivost a důvtip, ale dříve či později se dají rozpoznat některá slova a podle kontextu i ostatní zaměněné znaky. Podrobnější návod k luštění pomocí frekvenční analýzy uvádí Tůma v [7] nebo v uměleckém zpracování Poe v [4].

Metoda frekvenční analýzy byla známá v arabském světě již od 9. století, do Evropy se ale dostala až o několik století později. V 1. pol. 19. století ji pak proslavil americký spisovatel Edgar Alan Poe, který v povídce Zlatý brouk podrobně popsal postup, jak zprávu zašifrovanou pomocí jednoduché záměny rozluštit. Použil k tomu následující abecedu, která není kompletní, neboť se ve zprávě některé znaky nevyskytují:
Příklad 2.2:

Otevřená abeceda:	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
Šifrová abeceda:	5	2	-	†	8	1	3	4	9			0	6	*	‡	.		(	)	;		¶		:		

Zkuste rozeznat další kontext zprávy, dostanete-li z tabulky frekvenční analýzy, že E = 8 v následující zprávě:

```
5 3 ‡ ‡ † 3 0 5 ) ) 9 * ; 4 E 2 6 ) 4 ‡ . ) 4 ‡ ; E 0 9 *
; 4 E ‡ E ¶ 9 0 ) ) E 5 ; 1 - ( ; : * E - E 3 ( E E ) 5 *
‡ ; 4 9 ( ; E E * 9 6 * ? ; E ) * ‡ ( ; 4 E 5 ) ; 5 * † 2
: * ‡ ( ; 4 6 5 9 * 2 ( 5 * - 4 ) E ¶ E * ; 4 0 9 6 2 E 5
) ; ) 9 † E ) 4 ; 1 ( ‡ 6 ; 4 E 0 E 1 ; E : E ‡ 1 ; 4 E †
E 5 ; 4 ) 4 E 5 † 5 2 E E 0 9 * E 1 ( ‡ 6 ; 4 E ; ( E E ;
4 ( ‡ ? 3 4 ; 4 E ) 4 ‡ ; 1 9 1 ; : 1 E E ; ‡ ? ;
```

Rozluštěný text, Poe [4]:

> „A good glass in the bishop's hostel in the devil's seat forty-one degrees and thirteen minutes northeast and by north main branch seventh limb east side shoot from the left eye of the death's-head a bee line from the tree through the shot fifty feet out.“

Od chvíle, kdy i evropští kryptoanalytici ovládli techniku frekvenční analýzy, musel každý, kdo použil šifru založenou na jednoduché záměně, počítat s možností jejího rozluštění. Bylo tedy nutné hledat novou a účinnější metodu šifrování.

Základní myšlenku Vigenèrovy šifry položil v 60. letech 15. století Leon Battis Alberti, který zveřejnil esej na téma kryptografie po náhodném rozhovoru se svým přítelem Leonardem Datem. Navrhl použít dvě či více šifrových abeced, místo jedné a

zabránit tak rozluštění zprávy pomocí frekvenční analýzy. Přestože narazil v kryptografii na největší objev tisíciletí, dále svou myšlenku nerozvinul. Postupně na jeho esej navázali další badatelé – Johannes Trithemius na konci 15. století, Giovanni Porta v 16. století a nakonec francouzský diplomat Blaise de Vigenère, když si pro svou diplomatickou misi v Římě v roce 1549 prostudoval práce Albertiho, Trithemia a Porty. O dvanáct let později pak zveřejnil ucelený návrh šifry, která dnes nese jeho jméno. Síla této šifry spočívá v tom, že k zašifrování textu se místo jedné používá až 26 šifrových abeced.

Pro snazší šifrování a dešifrování je lepší vyrobit si pomůcku – šifrovací tabulku, které se říká Vigenèrův čtverec. Ukázka Vigenèrova čtverce je v dodatcích Tab. 9, zde uvedeme pouze příklad zašifrování otevřeného textu, který zní 'Vigenèrova šifra'. Před samotným zašifrováním je potřeba text ještě trochu upravit – odstranit interpunkční znaménka a mezery, protože nejsou součástí šifry a prozrazují strukturu textu, což by mohlo usnadnit její rozluštění.

Postup zašifrování zprávy.

Máme k dispozici Vigenèrův čtverec a text otevřené zprávy. Nejdříve je potřeba zvolit si heslo, které nám stanoví pořadí použitých šifrových abeced z Vigenèrova čtverce. Heslo nadepíšeme opakovaně nad písmena upravené otevřené zprávy a získáme dvojice: Písmeno hesla – písmeno zprávy. V tuto chvíli použijeme Vigenèrův čtverec. Z dvojice písmeno hesla – písmeno zprávy získáme šifrové písmeno tak, že ve čtverci nalezneme *řádek*, který začíná písmenem *hesla*, a poté *sloupec*, který začíná aktuálním písmenem *zprávy*. Získané písmeno, které nalezneme v průsečíku vybraného sloupce a řádku, je hledaným šifrovým písmenem. Ukažme si první kroky provedené v příkladu 2.3. Z klíče **HESLO** vezmeme znak **H**, z otevřeného textu **vigenerovasifra** vezmeme znak **v**. **H** se nachází na začátku 7. řádku, **v** na začátku 22. sloupce. V průsečíku 7. řádku a 22. sloupce je písmeno **C**, které je prvním znakem šifrové zprávy. V druhém kroku vezmeme z hesla **HESLO** písmeno **E** a ze zprávy **vigenerovasifra** písmeno **i**, písmenem **E** začíná 4. řádek, **i** 9. sloupec. Průsečíkem je písmeno **M**. V dalším kroku vezmeme z hesla **HESLO** písmeno **S**, ze zprávy **vigenerovasifra** písmeno **g** a z průsečíku dostáváme písmeno **Y**. Takto pokračujeme až do konce otevřené zprávy, přičemž heslo se opakuje tolikrát, kolikrát se vejde do délky otevřeného textu.

Příklad 2.3:

Heslo:		H E S L O
Klíč:	heslo upravené pro šifrování:	H E S L O H E S L O H E S L O
Otevřený text:	upravený pro zašifrování:	v i g e n e r o v a s i f r a
Šifrový text:		C M Y P B L Y G G O Z M X C O

Při dešifrování postupujeme obráceně. Máme šifrovou zprávu a heslo, které nám nějakým způsobem odesílatel předal. Opět použijeme Vigenèrův čtverec, ale nyní vezmeme první písmeno hesla **HESLO**, tedy **H**, nalezneme ve Vigenèrově čtverci řádek, který písmenem **H** začíná a v tomto řádku najdeme první písmeno šifrové zprávy **CMYPBLYGGOZMXCO** – tedy **C** – a podíváme se, v jakém sloupci toto písmeno je. Zjistíme, že je ve 22. sloupci, který začíná písmenem **v**. **V** je tedy prvním písmenem otevřené zprávy. Dále hledáme v řádku začínajícím písmenem **E** další písmeno šifrového textu – **M**. To leží v 9. sloupci, který začíná písmenem **i**. Máme tedy část otevřené zprávy **vi**. Takto pokračujeme až do konce šifrového textu a dostaneme zprávu **vigenerovasifra**, kterou doplníme diakritikou a dostaneme **Vigenèrova šifra**.

2.2.1 Knižní šifra

Knižní šifra byla používána především při špionáži, kde bylo důležité, aby se u špiona nenašly žádné pomůcky pro výzvědnou činnost. Tato jednoduchá metoda šifrování je speciální případ Vigenèrovy šifry s předem dohodnutým klíčem – knihou. Jako zdroj klíčů tedy sloužila domácí knihovna, ve které nechyběla kniha, na které byl špion domluven s příjemcem zpráv. Před posláním zprávy zašifroval otevřený text podle klíče – textu v knize, který začínal za písmenem, na kterém skončil při šifrování zprávy minulé. Šifrování může probíhat stejně jako u Vigenèrovy šifry s pomocí Vigenèrova čtverce nebo pomocí modulární aritmetiky, který nevyžaduje žádnou šifrovací pomůcku. Tento způsob je popsán níže.

V následujícím příkladu knižní šifry je jako klíč použit úvod povídky The Gold-bug od E. A. Poa: 'Many years ago I contracted an int...'. Začátek zprávy, kterou se snažil v této povídce přítel autora rozluštit, je zde otevřeným textem.

Příklad 2.4:

Klíč:	`M anyy earsa go Ico ntract e danint...`
Otevřený text:	`A good glass in the bishop's hostel...`
Šifrový text:	`M GBMB KLRKS OB BJS OBJHQI W KOFBRE...`

Na závěr uveďme způsob rozluštění knižní šifry.

Jednoduchost, s jakou se získá klíč, dává kryptoanalytikům do ruky nástroj, jak tuto šifru prolomit. Kniha totiž dává klíč, který má známou strukturu. Stačí tedy, aby kryptoanalytik vzal nějaké často používané slovo v daném jazyce (v češtině je to například slovo 'ale', v angličtině 'the') a zkusil jím – co by částí klíče – dešifrovat začátek šifrového textu. Dostane-li smysluplnou část otevřené zprávy, může odvodit další souvislosti. Vyjde-li mu nesmyslný text, posune se o písmeno zprávy dále a zkouší znovu dešifrovat. Takto vyzkouší všechny možné pozice umístění slova v textu klíče, kterým byla zpráva zašifrovaná, a protože vybral slovo, které se vyskytuje často, měl by získat část otevřeného textu.

Modulární aritmetika

Než si ukážeme další šifru, definujme si operace, které budeme dále používat při šifrování a dešifrování. Nejdříve budeme pracovat pouze s čísly, na kterých si ukážeme operace sčítání a odčítání v modulární aritmetice. Tyto operace pak budou odpovídat procesu šifrování a dešifrování. V modulární aritmetice máme dané kladné celé číslo p, které nazýváme modul. Tímto modulem upravujeme výsledky aritmetických operací. Sčítání a odčítání čísel x a y modulo p pak definujeme takto:

$$x + y = z \pmod{p},$$

$$x - y = x + (p - y) = w \pmod{p}, \tag{1}$$

kde x, y, z a w jsou celá čísla mezi 0 a $p - 1$. Čísla z a w spočítáme jako zbytky po celočíselném dělení čísel $(x + y)$ a $(x + (p - y))$ číslem p.

Modulární aritmetiku používáme každý den, aniž si to uvědomujeme. Stačí, aby nám někdo sdělil: „Vrátím se za pět hodin“ nebo „Jsem tu již deset hodin“. Tyto

časové údaje neznamenají nic jiného než počítání v modulární aritmetice s modulem 12, protože kdykoliv při udávání času překročíme poledne či půlnoc (12. hodinu), musíme naše počítání vynulovat. Uveďme si to na příkladu.

Příklad 2.5:

Sečteme a odečteme čísla 9 a 7 modulo 12.

$9 + 7 = 16$ v modulární aritmetice spočítáme zbytek po dělení čísla 16 číslem 12. $16 : 12 = 1$ *zbytek* 4, výsledkem $9 + 7 \pmod{12}$ je tedy číslo 4.

Píšeme $9 + 7 = 4 \pmod{12}$, což lze interpretovat pomocí časového údaje takto: Když v 9 hodin ráno sdělíme, že se vrátíme za 7 hodin, znamená to, že přijdeme ve 4 hodiny odpoledne.

Podobně pro rozdíl. $9 + (12 - 7) = 14$, zbytek po dělení čísla 14 číslem 12 je 2.

Píšeme tedy, že $9 - 7 = 2 \pmod{12}$.

Později budeme potřebovat také násobení a mocnění v modulární aritmetice $(\mathrm{mod}\ p)$.

$$x \cdot y = r \pmod{p},$$

$$x^y = s \pmod{p}. \tag{2}$$

Výsledky těchto operací musíme stejně jako u sčítání modulovat číslem p, tj. r a s spočítat jako zbytky po celočíselném dělení čísel $(x \cdot y)$ a (x^y) číslem p.

Nyní přibereme do hry písmena. Vezmeme-li mezinárodní abecedu o 26 písmenech a každé písmeno nahradíme číslem, které odpovídá jeho pořadí v abecedě začínající od 0, dostaneme převodní tabulku.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Posouvání písmene v abecedě doprava či doleva pak můžeme definovat pomocí modulární aritmetiky – operace sčítání a odčítání na písmenech abecedy jako součet či rozdíl čísel v této tabulce **modulo 26**.

Příklad 2.6:

Jaké písmeno dostaneme sečtením a odečtením písmena P a U?

Písmeno P odpovídá v tabulce číslu 15, písmeno U číslu 20. Z rovnice $15 + 20 = 9 \pmod{26}$ vidíme, že řešením je číslo 9, které podle tabulky odpovídá písmenu J. Stejný výsledek dostaneme, pokud písmeno P posuneme v abecedě o 20 místa *doprava* (přechodem z písmene Z na A).

Obdobně spočteme rozdíl: $15 - 20 = 15 + (26 - 20) = 21 \pmod{26}$, což podle tabulky dá písmeno V. Ke stejnému výsledku dospějeme, posuneme-li písmeno P o 20 míst *doleva*.

Právě předvedené operace se většinou zapisují pomocí písmen jako

$$\begin{aligned} \mathrm{P} + \mathrm{U} &= \mathrm{J}, \\ \mathrm{P} - \mathrm{U} &= \mathrm{V}, \end{aligned} \tag{3}$$

nyní již bez (mod 26), které na písmenech abecedy pokládáme za samozřejmé.

Při šifrování a dešifrování pak výše uvedeným způsobem zpracujeme celou zprávu, písmeno po písmenu. Mluvíme pak o sečtení a odečtení zprávy.

2.3 Vernamova šifra – konečně bezpečí?

V roce 1917 si dal Gilbert Vernam patentovat šifru založenou na výše popsaném principu, kdy se písmeno otevřeného textu sčítá (resp. odčítá) s písmenem klíče. Na první pohled by nám mohla připadat stejná jako šifra knižní, její síla však spočívá ve spojení těchto dvou podmínek:

1. *klíč* pro zašifrování zprávy *je jednorázový*,
2. klíč je *stejně dlouhý jako otevřený text* a skládá se z *náhodné posloupnosti písmen.*

Porušení jen jediné z těchto podmínek bezpečnost šifry radikálně snižuje. První bod – *jednorázové použití hesla*, anglicky *one-time-pad*, což je také známější název této šifrovací metody – nám zaručuje bezpečnost tím, že se klíč nebude opakovat v žádné další zprávě. V první fázi prolomení nové šifrovací metody se kryptoanalytici snaží odhalit zákonitosti či opakované sekvence v šifrovém textu nebo několika zprávách od stejného zdroje. Pokud by se odesílatel dopustil chyby a použil stejný klíč pro dvě zprávy, ztrácí Vernamova šifra svoji sílu a je jednoduchou záležitostí pro kryptoanalytiky. Tomu stačí dvě zprávy zašifrované stejným klíčem, aby převedl Vernamovu šifru na knižní. K podrobnostem se ještě vrátíme.

Náhodná posloupnost písmen v druhém bodě říká, že všechna písmena klíče jsou stejně pravděpodobná. To nám zaručuje, že výsledný šifrový text nebude obsahovat žádné zákonitosti jazyka, ve kterém byla otevřená zpráva napsána. Výsledný šifrový text tedy nenese žádnou informaci o původní zprávě.

Ačkoliv byl Vernam o bezpečnosti své metody přesvědčen, nebyl schopen její sílu matematicky ověřit. To se podařilo až o 30 let později C.E. Shannonovi. Ten dokázal, že text zašifrovaný Vernamovou šifrou není rozeznatelný od náhodné posloupnosti písmen.

Můžeme tedy konečně bezpečně komunikovat, aniž bychom se museli bát vyzrazení našeho soukromí? Odpověď zní ne, protože pro praktické použití Vernamovy šifry se nám do cesty kladou dva problémy: Jak sestavit náhodný klíč? Jak si jej bezpečně předat?

Použití Vernamovy šifry

Prvním úkolem je předání klíče, což musí proběhnout spolehlivým způsobem – nejlépe osobním setkáním příjemce a odesílatele zpráv. Jednu kopii klíče si ponechá příjemce, druhou předá odesílateli. Odesílatel po zašifrování zprávy klíč zničí, taktéž učiní příjemce po dešifrování zprávy. V případě prozrazení, jsou obě kopie klíčů zničeny.

Samotné šifrování zprávy pak probíhá následujícím postupem:

Zprávu před zašifrováním zbavíme interpunkčních znamének (případně i mezer) a dále ji i klíč budeme brát po jednotlivých písmenech a každou dvojici písmen sečteme.

Příklad 2.7:

Použití Vernamovy šifry.

Klíč:	U	M	Y	F	O	S	Q	R	A	H	J	J	Y	M	S	R	D	E	U	E	S
Klíč číselně:	20	12	24	5	14	18	16	17	0	7	9	9	24	12	18	17	3	4	20	4	18
Otevřený text:	p	r	i	k	l	a	d	v	e	r	n	a	m	o	v	y	s	i	f	r	y
Šifrový text:	J	D	G	P	Z	S	T	M	E	Y	W	J	K	A	N	P	V	M	Z	V	Q

Text zašifrovaný Vernamovou šifrou nenese žádnou informaci o původním textu. Pokud neznáme klíč, najdeme snadno k šifrovému textu další smysluplné zprávy, sestavené podle různých klíčů. Lze pak jen těžko rozhodnout, která z těchto zpráv je ta, kterou autor zašifroval, protože každá z nich má stejnou pravděpodobnost, že je správná. Následující ukázka je toho příkladem. Vidíme, že šifrový text je stejný jako v předchozím příkladu.

Příklad 2.8:

Stejná šifrová zpráva zašifrovaná jiným klíčem.

Klíč 2. zprávy:	R	K	C	G	M	O	U	M	M	Q	R	S	W	F	N	C	X	T	V	Y	X
Klíč číselně:	17	10	2	6	12	14	20	12	12	16	17	18	22	5	13	2	23	19	21	24	23
Otevřený text:	s	t	e	j	n	e	z	a	s	i	f	r	o	v	a	n	y	t	e	x	t
Šifrový text:	J	D	G	P	Z	S	T	M	E	Y	W	J	K	A	N	P	V	M	Z	V	Q

Vernam a knižní šifra

Jak lze převést Vernamovu šifru na knižní? Mějme dvě šifrové zprávy, A o znacích $a_1 a_2 \dots a_n$ a B o znacích $b_1 b_2 \dots b_n$, o kterých se domníváme, že jsou zašifrované Vernamovou šifrou se stejným klíčem. Jaký je vztah mezi těmito zprávami? Podívejme se, co lze říci o znacích a_i a b_i, pro $i = 1, \dots, n$.

Znak a_i šifrové zprávy musel být zašifrován i-tým znakem k_i klíče K. Stejně tak b_i musel být zašifrován týmž znakem k_i klíče K. Platí tedy, že $a_i = o_i^a + k_i$ a $b_i = o_i^b + k_i$ pro nějaké znaky otevřeného textu o_i^a a o_i^b. Když tedy od sebe a_i a b_i odečtu, dostanu, že $a_i - b_i = o_i^a + k_i - (o_i^b + k_i) = o_i^a - o_i^b$. Získáme tak typ knižní šifry, kdy máme jednu zprávu zašifrovanou pomocí druhé. Při luštění budeme postupovat stejně jako v případě knižní šifry s tím rozdílem, že zde musíme zvolené slovo přičítat.

Ačkoliv byla metoda one-time-pad známá již ve 20. letech 20. století, nebyla příliš používána právě kvůli problémům se sestavením náhodného klíče. Používala se tak pouze ve vysokých diplomatických kruzích, kde byla bezpečná komunikace nade vše. Stala se však výzvou pro dnešní dny, neboť její používání může být snadné, najde-li se způsob generování náhodných posloupností znaků a snadný způsob předání klíče.

2.4 Moderní metody šifrování

Moderní metody šifrování jsou svázány s vývojem počítačů. Počítač pracuje na nejnižší úrovni s elektrickými impulsy, které se interpretují jako 1 – prochází proud, 0 – neprochází proud. Všechno, co chceme zpracovat pomocí počítače, musíme tedy dokázat převést na posloupnosti 0 a 1. Mluvíme o binárním kódování, které si nyní vysvětlíme.

2.4.1 Binární kódování

Binární kód je číslo v dvojkové (binární) soustavě, ve které je každé číslo vyjádřeno posloupností 0 a 1. Jedné číslici binárního kódu říkáme **bit** – z anglického **bi***nary digi***t**, 'dvojková číslice', který je zároveň základní jednotkou informace. Další jednotkou je **byte**, pro který platí vztah: 1byte = 8 bitů. Velikost zadaných dat potom definujeme jako počet bitů, do kterých lze tato data uložit, přičemž data mohou dosahovat velikosti stovek, tisíců, miliónů bytů. Odvozujeme tak další jednotky: kilobyte (2^{10} bytů), megabyte (2^{20}), giga– (2^{30}), tera– (2^{40}), ...

Nejdříve si ukažme převod čísel z naší běžné, tedy desítkové, soustavy do binární. Pro převod používáme následující algoritmus: Zadané číslo, které chceme převést na číslo binární, rozložíme na součet mocnin čísla 2, včetně $2^0 = 1$. Součet doplníme 0-násobky mocnin dvojky, které v tomto součtu chybí. Binární tvar zadaného čísla pak odpovídá násobkům mocnin čísla 2, napsaných za sebe od nejvyšší mocniny.

Příklad 2.9:

Převeďme číslo 121 do binární soustavy.

$$\begin{aligned} 121_{10} &= 64 + 32 + 16 + 8 + 1 \\ &= 2^6 + 2^5 + 2^4 + 2^3 + 2^0 \\ &= 1 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 \\ &= 1111001_{\mathrm{B}} \end{aligned}$$

Dovedeme-li převést čísla na sekvenci 0 a 1, není problém zavést kódy reprezentující znaky. Tak vznikla tabulka znaků zobrazitelných na počítači a představuje příklad toho, jak je lze kódovat do binární soustavy. Byla přijatá jako mezinárodní standard pod názvem ASCII tabulka (American Standard Code for Information Interchange table). Kódem znaku je pořadové číslo v této tabulce, převedené do dvojkové soustavy a zarovnané má pevnou délku 1 byte. Znaky základní ASCII tabulky jsou tvořeny 128 mezinárodně používanými znaky. Uvedeny jsou v dodatcích Tab. 10. Zbylých 128 volných kódů je vyhrazeno pro národní znaky a tvoří tak prostor pro různé znakové sady.

Příklad 2.10:

Uveďme si příklad převodu písmena 'A' z ASCII tabulky na binární kód. 'A' je v ASCII tabulce na 65. místě, jeho binárním kódem bude tedy číslo 65 v binární soustavě uložené do 1 bytu: $65_{10} = 01000001_{\mathrm{B}}$. Podobně lze převést i ostatní znaky.

Za zmínku stojí zajímavá vlastnost Vernamovy šifry a to, že bude beze změn fungovat nad jakoukoliv množinou znaků, tedy i pro 0 a 1. Posun písmen ve dvouznakové

abecedě je možný pouze o 1 místo nebo žádné, klíčem je tedy posloupnost 0 a 1. Každý bit klíče odpovídá jednomu bitu zprávy a říká, zda se tento bit má při šifrování změnit či zůstat nezměněný. Operace sloučení dvou bitů se jmenuje XOR. V následující tabulce jsou uvedeny základní výsledky operace XOR.

x	y	x XOR y	$(x$ XOR $y)$ XOR $y = x$
0	0	0	0
0	1	1	0
1	0	1	1
1	1	0	1

Příklad 2.11:

Na závěr uveďme příklad zašifrování zprávy pomocí Vernamovy šifry nad binární abecedou:

Otevřený text:	`Hello`	`Bob.`			
Otevřený text v ASCII	`01001000`	`01100101`	`01101100`	`01101100`	`01101111`
převedený na bin. kód:	`00100000`	`01000010`	`01101111`	`01100010`	`00101110`
Klíč:	`00100100`	`01000000`	`01001000`	`01000110`	`01000000`
	`01101011`	`00001101`	`00000111`	`01000001`	`00001100`
	`01101100`	`00100101`	`00100100`	`00101010`	`00101111`
	`01001011`	`01001111`	`01101000`	`00100011`	`00100010`
Šifrový text v ASCII:	`l % $ *`	`/ K O h`	`# "`		

2.4.2 Strojové šifrování, šifrování a počítače

Již od 15. století byly k šifrování používány různé šifrovací pomůcky – šifrovací desky, které mohou být považovány za předchůdce šifrovacích strojů. Dvacáté století bylo století velkého technického pokroku. Snaha obstarat co nejvíce práce pomocí strojů vedla také k mechanizaci šifrování. Použití strojů nejen zrychlilo proces šifrování zpráv, ale také umožnilo vzniknout novým šifrovacím systémům, které se opíraly o hranice technických možností své doby. Nejčastějším způsobem zpracování zprávy je písmeno po písmenu, tak jak tomu bylo při ručním šifrování.

Enigma

Nejznámějším strojem pro šifrování zpráv je Enigma. Německý vynálezce Arthur Schrebius si její první verzi nechal patentovat v roce 1918, ale teprve v roce 1927 se dostala do povědomí kryptoanalytiků, kteří zjistili, že nejsou schopni rozluštit německé depeše.

Šifrování zprávy pomocí Enigmy probíhalo tak, že stisknutí písmene z otevřené zprávy vyslalo elektrický impuls, který prošel šifrovacím mechanismem stroje a rozsvítil žárovku odpovídající šifrovému písmenu. Šifrovací jádro stroje se dá rozdělit na tři základních části:

1. *Klávesnici*, na kterou se vyťukává vstup po jednotlivých znacích a indukuje tak elektrický impuls, který postupuje dále,

2. *šifrovací jednotku*, ze které vyjde šifrovací písmeno na výstup,

3. *signální desku*, která obsahuje žárovky s písmeny abecedy. Rozsvítí se vždy jen jedna, která odpovídá výstupnímu šifrovému písmenu ze zadaného či naopak.

Šifrovací jednotka je základem celého systému Enigma. Skládá se z rotoru – otočného kotouče, do kterého vstupuje 26 vodičů vedoucích přímo z klávesnice, a ze kterého opět 26 vodičů vystupuje. Uvnitř rotoru se vodiče různě otáčejí a přehýbají. Vnitřní zapojení rotoru je neměnné a určuje, jak budou jednotlivá písmena zprávy zašifrována.

Zpracovaný signál, vystupující z prvního rotoru pokračuje do dalšího, celkem signál prochází třemi. Sílou Enigmy bylo to, jak spolu rotory pracovaly dohromady. Pokaždé, když impuls přešel od prvního rotoru k druhému, pootočil se o jedno písmeno, takže stejný znak, který by přišel ze vstupu, by se zašifroval jinak. Druhý rotor se pootočil o jedno písmeno až tehdy, když první dokončil celou jednu otáčku (přes 26 písmen) a třetí až při dokončení otáčky rotoru druhého. Zde je vidět, že Enigma může zašifrovat stejně tentýž znak, ale k zopakování dojde až po 26 otáčkách na třetím rotoru – tedy po 17 576 zadaných písmenech.

Pro zvýšení bezpečnosti později Schrebius přidal do Enigmy další část – *propojovací desku*, která promíchala vstupní písmena. Jednalo se o jednoduché prohození písmen pomocí přehození drátů vedoucích z klávesnice, například A za X, B za D (a tím i X za A a D za B).

Další verze Enigmy pak umožňovala měnit pořadí rotorů, jejichž vnitřní zapojení bylo odlišné a tím zvýšit počet možných nastavení stroje. V kombinaci s ostatními částmi šifrovací jednotky se tak tento počet blížil číslu 10^{15}.

Poslední část tvořil *reflektor*, který výstupní signál z třetího rotoru neposílal rovnou na signální desku, ale zpět přes rotory a teprve potom na signální desku. Na první pohled by se tato část mohla jevit zbytečná, ale svou roli hrála především při dešifrování zprávy, které probíhalo opět pomocí Enigmy. Pokud do ní napíšete šifrový text, dostanete text otevřený a to právě díky reflektoru. Reflektor je tak jakýmsi zrcadlem šifrového a otevřeného textu. Postup měl jen jediný háček – počáteční nastavení rotorů. Před šifrováním zprávy bylo potřeba nastavit každý z rotorů do počáteční polohy (ne nutně AAA), která tvořila klíč k dešifrování. Příjemce, který zprávu obdržel, musel nejdříve nastavit rotory do stejné polohy jako odesílatel před zahájením šifrování. Jinak by musel vyzkoušet všechna možná nastavení, kterých je tolik, co možných pootočení rotorů – tedy 17 576. Po přidání propojovací desky se součástí klíče stalo i propojení desky a v další verzi pak i pořadí rotorů.

Princip šifrování Enigmou spočívá v tom, že každé písmeno se posune o jiný počet pozic. Měla však jednu slabinu: způsob, jakým byla používána. Toho si všiml mladý polský matematik Marian Rejewski a těsně před tím, než bylo Polsko obsazeno nacisty, stihl předat své výsledky Francouzům a Britům. Na jeho práci pak navázal Alan Turing a navrhl „dešifrovací stroj“ na rutinní práci při hledání správného nastavení, s jehož pomocí byly zprávy šifrované Enigmou rozluštěny. Podrobnosti o prolomení Enigmy naleznete například v Singhově knize [6].

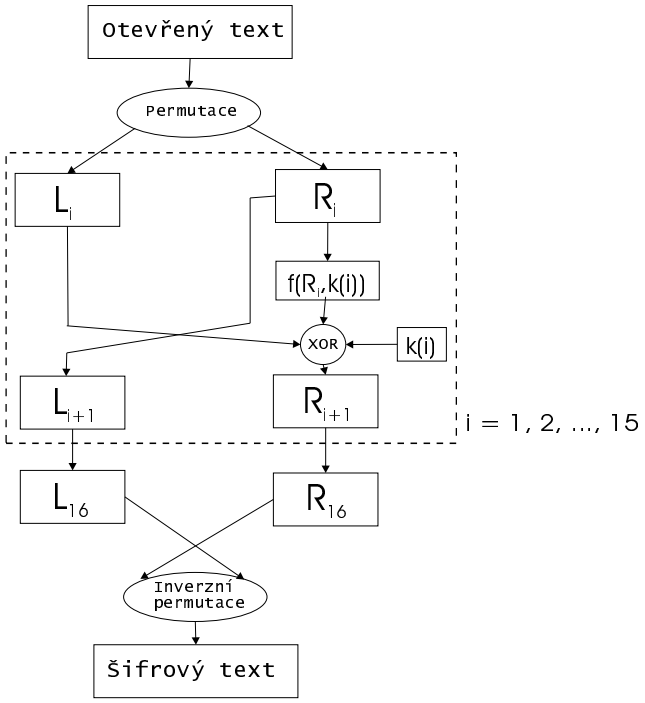
Ze způsobu vnitřního zapojení Schrebius odvodil, že stroj má 17 576 různých nastavení, které by bylo potřeba vyzkoušet, aby mohla být zachycená zpráva rozluštěna. V době, kdy Enigmu sestavil to bylo více než spolehlivé zařízení pro utajení zpráv. Nee-

xistoval žádný stroj, který by byl schopen v rozumném čase prověřit všechna nastavení Enigmy a jednomu člověku by vyzkoušení všech možností zabralo asi dva týdny. V bezpečnější verzi Enigmy s propojovací deskou se pak počet možných nastavení Enigmy zvýšil na přibližně 10^{15}. Chybný předpoklad na technické možnosti jiných států tak nechalo Německo v poklidu, že jejich zprávy jsou dostatečně chráněné.

DES

Po druhé světové válce došlo k rozvoji počítačové techniky. V 60. letech pak výkon počítačů a cena byly natolik příznivé, že je bylo možné využívat i v komerční sféře. Kryptografové tak byli postaveni před nový problém: chránit informace jednotlivých korporací, ale přitom najít způsob, jak si mohou navzájem informace předat. Jinými slovy, najít standardní šifrovací systém, který by mohli používat všichni. Americký standardizační úřad National Bureau for Standards (NBS) tak 15. května 1973 vyhlásil projekt na nalezení standardního šifrovacího systém nazvaného DES (Data Encryption Standard), jehož vítězem se stal šifrovací systém **Lucifer**.

Lucifer od autora německého původu Horsta Feistlera je počítačová šifra, která zpracovává otevřený text (binárně kódovaný) po blocích o velikosti 128 bitů. Tedy ne znak po znaku, jak tomu bylo u jiných šifer. Každý blok se šifruje samostatně tak, že je rozdělen na levou a pravou polovinu o 64 bitech a dále prochází procesem „mandlování“, při kterém je pravá část bloku spolu s vygenerovaným klíčem navzájem promíchána a potom XORována s levou částí bloku. Výstupní blok se stává novým pravým blokem, původní pravý se stává novým levým blokem a původní pravý blok se zahodí. Této fázi se říká runda (nebo také kolo), každý blok projde celkem 16 rundami. Po poslední rundě ještě dojde k výměně levého a pravého bloku. Pro lepší ilustraci je tento průběh znázorněn na obrázku Obr. 1.



Obr. 1: Průběh zpracování jednoho bloku textu šifrou DES.

Funkce, podle které probíhá proces zamíchání, se nazývá **rundovní funkce** a na jejím vstupu kromě bloku otevřeného textu musí být i klíč. Před vlastním procesem mandlování a hned po něm jsou na text aplikovány permutace bitů kvůli tzv. zašumění textu. Permutace jsou pevně zadané a navzájem inverzní.

Jedna runda šifrování se pak dá popsat vzorcem:

$$(\mathrm{L}_{i+1}, \mathrm{R}_{i+1}) = (\mathrm{R}_i, f(\mathrm{R}_i, k(i) \text{ XOR } \mathrm{L}_i), \tag{4}$$

kde (L_i,R_i) jsou šifrované bloky v i-tém kroku „mandlování“, $i = 1, \ldots, 16$, *k(i)* rundovní klíč v i-tém kroku vygenerovaný ze zadaného klíče a f rundovní funkce.

DES je nejpoužívanějším šifrovacím systémem na světě, avšak od doby svého vzniku povážlivě vzrostla výkonnost počítačů. Kritici poukazovali na zastaralost tohoto systému a když v letech 1998–1999 proběhlo několik luštících akcí nazvaných DES-Cracker, které dokázali, že DES je prolomitelná použitím hrubé síly – tj. vyzkoušením všech možností, pokud se spojí větší množství počítačů přes Internet a rozdělí si úkoly, nastal čas na změnu. NBS se tuto situaci snažila zachránit zavedením nového standardu TripleDES, což bylo původní DES s prodloužením klíče na trojnásobek – z původních 56 na 112 nebo 168 bitů. Nakonec však vyhlásila nové řízení na standardní šifru AES (Advanced Encryption Standard), kterou v roce 2002 vyhráli belgičtí kryptologové Joan Daemen a Vincent Rijmen se svou šifrou **Rijndael**. V současnosti je DES nahrazen AES a může být používán jen na dobíhajících systémech.

2.4.3 Problém distribuce klíče

V novodobé kryptografii se vyvinuly nejen nové metody šifrování, ale také příklad, na kterém se nejčastěji demonstruje princip nové metody. Říká se mu s trochou nadsázky ‘příběh Alice a Boba’: Mějme dvě strany, které si chtějí vyměnit tajnou informaci, ale potřebují k tomu klíč, aby mohly posílanou zprávu bezpečně zašifrovat. Odesílatele označme jako A a příjemce jako B. Abychom se k nim zachovali lidštěji, říkáme jim Alice a Bob. Stejně tak určíme „odposlouchávače“ (anglicky *eavesdropper*) Evu, která chce jejich komunikaci zachytit a rozluštit. V následujícím textu bude popsáno několik příběhů této trojice.

Do této chvíle jsme představili pouze šifry, které k šifrování a dešifrování potřebují stejný klíč. Mají-li adresát i příjemce použít stejný klíč, musí se nejdříve na něm nějak dohodnout. Buď se sejít nebo se spolehnout na diskrétnost třetí strany, která klíč od jednoho k druhému dopraví. Nejinak tomu bylo i ve dvacátém století, při používání šifry DES. Problém distribuce klíče tak trápil kryptografy po celá staletí a platilo dogma, že problém distribuce klíče je neoddělitelnou součástí kryptografie.

Symetrické šifrování – jednosměrné funkce

Diffie–Hellman–Merkle v roce 1976 představili svoji ideu, jak se vyhnout distribuci klíče. Představme si, že Alice chce poslat zprávu Bobovi. Aby zprávu nepřečetl nikdo jiný, zamkne ji do skříňky, klíč si ponechá a odešle skříňku Bobovi. Bob vezme skříňku, přidá na ni druhý zámek – svůj a odešle ji zpět Alici. Alice obdrží skříňku opatřenou dvěma zámky – svým a Bobovým. Nyní může svůj zámek sejmout a zpráva zůstane stále

bezpečně uzamčena. Odešle skříňku zpět Bobovi, který má zprávu chráněnou pouze vlastním zámkem, takže nemá problém skříňku otevřít a získat tak zprávu od Alice. Tato myšlenka je velmi jednoduchá a elegantně řeší problém distribuce klíče. Problém ale je, jak tuto analogii převést do kryptografie, resp. do počítačové kryptografie.

Tým Diffie–Hellman–Merkle se snažil nalézt matematický aparát, který by měl tyto vlastnosti. Při svém hledání se jeho členové zaměřili na tzv. **jednosměrné funkce**. Jednosměrné funkce jsou takové, které lze snadno použít jedním směrem, tj. k zadanému číslu x najít y odpovídající rovnici $f(x) = y$, ale je těžké k zadanému y najít číslo x tak, aby $y = f(x)$, neboli mít k dispozici inverzní funkci f^{-1}, pro kterou platí $f^{-1}(y) = x$. Jak těžká je tato matematická úloha si lze představit na příkladu ze života – smíchání barev. Smíchat dvě barvy, které máme k dispozici, je snadné – dostaneme tak barvu novou. Máme-li však jen tuto novou barvu je velmi těžké zjistit, z jakých barev a v jakém poměru byla namíchána.

Charakteristice jednosměrných funkcí v matematice nejlépe odpovídá modulární aritmetika, která se za jistých podmínek může tak chovat. Hledání zabralo této trojici dva roky, ale nakonec se podařilo takovou funkci, která splňuje požadavky symetrické šifry:

$$f(x) = y^x \pmod{p}, y < p, p \text{ jeprvočíslo.} \tag{5}$$

Jakým způsobem se Alice a Bob domluví na klíči?

Alice s Bobem si zavolají a domluví se na dvou číslech – čísle y a čísle p. Každý si pak zvolí jedno číslo – Alice zvolí číslo A, Bob zvolí číslo B. Každý zvlášť spočte rovnici $y^x \pmod{P}$, kde za x dosadí Alice číslo A a Bob číslo B. Výsledky a a b z této rovnice si opět sdělí veřejným kanálem. Nyní Bob vezme Alicin výsledek a a dosadí ho znovu do své rovnice $a^{\mathrm{B}} \pmod{p}$, taktéž učiní Alice s Bobovým výsledkem b, $b^{\mathrm{A}} \pmod{p}$. Po provedení této operace získají klíč, který vyjde oběma stejně a který znají jen oni. Přitom Alice neví, jaké číslo původně zvolil Bob a taktéž Bob neví, s jakým číslem začala počítat Alice. Po nalezení klíče již mohou zašifrovat připravenou zprávu a poslat druhému. Pro názornost si ukažme výměnu klíče na příkladu.

Fáze 1

Alice se s Bobem domluví na prvočíslu a číslu, přes které budou počítat v modulární aritmetice. Zvolí si 13 jako p a číslo 11 jako y.

Fáze 2

Alice zvolí číslo A = 5. Bob zvolí číslo B = 3.

Fáze 3

Alice vloží do jednosměrné funkce číslo A – tj. 5 a z rovnice $11^5 \pmod{13}$ dostane výsledek 7. Stejně tak učiní Bob a z rovnice $11^3 \pmod{13}$ dostane číslo 5.

Fáze 4

Alice pošle výsledek $a = 7$ Bobovi a ten ji pošle svůj výsledek $b = 5$.

Fáze 5

Alice z Bobova čísla b spočítá klíč: $5^5 \pmod{13}$ a dostane klíč 5. Stejně tak Bob po spočtení $7^3 \pmod{13}$ dostane klíč 5.

Pokud Alice s Bobem zvolí na počátku dostatečně velká čísla p, y a A, B, má Eva malou naději zjistit, jaký klíč Alice s Bobem dostali. Jedinou její šancí je vyzkoušet všechna řešení rovnice, k čemuž ale při dostatečně velkých A, B nedojde v rozumném čase.

Na svět tak přišlo symetrické šifrování bez potřeby distribuce klíče. Mělo jen jednu nevýhodu: k zašifrování zprávy se musí obě strany – Alice a Bob – spojit ve stejnou dobu a domluvit se na klíči. Tento způsob ale odporuje nesymetrické komunikaci jakou je například e-mail. Bylo by totiž velice nepohodlné, kdyby Alice před odesláním každého emailu nejdříve volala Bobovi a domlouvala se s ním na klíči. Kryptografii tak čekal ještě další krok kupředu – asymetrické šifrování.

Asymetrické šifrování

Myšlenka asymetrického šifrování byla naprosto revoluční v uvažování kryptografů. S původní myšlenkou přišel Diffie, když si představil, že by bylo výhodné najít metodu šifrování, pro kterou by neexistoval pouze jeden klíč na šifrování a dešifrování, ale dva. Jeden, kterým by byla zpráva zašifrována, ale nešla by pomocí něj rozšifrovat, a druhý k dešifrování. Pak by totiž bylo možné, aby každý člověk měl jeden tajný klíč, tzv. **soukromý klíč**, kterým by dešifroval zprávy a znal by ho jen on sám, ale každému by mohl dát k dispozici druhý, tzv. **veřejný klíč**, pomocí kterého by mohli lidé šifrovat zprávy určené jemu.

Analogicky si tuto situaci můžeme představit znovu na zámcích a skříňce. Alice má zámek a k němu klíč. Tento zámek je však speciální – k jeho uzamčení není potřeba klíče, ale stačí ho jen zaklapnout. Klíč si Alice schová a k zámku nechá vyrobit velké množství kopií. Tyto kopie nechá rozeslat všude možně po světě. Každý, kdo potom bude chtít Alici poslat tajnou zprávu, schová ji do schránky, vyzvedne si jeden Alicin zámek a zaklapne ho. Od této chvíle je Alice jediným člověkem, který může zprávu ze skříňky získat.

S touto myšlenkou asymetrického šifrování přišel tým Diffie–Hellmann–Merkle asi v polovině 80. let. Nepodařilo se jim však najít žádný vhodný matematický nástroj, pomocí kterého by mohli realizovat myšlenku veřejného klíče. Objev první asymetrické šifry si tak připsali kryptografové Ronald Rivest, Adi Shamir a Leonard Adleman, jejichž počáteční písmena příjmení dala vzniknout názvu dnes nejznámější asymetrické šifry RSA.

RSA

Základem RSA je opět jednosměrná funkce, která vhodně využívá modulární aritmetiku. Zprávu je potřeba zakódovat do čísla, které je vloženo do šifrovací funkce. Tato funkce je tak speciální, že jde za určitých podmínek invertovat.

Fáze 1

Alice zvolí dvě dostatečně velká prvočísla, označí je p a q. Tato dvě čísla musí uchovat v tajnosti.

Fáze 2

Alice vynásobí obě prvočísla a součin nazve N. Dále zvolí číslo e, které musí spl-

ňovat nerovnost $1 < e < (p-1) \times (q-1)$ a navíc nesmí být soudělné s číslem $(p-1) \times (q-1)$. N spolu s e tvoří Alicin veřejný klíč, který Alice zveřejní na různých místech (svých webových stránkách, na úřadech atp.).

Fáze 3

Bob, který chce Alici poslat tajnou zprávu, si vyzvedne její veřejný klíč – (N, e), zprávu zakóduje do čísla M a zašifruje podle vzorce $M^e \pmod N$. Výsledek této operace je zašifrovaná zpráva C, kterou pošle Alici.

Fáze 4

Alice obdrží zprávu C. Pro její dešifrování si musí nejdříve dopočítat svůj soukromý klíč d. Ten získá tak, že d vypočítá z rovnice

$$e \times d = 1 \pmod{(p-1) \times (q-1)}, \tag{6}$$

a pomocí d dešifruje zprávu

$$C^d \pmod N, \tag{7}$$

čímž dostane znovu zprávu M.

Z postupu je zřejmé, že slabinou šifry je možnost rozkladu čísla N na součin prvočísel p a q. Rozklad čísla N na prvočinitele se nazývá **problém faktorizace** a je jedním z dalších problémů, pro které v tuto chvíli neznáme rychlý algoritmus, který by je řešil. Pokud jsou však p a q zvolena dostatečně velká, není na světě v tuto chvíli žádná technika, která by dokázala v rozumném čase najít k zadanému N čísla p a q.

Firma RSA Security vyhlásila na svých stránkách soutěž o nalezení faktorizace čísla N, které má délku 128, 256 atd. bitů. Nejnovější faktorizace nalezená v listopadu 2005 je na klíč N o délce 640 bitů a spolupracovalo na ní 30 počítačů s výkonem procesorů 2,2 GHz. Odhaduje se, že pro dnešní dny je dostatečně bezpečný klíč o délce 2048 bitů (což odpovídá prvočíslům p a q řádu přibližně 10^{300}). Podrobnosti jsou na stránce RSA Security [8].

V roce 1997 byla patentována šifra multi-prime RSA, která v RSA využívá k výpočtu čísla N součin více než dvou prvočísel. To ale nemusí bezpečnost šifry zvýšit, neboť nevhodnou volbou většího počtu prvočísel můžeme snížit jejich řád a tím zjednodušit faktorizaci.

PGP

Pretty Good Privacy – 'docela dobré soukromí', takto pojmenoval Phil Zimmermann svůj projekt, který by mohl nést podtitul „Soukromí pro každého". Nechtěl se totiž smířit s tím, že síla šifry RSA bude dostupná pouze vládám a bohatým organizacím, které budou mít dostatek peněz a techniky na její používání. Zimmermann se proto snažil vytvořit levný a výkonný produkt, který by byl použitelný na každém osobním počítači a navíc ho mohl ovládat každý – nejen expert na kryptografii. Výsledkem jeho práce byl balíček šifrovacího software, který zveřejnil koncem 80. let 20. století.

Jeho cílem bylo zrychlit proces šifrování, aby bylo realizovatelné i na pomalých domácích počítačích. Symetrické šifrování je oproti asymetrickému rychlejší, ale je nutné „bezpečně distribuovat klíč". Asymetrická naopak nepotřebuje klíč distribuovat, ale

proces šifrování je pomalejší. Zimmermanna napadlo zkombinovat tyto dvě šifrovací metody a celý proces šifrování tak zrychlit. Problém předání klíče pro symetrickou šifru, jíž bude zašifrována zpráva, vyřeší pomocí asymetrické šifry, kterou zašifruje klíč. Klíč pro symetrickou šifru typu DES je totiž mnohem kratší než celá zpráva a její zašifrování proběhne rychleji, než kdybychom asymetrickou šifrou zpracovávali celou zprávu.

Fáze 1

Alice zašifruje zprávu symetrickou šifrou. K tomu musí zvolit klíč, který potřebuje předat Bobovi, aby mohl zprávu dešifrovat.

Fáze 2

Alice vyhledá Bobův veřejný klíč pro RSA, kterým zašifruje klíč symetrické šifry.

Fáze 3

Alice Bobovi pošle dvě zašifrované zprávy:

- klíč ke zprávě zašifrovaný Bobovým veřejným klíčem pro RSA,
- zprávu zašifrovanou symetrickou šifrou a klíčem, který Alice zvolila a poslala Bobovi.

Fáze 4

Bob nejdříve svým soukromým klíčem pro RSA dešifruje klíč zprávy a poté i samotnou zprávu, kterou mu Alice poslala.

Když Zimmermann vyřešil problém předání klíče pro symetrickou šifru, obohatil program o další uživatelsky příjemné aplikace: generátor klíčů pro asymetrickou šifru, který po uživateli nechce nic jiného, než lehce pohnout myší. Tím se přidá do generovaného klíče náhodný prvek. Další výbavou PGP je možnost aplikace digitálního podpisu.

Od léta 1991 Phil Zimmermann poskytl svůj produkt volně ke stažení na Internetu. Byl si sice vědom, že jádro jeho systému – RSA – je chráněno patentovým zákonem a k jeho použití potřebuje licenci od RSA Data Security. Velmi mu ale záleželo, aby se PGP dostalo co nejdříve na veřejnost a tak se rozhodl tento problém ignorovat. PGP se zatím stalo velmi populární a počet stažení den ode dne rostl. V roce 1993 se Zimmermann dočkal obvinění, ale úplně jiného než čekal: Z nelegálního exportu zbraní, za který je šifrovací software považován. Ačkoliv byla žaloba v roce 1996 stažena, otevřela tato aféra diskuzi, která se řeší dodnes a bude se řešit i v budoucnu: Kde je hranice mezi ochranou svého vlastního soukromí a ochranou zločinců, kteří mohou stejnými prostředky docílit bezpečné komunikace pro nelegální činnost.

2.4.4 Kvantová kryptografie

Kvantová kryptografie je nejnovějším objevem kryptografie. Opírá se o přírodní zákony popsané kvantovou fyzikou, která je považována za skvělý zdroj náhodných jevů. A protože vše, co se jeví jako náhodné, je v kryptografii pokládáno za bezpečné, stala se kvantová kryptografie skvělým objektem pro zkoumání a hledání nových metod šifrování. Od 80. let 20. století byly popsány dva postupy získání náhodného klíče pro Vernamovu šifru pomocí kvantových jevů. První se nazývá BB84 a druhý Ekertovo schéma.

Kvantová kryptografie se opírá o dva základní pilíře kvantové mechaniky a to:

1. *Jevy v kvantové mechanice jsou dokonale náhodné.*

   Díky tomu máme možnost získat náhodný klíč.

2. *Měřením na kvantovém systému nutně způsobíme změnu tohoto systému.*

   Nelze si tedy posílaný signál zkopírovat bez toho, aby se tento úkon projevil v systému při dalším měření.

V kvantové kryptografii se ve finále šifruje otevřená zpráva Vernamovou šifrou. K tomu, aby se mohla zašifrovat, je však potřeba náhodný klíč. Právě k jeho vytvoření a předání se používá kvantový kanál. Nyní již víme, že nám jako klíč zprávy postačí sekvence 0 a 1, pomocí kterých umíme reprezentovat znaky abecedy. Dále se tedy budeme zabývat procesem předání 0 a 1.

Pro posílání signálu složeného z 0 a 1 se v kvantové kryptografii používají částice elektromagnetického záření – fotony. Fotony představují vlnění, které kmitá ve všech směrech kolmých na směr letu fotonu. Dnešní technologie ale dokáží kmity fotonů usměrnit a to například pomocí polarizačních filtrů. Hovoříme o polarizaci fotonů, což je jev, kdy fotony kmitají pouze v jedné rovině (například směrem nahoru a dolů). Fotony kmitající ve stejné rovině dané polarizačním filtrem projdou, fotony kolmé neprojdou a pokud se ostatním podaří projít, tak jen za cenu toho, že se usměrní do roviny polarizačního filtru. Rovin polarizace může být nekonečně mnoho, nám však postačí jen několik z nich.

Vezměme nyní do úvahy 4 roviny polarizace – ve směrech — | / \, dvě budou představovat 1, dvě 0. Dvojice polarizací, které jsou navzájem kolmé tvoří schéma polarizace. Dostáváme tak dvě schémata + (plus-schéma) a × (x-schéma). Rozvržení bitů ukazuje následující tabulka.

rovina polarizace	hodnota bitu	schéma polarizace
—	0	+
|	1	+
/	0	×
\	1	×

Při měření v plus-schématu můžeme dostat jako výsledek foton kmitající v rovině —, který podle tabulky reprezentuje poslanou 0, nebo |, který reprezentuje 1. Při měření v x-schématu, dostaneme výsledek / (představuje 0) nebo \ (představuje 1). Z kvantové

mechaniky plyne, že pokud zvolíme správné schéma, bude výsledek měření odpovídat polarizaci fotonu. Zvolíme-li však nesprávné schéma, dostaneme jeden z možných výsledků (0 nebo 1) zcela náhodně s pravděpodobností 1/2. Polarizace fotonu se přitom zákonitě změní na tu, která byla výsledkem měření, takže není možno měřit v obou bázích současně a získat tak plnou informaci o stavu fotonu.

BB84

Charles Bennett a Gilles Brassard v roce 1984 popsali kryptografický protokol pro výměnu klíče postavený na kvantové mechanice. Jméno dostal podle počátečních písmen svých autorů a roku zveřejnění. Protokol BB84 řeší problém bezpečné výměny klíče bez setkání komunikujících stran či použití spolehlivého prostředníka. Ve chvíli, kdy mají obě strany k dispozici náhodný klíč odpovídající délce zprávy, aplikují algoritmus Vernamovy šifry.

Jak BB84 pracuje?

Vytvoření náhodného klíče probíhá v několika fázích a je k němu potřeba dvou komunikačních kanálů – kvantového, který zaručí dokonalé bezpečí a běžného, nechráněného, po kterém může projít zašifrovaná zpráva a další informace.

Fáze 1

Alice začne vysílat náhodné sekvence bitů (tj. 1 a 0), přičemž náhodně střídá schémata polarizace fotonů. Tato sekvence prochází kvantovým kanálem k Bobovi.

Fáze 2

Bob změří polarizaci fotonů. Protože ze zákonů kvantové mechaniky nemůže foton změřit v obou schématech a neví, jaké schéma Alice použila, nezbývá mu nic jiného, než náhodně střídat schémata a na přijatých fotonech zjistit, zda od Alice přišla 0 či 1. Když zvolí schéma správně, dostane i správný výsledek – přesně to, co Alice posílala. Zvolí-li schéma chybně, může dostat libovolný výsledek (tj. 0 i 1). Počet chybně zvolených schémat je 1/2 ze zachycených fotonů.

Fáze 3

Po ukončení vysílání fotonů (těch musí být dostatečné množství, aby bylo možné vygenerovat klíč alespoň stejné délky jako zpráva, která bude posílána) si Alice s Bobem zavolají – například běžnou telefonní linkou – a Alice sdělí Bobovi pořadí schémat, ve kterých fotony posílala. **Nesmí však prozradit, zda posílala 0 či 1**. Bob si poznamená, které fotony změřil ve správném schématu, a sdělí to Alici. Od této chvíle oba zahodí všechny bity, ve kterých se neshodli na schématu a dále uvažují jen ty, které Bob změřil správně.

Fáze 4

Pro detekci odposlechu je potřeba, aby Alice s Bobem ještě obětovali část výsledného klíče a sdělili si, jaké hodnoty Alice vysílala a jaké hodnoty Bob naměřil. Pokud se shodují, zbývající bity jsou použity jako klíč. Pokud se neshodují, je nutné celý proces opakovat.

Fáze 5

Nyní mají Alice i Bob náhodný klíč skládající se z 0 a 1, který znají pouze oni a nikdo jiný. Zpráva může být zašifrována a poslána veřejným kanálem.

Co se stane, pokud Eva poslouchá?

Pokud Eva poslouchá na kvantovém kanálu, ani ona stejně jako Bob neví, jaké schéma Alice pro vyslání fotonu zvolí a protože nemůže měřit zároveň v obou schématech, a tak je podle vlastního uvážení střídá. Někdy zvolí správné nastavení, jindy ne. V průměru vychází, že Eva zvolí správné nastavení s Bobem asi ve čtvrtině případů. Má tak šanci získat malou část klíče.

BB84 jde ještě dál a umožňuje Alici a Bobovi zjistit, zda je Eva na kvantovém kanálu odposlouchávala. Pokud totiž Alice a Bob měli správné nastavení schématu a Eva zvolila schéma jiné, pak zcela jistě foton změnila a asi v polovině případů dostane Bob při svém měření nesprávnou hodnotu bitu. Například pokud Alice poslala 1 v x-schématu a Bob v x-schématu naměřil 0, je zřejmé, že jejich kanál je odposloucháván. Pokud dojdou k rozporu, je Eva odhalena. Metoda kontroly odposlouchávání není stoprocentní, ale pravděpodobnost, že Eva nebude odhalena je tak malá, že v praxi nemá šanci. Při n porovnaných bitech je pravděpodobnost odhalení $1-(3/4)^n$ (pro vyjádření v procentech toto číslo vynásobíme číslem 100), tj. například při porovnání 32 bitů klíče bude Eva odhalena s pravděpodobností 99,99%. Pokud Eva zachytí až zašifrovanou zprávu, která prochází nechráněným kanálem, tak si s ní nebude schopna poradit. Viz Vernamova šifra.

Ekertovo schéma

Nezávisle na Bennettu a Brassardovi přišel v roce 1991 Artur Ekert se svými výsledky v oblasti kvantové kryptografie. Pro své zkoumání zvolil kvantový jev zvaný 'propletené' částice (anglicky *entangled*, česká terminologie není jednotná). Dvě částice nazveme propleteným párem, pokud mají navzájem opačný spin a jsou v superpozici (tj. obě mají spin nahoru či dolů se stejnou pravděpodobností, nevíme v jakém ze dvou možných stavů se ta která částice nachází). Ve chvíli, kdy jednu částici změříme, zkolabuje druhá z páru do stavu opačného a to i v případě, že je libovolně vzdálená od té první. Polarizační schémata, ve kterých Alice a Bob měří letící částice, se od protokolu BB84 liší. Alice měří v jedné ze 3 zvolených rovin polarizace | / __, Bob analogicky v \ | /. Hodnota bitu je daná směrem, kterým zachycená částice kmitá. Kmitá-li zdola nahoru, hodnota bitu je 1, kmitá-li shora dolů, hodnota bitu je 0. Protože se používají propletené páry částic, Bob s Alice změří navzájem opačné kmitání. Pokud Alice naměřila 1 (například v bázi /) a Bob měřil ve stejné bázi (také /), potom on dostane 0. Je pouze otázkou dohody, kdo z nich před zašifrováním zprávy bity své kopie klíče zneguje, aby dostali stejný klíči.

Jak pracuje Ekertovo schéma?

Stejně jako v předchozím protokolu BB84, i zde jsou v praxi používány fotony a různá polarizační schémata, používají ale jiným způsobem. Vysílání fotonů pro vytvoření

náhodného klíče je však oproti BB84 **nezávislé** na Alici a Bobovi. Částice, z kterých bude určen klíč, může produkovat nezávislý zdroj. Zdroj vyrobí z propleteného páru dvě částice, jednu pošle Alici, druhou Bobovi. Zajímavostí tohoto protokolu je, že bit klíče se vytvoří až v okamžiku měření u příjemce (tedy u Alice nebo Boba). Samotná letící částice z propleteného páru není nositelem žádné informace.

Fáze 1

Alice i Bob zachytí posílaný foton. Ani jeden z nich neví, v jakém směru byl polarizován a tak náhodně volí jedno ze 3 schémat: Alice z |/__ a Bob z \|/. Pokud ve zvoleném schématu naměří spin zdola nahoru, zapíší si hodnotu 1, pokud je spin opačný, zapíší si 0. Je vidět, že Alice a Bob mohou měřit ve dvou shodných schématech (| a /) a jednom rozdílném (Alice __, Bob \). Vzájemný vztah mezi schématy je důležitý pro detekci odposlechu.

Fáze 2

Po ukončení vysílání fotonů (těch musí být dostatečné množství, aby bylo možné vygenerovat klíč alespoň stejné délky jako zpráva, která bude posílána) si Alice s Bobem zavolají – například běžnou telefonní linkou – a sdělí si pořadí schémat, ve kterých fotony měřili. **Nesmí však prozradit hodnoty, které naměřili**. Poznamenají si, ve kterých bitech se shodli.

Fáze 3

Hodnoty fotonů naměřené v různých schématech si sdělí a určí z nich korelační koeficient. Výpočet této fyzikální veličiny popisuje Ekert v [1] a zde ho nebudeme uvádět.

Fáze 4

Nesplňuje-li předchozí výpočet Bellovy nerovnosti, vědí, že získané měření je v pořádku. Od této chvíle mají náhodný klíč skládající se z 0 a 1, který znají pouze oni a nikdo jiný a zpráva může být zašifrována a poslána veřejným kanálem.

Co se stane, pokud Eva poslouchá?

I zde má Eva smůlu. Ekertův protokol totiž využívá propletený pár částic, pro který lze vypočítat korelační koeficient S, který by se u superponovaných částic měl blížit číslu $-2\sqrt{2}$. Pokud se Eva pokusí zachytit vysílaný foton, nutně zruší jeho superpozici. V kvantové mechanice neplatí Bellovy nerovnosti, které omezují korelační koeficient $-\sqrt{2} < S < \sqrt{2}$. Pokud Eva na kanále měří nebo částice falšuje, zruší superpozici částic a Bellovy nerovnosti začnou platit. Alice s Bobem však ví, že korelace má být přibližně rovna $-2\sqrt{2}$. Pokud tedy spočítají korelaci větší, jsou odposlouchávání. Eleganci tohoto řešení navíc dokresluje skutečnost, že k ověření bezpečnosti kanálu mohou použít fotony, v kterých se neshodli. Nemusí tedy obětovat jediný bit klíče.

2.5 Budoucnost

Kvantová kryptografie se zdá být koncem bitvy mezi kryptografy a kryptoanalytiky, z níž kryptografové vychází jako vítězové, protože navržené kvantové protokoly tvoří nerozluštitelný šifrovací systém. Toto tvrzení se může jevit jako příliš nadnesené, protože již několikrát v dějinách kryptografie bylo dokázáno, že i ty nejdůmyslnější systémy mají svou slabinu, kterou lze využít k prolomení – Vigenèrova šifra, Enigma, RSA. Tvrzení, že kvantová kryptografie je neprolomitelným systémem, se však od ostatních liší: Její bezpečnost nám zaručují přírodní zákony. Nejde jen o dočasnou bezpečnost, kdy se důmyslně využije slabina šifry – opakování klíče jako tomu bylo u Vigenèrovy šifry, ani se neopírá o technické možnosti dnešní společnosti – jako tomu bylo u Enigmy či RSA. Žádný pokrok lidstva nemůže změnit matematický důkaz potvrzující bezpečnost Vernamovy šifry a žádné lidské úsilí nezmění přírodní zákony – kvantovou mechaniku, která se řadí mezi největší úspěchy moderní fyziky. Kvantová kryptografie nám tak zaručuje bezpečnost, o kterou kryptografové tak dlouho usilovali. Nazývá se **nepodmíněná bezpečnost**, protože bezpečnost systému není podmíněna žádnými předpoklady na schopnosti a technické možnosti útočníka.

Do budoucna tak máme vizi, že pokud se podaří sestrojit systémy kvantové kryptografie, které budou fungovat i na velké vzdálenosti, budeme moci dokonale chránit své soukromí. Na druhou stranu však tyto systémy mohou použít rozsáhlé zločinecké skupiny pro bezpečnou komunikaci bez možnosti kontroly okolního světa. Kvantová kryptografie by vládám takovou kontrolu nad informacemi znemožnila. Je nutné zvážit, zda je pro nás důležitější vlastní soukromí či vlastní bezpečí.

Kapitola 3
Kódování informace a testy

3.1 Kódování množiny znaků

Vraťme se nyní k binárnímu kódování, které bylo popsáno v kapitole 2.4.1. Binární kódování můžeme brát jako binární čísla – posloupnosti 0 a 1, kde každá cifra odpovídá základní jednotce informace – 1 bitu. Ukázali jsme si, jak lze do binárních čísel zakódovat čísla a znaky. Binární kódování můžeme využít také pro sestavení kódu pro libovolnou množinu symbolů, přičemž nutně potřebujeme mít požadavek, aby tato množina byla konečná, protože pouze konečnou množinu symbolů můžeme jednoznačně reprezentovat konečným kódem.

Nejdříve uveďme pojmy, které budeme používat: **Kódováním** rozumíme zobrazení, které každému znaku ze zadané množiny (označme ji $\mathcal{M}$) přiřadí skupinu znaků jiné množiny (označme ji $\mathcal{Z}$). Kódování musí být jednoznačně dekódovatelné, tj. zobrazení z množiny $\mathcal{M}$ do množiny $\mathcal{Z}$ musí být prosté. Nadále v tomto textu budeme kódováním rozumět binární kódování, pokud nebude uvedeno jinak.

Přiřazením posloupnosti znaků z množiny $\mathcal{Z}$ prvkům množiny $\mathcal{M}$ vznikne **kódové slovo** w_i, index i udává, kolikátému prvku množiny $\mathcal{M}$ kódové slovo w_i patří. **Kódem** pak rozumíme množinu všech kódových slov (označme ji $\mathcal{C}$). Kód často zapisujeme pomocí tabulky, kde jsou v prvním řádku (či sloupci) uvedeny symboly množiny $\mathcal{M}$ a v druhém kódová slova z $\mathcal{C}$, jak je vidět v příkladu 3.1.

Délka kódu je počet všech různých kódových slov. Délku kódu je nutné rozlišovat od **délky kódového slova**, které udává počet kódových symbolů v daném kódovém slovu.

Naší snahou bude kód minimalizovat a to vzhledem k délce kódového slova. Později si ukážeme, jak minimalizovat průměrnou délku slov použitím kódů různé délky (viz optimální kódování v kapitole 4).

Jak nalézt nejkratší délku kódových slov pevné délky?

Je-li daná množina symbolů, ke kterým se má nalézt kódování pevné délky, které bude mít nejkratší kódová slova, spočteme si nejprve, do jakého nejmenšího počtu bitů je možné prvky dané množiny zakódovat. Vezmeme množinu symbolů, pro které hledáme kódování (označme ji $\mathcal{M}$), spočteme její velikost $|\mathcal{M}| = N$) a z rovnice

$$k = \lceil \log_2 N \rceil \tag{8}$$

určíme číslo k. To udává nejmenší délku kódových slov, které kódují prvky zadané množiny $\mathcal{M}$. Ke vzorci dospějeme následující úvahou. K nalezení nejkratšího kódování vybrané množiny znaků o velikosti N, je potřeba právě N navzájem různých kombinací 0 a 1, aby bylo možné od sebe jednotlivé znaky v kódu odlišit. A protože jejich počet je také roven počtu možností prostého zobrazení každého prvku z množiny $\mathcal{M}$ do množiny

$\{0,1\}^k$, kterých je 2^k, dostáváme rovnost $N = 2^k$ pro neznámé k. Po úpravě získáme rovnici $k = \log_2 N$, ze které dostaneme rovnici (8) po úvaze, že hledaný počet bitů musí být nejbližší vyšší celé číslo. Vezmeme tedy horní celou část z tohoto logaritmu. Délka každého kódového slova pro prvky z množiny $\mathcal{M}$ je tedy k.

Příklad 3.1:

Nalezněme binární kódování znaků z množiny $\mathcal{M} = \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit, \bullet, \wr, \star\}$.

Počet prvků v množině $\mathcal{M}$ je 7, z rovnice $k = \lceil \log_2 7 \rceil$ dostaneme, že $k = 3$, na kód každého znaku nám tedy postačí 3 bity. Následující tabulka ukazuje jedno z možných kódování.

$\clubsuit$	$\diamondsuit$	$\heartsuit$	$\spadesuit$	$\bullet$	$\wr$	$\star$
000	001	010	011	100	101	110

Pokud bychom přidali do množiny další znak – například †, stále nám postačí 3 bity ($3 = \lceil \log_2 8 \rceil$) a kód znaku † bude '111'. Přidáním dalšího znaku ‡, by již k bylo větší než 3 a nejmenší počet bitů, do kterých uložíme prvky množiny $\mathcal{M}$, by vzrostl na 4. Ke každému kódovému slovu bychom museli přidat zleva další bit odpovídající hodnotě 0 a novému znaku ‡ například kódové slovo '1000'.

Kódování pevné délky, které jsme zatím používali, se nazývá **blokové**. S blokovými kódy se lépe pracuje, protože přesně víme, kde ve zprávě začíná a kde končí každé kódové slovo. V našem případě každá trojice bitů výsledného řetězce 0 a 1 má význam jednoho symbolu výchozí množiny.

Ukážeme si, jak bychom mohli použít kódování různé délky. Pokud se rozhodneme, že kódová slova předchozího příkladu zkrátíme, a učiníme tak nevhodným způsobem, dostaneme se do nemalých komplikací, jak ukazuje následující text. Zvolíme si tedy pro ilustraci následující kódování pro stejnou množinu $\mathcal{M}$.

$\clubsuit$	$\diamondsuit$	$\heartsuit$	$\spadesuit$	$\bullet$	$\wr$	$\star$
0	1	10	11	100	101	110

Takové kódování je ovšem naprosto nevhodné. Z výsledné posloupnosti 0 a 1 totiž nedokážeme rozeznat, kde končí jedno kódové slovo a kde začíná další. Kódové slovo znaku $\star$ (110) tak můžeme snadno zaměnit s kódem znaků $\diamondsuit$ (1) a $\heartsuit$ (10). Při obdržení zprávy 1101011 tak dostáváme hned několik možností interpretace:

110 101 1, 110 10 11, 11 0 101 1 atp.

Z těchto několika interpretací vidíme, že dodáme-li ke kódovým slovům další symbol – mezeru, dostaneme kód jednoznačný. Mezera se ale stává součástí kódu a pro lepší viditelnost ji označme $\sqcup$. Máme tak místo binárního kódování tzv. ternární, tj. v množině tří znaků $\{0, 1, \sqcup\}$ a kód množiny $\mathcal{M}$ pak vypadá takto: $\{0\sqcup, 1\sqcup, 10\sqcup, 11\sqcup, 100\sqcup, 101\sqcup, 110\sqcup\}$. Vidíme, že jsme sice zkrátili kódy prvních symbolů množiny, ale naopak jsme prodloužili kódy posledních. Kdy je vhodnější použít blokové kódování a kdy kódování nepevné délky, závisí na vlastnostech zadané množiny symbolů. Více je popsáno v kapitole 4, kde se mimo jiné budeme věnovat optimálnímu kódování.

3.2 Multiple-choice testy

Psaní testů. Oproti klasické písemné práci má mnoho výhod: Testy se snadněji opravují, hodnocení je objektivnější (nehrozí špatné pochopení odpovědi, buď je zaškrtnutá správná možnost nebo není), z výsledků můžeme snadno sestavit statistiky, srovnání...

V době, kdy chceme mít co nejvíce informací a možností volby na základě srovnávání, to je samozřejmě příjemné. Na druhou stranu, *vyplňování* testů oproti *psaní* písemných prací, má i své nevýhody. Jednou z nich je nemožnost vyjádřit svou myšlenku a popsat danou problematiku. Také se nabízí otázka, jakou informaci z vyhodnocených testů vlastně získáváme. Jaké množství informace se v testech skrývá? Touto otázkou se nyní budeme zabývat podrobněji. Zaměříme se přitom na jeden typ testů tzv. multiple-choice. Multiple-choice test je typ zaškrtávacích testů s možností výběru jediné správné odpovědi z nabízených 3–4 variant (typicky označené možnostmi A, B, C nebo D).

Pokud studenti píší písemnou práci, kde musí sami vytvořit odpověď, je tato odpověď jen velmi těžko předatelná. Student by ji musel napsat v plném znění a takovou poslat ostatním. Nemůže ji snadno zestručnit a tím minimalizovat množství předávané informace. Odpověď je *příliš veliká* na to, aby ji mohl snadno předat. Pokud však dostane na výběr z několika málo možností, potom se pro něj celá otázka zredukuje na tento problém: Je správně odpověď první, druhá, třetí? V tu chvíli přestává být důležité, co se v které odpovědi píše, ale do popředí zájmu se dostává myšlenka, kterou z nabízených možností je nejvhodnější zaškrtnout. A na pomoc s rozhodnutím stačí pouze nenápadná nápověda o velikosti několika málo bitů.

Jaký je postup?
V případě multiple-choice testu, kde každá otázka nabízí 4 možnosti – A, B, C nebo D, snadno spočteme, že množství informace, kterou z odpovědi na otázku získáme, odpovídá počtu bitů, do kterých dokážeme odpověď (přesněji řečeno možnost) zakódovat. Dříve uvedeným postupem zjistíme, že na kódování množiny o 4 prvcích {A, B, C, D} nám postačí pouhé 2 bity:

$$\mathrm{A}-00, \mathrm{B}-01, \mathrm{C}-10, \mathrm{D}-11\,.$$

Množství informace, které nám student ve své odpovědi sdělí, je tedy 2 bity! 2 bity, 4 rozdílná gesta, pomocí kterých se může snadno dostat ke správné odpovědi.

Podívejme se ještě jednou na stejný problém, ale nyní ze strany spolupracujících studentů. Jak je těžké předat si informaci o hodnotě několika málo bitů v dnešní době, kdy digitální technologie jsou na takové úrovni, že informace o stovkách, tisících, milionech bitů lze předat v pouhém okamžiku? Jaké jsou možnosti využití této slabiny?

3.2.1 Předání informace

Vycházejme ze situace, že studenty ve škole čeká obávaný test. Předem vědí, že se bude jednat o test typu multiple-choice. Co udělají pro to, aby v tomto testu dopadli co nejlépe? Nejsnazší cesta vede přes třídního premianta, který je ochotný spolupracovat

a pokusí se distribuovat své výsledky ostatním. K tomu potřebují předem smluvený způsob komunikace. Když tedy přijde čas testu a premiant test vyřeší, může zbytek času věnovat na vysílání řešení.

Využití velikosti předávané informace

Jak jsme si již řekli, množství informace obsažené v typické testové otázce odpovídá 2 bitům – 4 možnostem. Stačí tedy, aby měli studenti mezi sebou domluvené 4 rozdílné signály: Jeden pro možnost, že správná odpověď je A, druhý pro B, třetí pro C a čtvrtý pro D. Může jím být ťuknutí tužkou do stolu, podrbání se ve vlasech, či zcela nenápadná otázka na učitele v určenou dobu. Záleží pouze na vynalézavosti konkrétního kolektivu, schopnostech využít prostředí, ve kterém test píší, či na slabostech vyučujícího, který je zrovna hlídá. Pokud budou takto cílevědomě postupovat několik let, od prvního ročníku až k maturitě, mohou být jejich způsoby tajné komunikace jen velmi těžko odlišitelné od přirozených rušivých gest či zvuků, kterým učitel stejně nemůže předejít, ani je rozpoznat, či vůbec zpozorovat.

Využití vhodného kódování

Další možností, jak si předat výsledky testu, je pokusit se předat vhodně zašifrované řešení: 10 otázek po 2 bitech, tj. celkem posloupnost 20 bitů. Nabízí se tedy převod 20-bitové posloupnosti binárních číslic do vhodného formátu, do kterého a z kterého by existoval snadný algoritmus převedení a riziko chyby při převodu by bylo minimální. Převod do desítkové soustavy není příliš vhodný – dostali bychom číslo příliš velké – a navíc postup mocnění dvojkou skrývá snadné chybování. Pokud ale zvolíme vhodnější soustavu – například šestnáctkovou (též nazývanou *hexadecimální*), nejen že počet cifer bude menší, ale i převod do a z binární soustavy bude rychlejší a riziko chyby velmi malé. Využijeme přitom vlastnosti, že šestnáctková soustava má základ $16 = 2^4$, z čehož vychází příjemná vlastnost pro převádění: 1 šestnáctková číslice odpovídá 4 bitům binárního čísla. Z 20 bitů informace tak dostaneme 5-ciferné číslo v šestnáctkové soustavě.

Jak se převod realizuje?

Posloupnost 0 a 1 rozdělíme na úseky po 4 číslicích 0 a 1. Z kterého konce začneme posloupnost rozdělovat, je věc dohody. My budeme používat variantu dělení **zprava**. Pokud poslední čtveřice (ta nejlevější) není kompletní, doplníme ji zleva nulami a dále s každou čtveřicí pracujeme samostatně: Převedeme ji na hexadecimální číslici podle tabulky Tab. 2.

V tabulce jsou kromě číslic použita i velká písmena anglické abecedy. Je tomu tak proto, že v soustavách o základu vyšším než 10 potřebujeme další symboly pro vyjádření číslice (10, 11, atd.). 10 i 11 jsou však symboly o dvou znacích, my je ale potřebujeme vyjádřit pouze jedním znakem. Vezmeme tedy velká písmena anglické abecedy. V šestnáctkové soustavě to jsou písmena A, B, C, D, E a F.

Hexadecimální číslo	Binární kód	Hexadecimální číslo	Binární kód
0	0000	8	1000
1	0001	9	1001
2	0010	**A** (10)	1010
3	0011	**B** (11)	1011
4	0100	**C** (12)	1100
5	0101	**D** (13)	1101
6	0110	**E** (14)	1110
7	0111	**F** (15)	1111

Tab. 2: Číslice hexadecimální soustavy.

Nyní zkusme zakódovat řešení testu o 10 otázkách. Máme k dispozici tyto správné odpovědi:

BBCDC CDDCC.

Podle předchozího kódování dostáváme binární číslo 01011011101011111010. Přerozdělíme ho (zprava) po 4 bitech na 0101 1011 1010 1111 1010 a podle tabulky převedeme na číslice šestnáctkové soustavy: 5BAFA. Tato podivná značka může být nesmyslná pro hlídajícího učitele, který papírek s tímto řešením zadrží, ovšem pro studenty může znamenat uspět v obávaném testu. Musí ale dokázat převést kód zpět na řešení testových otázek.

Řešení se převede zpět do binární soustavy a dekódování probíhá opačným způsobem, než zakódování: Obdržené řešení 5BAFA se přepíše do binárních číslic 0101 1011 1010 1111 1010 a zprava postupně se každá dvojici bitů vyjádří možností v testu: BB CD CC DD CC.

Problém při kódování může nastat, pokud počet otázek v testu není takový, aby po zakódování do binárního čísla dal celé čtveřice bitů. Například u 3 otázek s řešením ACD dostáváme posloupnost 00 10 11, což po rozdělení na čtveřice dává 00 1011 – tedy nekompletní druhou čtveřici (počítáme zprava). Zde je ale snadná pomoc, chybějící bity doplníme nulami a při kódování a dekódování využijeme toho, že řešení kódujeme a dekódujeme (zprava) a také toho, že známe počet otázek v testu. Víme tak, které bity v řešení chybí, či jsou nadbytečné. V našem příkladu nejdříve doplníme řešení 00 1011 na 8 bitů, tedy **00**00 1011, a pak převedeme na hexadecimální číslo 0B, tedy B, protože 0 můžeme vypustit. Při dekódování víme, že v testu byly 3 otázky, B však dá pouze řešení dvou z nich 1011, což má odpovídat řešení druhé a třetí otázky, C a D. Snadno ale odvodíme, že odpověď na první otázku je A, protože se zakódovala do kódu 00, který byl vynechán. Pokud obdržíme informaci 0B, tak při dekódování zjistíme, že řešení AACD je víc, než počet otázek v testu. První A vzniklo doplněním, je tedy nadbytečné, a řešením testu jsou až další tři písmena ACD.

Kapitola 4
Teorie informace

Pojem **informace** poprvé definoval C. E. Shannon ve své práci z roku 1948 Matematická teorie komunikace [5]. Tato práce se stala základem pro nově vzniklý vědní obor – teorie informace a následně dalších, například kryptologie.

4.1 Měření velikosti informace

Pro definici množství informace Shannon zavedl analogicky k termodynamice veličinu **entropie**. Entropií se vyjadřuje počet bitů informace připadající na 1 bit zprávy.

Mějme abecedu $s_1, s_2, \ldots, s_n$ a zprávy, ve kterých se jednotlivá písmena vyskytují nezávisle s pravděpodobnostmi $p_1, p_2, \ldots, p_n$. Entropii H potom definujeme jako:

$$\mathrm{H} = -\sum_{i=1}^{n} p_i \log(p_i) = \sum_{i=1}^{n} p_i \log\left(\frac{1}{p_i}\right), \tag{9}$$

Ukažme si několik příkladů: Předpokládejme, že očekáváme telegram, o kterém přesně víme, co v něm bude napsané. Telegram může mít následující znění: „Potvrzuji, že přijedu zítra ve smluvenou dobu.“ Z hlediska teorie informace takový telegram nemá žádnou informační hodnotu – zpráva obsahuje 0 bitů informace, protože pokud telegram přijde, tak ho ani nemusíme číst.

Stačí však, aby telegram obsahoval jiný údaj – například odpověď na otázku: „Přijedeš zítra ve tři hodiny?“ – a my již očekáváme, že z odpovědi získáme nějakou informaci. Naše očekávání je rovnoměrně rozděleno mezi dvě možnosti – ANO a NE. Telegram nese informaci o velikosti 1 bitu. Abychom se z něj potřebnou informaci dozvěděli, musíme jej přečíst. I když je zpráva vyjádřená několika písmeny, z pohledu teorie informace jde stále o 1 bit. Stejně tak může telegram na naši otázku vypadat takto: „Přijedu zítra ve tři hodiny, jsme tedy domluveni.“. Množství informace zůstává stále 1 bit.

Jak je z příkladu vidět, při posílání druhého telegramu jsme nezvolili nejvýhodnější kódování pro předání očekávané informace. Pokusme se najít optimální kódování.

Pod pojmem optimální kód si představíme kód kódující zprávu do co nejmenšího počtu bitů, tak aby zůstal zachován obsah zprávy. V našem příkladu by řešení bylo jednoduché: Stačí poslat 1/0 (ANO/NE).

Jednou z možností pro nalezení optimálního kódování je použití prefixového Huffmanova kódování [3].

Prefixový kód má tu vlastnost, že žádné kódové slovo nesmí být předponou jiného kódového slova. Příklad neprefixového kódu může být slovo s_1 zakódované jako 00 a s_2 s kódem 001. Je vidět, že kód 00 je prefixem (nebo též „předponou“) kódu 001.

V roce 1952 představil D. A. Huffman algoritmus pro konstrukci optimálního prefixového kódu. Kódování, které touto metodou vytvoříme, nazýváme **Huffmanovo kódování** nebo Huffmanův kód.

Postup konstrukce binárního Huffmanova kódu

Mějme abecedu S o symbolech $s_1, \ldots, s_q, q \geq 1$, pro kterou chceme najít Huffmanův kód. K této abecedě je dána (nebo ji musíme zjistit) pravděpodobnost p_i $(i = 1, \ldots, q)$ výskytu jednotlivých symbolů v textu, tj. pravděpodobnost, že k-tý znak zprávy bude s pravděpodobností p_i znak s_i. Bez újmy na obecnosti setřídíme symboly zadané abecedy podle jejich pravděpodobností výskytu do nerostoucí posloupnosti tak, aby pro $s_1, \ldots, s_q$ platilo:

$$p_1 \geq p_2 \geq p_3 \geq \ldots \geq p_q.$$

Nejméně používané symboly s_q a s_{q-1} sloučíme do nového symbolu s', který by se ve zprávě vyskytoval s pravděpodobností $p' = p_q + p_{q-1}$. Vznikne nám tak nová abeceda S′, která má o jeden symbol méně než abeceda původní.

Z abecedy S′ opět vezmeme dva nejméně se vyskytující symboly a ty sloučíme, jejich pravděpodobnosti sečteme. Takto postupujeme až do okamžiku, kdy nám zůstane k zakódování abeceda o jednom symbolu s pravděpodobností 1.

Nyní začneme tvořit kódování. Jednoprvkovou množinu, jejíž jediný znak se vyskytuje s pravděpodobností $p_1 = 0$, má kód w_1 prázdný, což vyjádříme symbolem λ*), tedy $w_1 = \lambda$.

Máme-li sestrojené kódy $w_1,\ w_2,\ w_3,\ \ldots,\ w_{q-2},\ w'$, sestrojíme kód w_{q-1} a w_q z kódu w' tak, že k w' doplníme symboly 1 a 0 tak, abychom neporušili vlastnosti prefixového kódu. Postup je naznačen v následujícím schématu:

$$\begin{aligned} \mathcal{C}^i &: \quad w_1, w_2, w_3, \ldots, w_{q-2}, \quad w' \quad , \\ \mathcal{C}^{i-1} &: \quad w_1, w_2, w_3, \ldots, w_{q-2}, w'\mathbf{0}, w'\mathbf{1}, \ i = 1, \ldots, q-1. \end{aligned}$$

Pokud kód obsahuje alespoň jeden ze symbolů 0, 1 (není tedy prázdný), symbol λ vynecháváme.

Z abecedy $\mathrm{S}' = \{s_1, s_2, \ldots, s_{q-2}, s'\}$ a kódování $\mathcal{C}' = \{w_1, w_2, w_3, \ldots, w_{q-2}, w'\}$ tak odvodíme pro původní abecedu $\mathrm{S} = \{s_1, s_2, \ldots, s_q\}$ kódování $\mathcal{C} = \{w_1, w_2, \ldots, w_q\}$, kde $w_{q-1} = 0w'$ a $w_q = 1w'$. Konstrukci si lépe ukážeme na příkladu.

Příklad 4.1:

Sestrojení Huffmanova kódu pro abecedu S= $\{s_1, s_2, s_3, s_4, s_5\}$ s pravděpodobnostmi $p_1 = 0,3, p_2 = 0,2, p_3 = 0,2, p_4 = 0,2$ a $p_5 = 0,1$.

*) λ se používá pro vyjádření prázdné posloupnosti, prázdného řetězce atp.

			s_1		s_2	s_3	s_4	s_5
S:			$0,3$		$0,2$	$0,2$	$0,2$	$0,1$
S′:			$0,3$	$\mathbf{0,3}$	$0,2$	$0,2$		
S″:		$\mathbf{0,4}$	$0,3$	$0,3$				
S‴:	$\mathbf{0,6}$	$0,4$						
S⁗:	**1**							
$\mathcal{C}''''$:	λ							
$\mathcal{C}'''$:	**0**	1						
$\mathcal{C}''$:		**1**	$\underline{0}0$	$\underline{0}1$				
$\mathcal{C}'$:			$\underline{0}0$	$\mathbf{\underline{0}1}$	$\underline{1}0$	$\underline{1}1$		
$\mathcal{C}$:			$\underline{0}0$		$\underline{1}0$	$\underline{1}1$	$\underline{01}0$	$\underline{01}1$

Jak je vidět z předchozího postupu, k abecedě $\mathrm{S} = \{s_1, s_2, s_3, s_4, s_5\}$ jsme zkonstruovali množinu kódů $\mathcal{C} = \{00, 10, 11, 010, 011\}$, což je vyjádřeno v následující tabulce.

Otevřená abeceda	Kódová abeceda
s_1	00
s_2	10
s_3	11
s_4	010
s_5	011

Zprávu $s_1 s_1 s_4 s_3 s_5$ zakódujeme jako 000001011011.

Ukažme si, jak může vypadat zpráva v přirozeném jazyce v různém kódování.

Příklad 4.2:

Text v přirozeném jazyce obsahuje nejen písmena abecedy, ale i další interpunkční znaménka popř. národní symboly. Podle ASCII tabulky víme, že každý znak textu zakódujeme do 8 bitů. Máme-li tedy text délky n, snadno spočítáme, že velikost tohoto textu je $8 \cdot n$ bitů. Například krátká elektronická zpráva délky 5 řádků po 70 znacích, má v ASCII kódování velikost $8 \cdot (5 \cdot 70) = 2800$ bitů.

Příklad 4.3:

Vezmeme si opět písmena abecedy – ale pouze anglické abecedy – a základní interpunkční znaménka: mezeru $\sqcup$, tečku . a čárku ,. Dohromady máme množinu 29 symbolů, ke kterým jsme schopni nalézt blokový kód o délce $\lceil \log_2 29 \rceil = 5$ bitů. Zprávu z předchozího příkladu (za předpokladu, že žádné další znaky neobsahuje) zakódujeme do $5 \cdot (5 \cdot 70) = 1750$ bitů.

Příklad 4.4:

Zvolme nyní optimální kódování. Udává se, že pro anglický jazyk, je průměrný počet bitů na jedno písmeno 1,5 bitu, Klíma [7]. Toto číslo se pro dostatečně dlouhé zprávy blíží konstantě, kterou označujeme r a nazýváme ji **obsažnost jazyka** k jednomu písmenu. Vychází nám, že zprávu lze zakódovat průměrně do $1,5 \cdot (5 \cdot 70) = 525$ bitů. Takové kódování však nemusíme být schopni v praxi nalézt nebo aplikovat.

Ukázali jsme, že zvolíme-li různá kódování, počet bitů zprávy se může lišit, nikoliv však množství informace obsažené ve zprávě. Toto množství se udává jako nejmenší počet bitů, do kterých jsme schopni zprávu zakódovat v optimálním kódování. Množství informace ve zprávě je totiž **nezávislé na použitém kódování**.

Kapitola 5
Metody měření

Při získávání dat pro diplomovou práci jsem využila dvou zdrojů:

- Vlastní webovou stránku, na které mohli návštěvníci anonymně vyplnit formulář, ve kterém popsali způsob napovídání, s kterým se setkali.
- Výsledky z testů, které jsem realizovala na pražské škole SPŠ ST Panská ve 2. ročnících technického lycea.

5.1 Webový formulář

Při sbírání dat pomocí webového formuláře jsem se zaměřila na metody napovídání. Účelem bylo zjistit, s jakými metodami se návštěvníci této stránky setkali. Zároveň ke každé metodě bylo nastaveno počítadlo, kolik návštěvníků tuto metodou zná. Počet návštěvníků, kteří metodu znají či používají, je jistou známkou kvality metody – čím méně lidí, tím je originálnější.

Pro mě nebyly zajímavé metody „dobře známé“, kterých se objevilo nejvíce, ale chtěla jsem tak zachytit i nějaké nové a zajímavé způsoby napovídání, které jsou originální a použitelné právě pro typ testování, které potřebuji. Poučena z těchto dat jsem tak mohla docílit lepšího proškolení studentů, na kterých jsem provedla měření pomocí testů. Zároveň každá třída byla na závěr požádána, aby své zkušenosti popsala do tohoto webového formuláře, aby mohla inspirovat další skupiny.

Formulář i se sebranými výsledky je zveřejněn na mých osobních stránkách:

http://jirina.hrusova.matfyz.cz/diplomka/metody.php.

5.1.1 Sesbírané metody

Příspěvky do sbírky mi posílali nejen studenti středních, ale také učitelé, studenti vysokých škol a náhodní návštěvníci stránky. Vznikla tak zajímavá sbírka, jejíž souhrn zde uvádím. Podrobnosti jsou ale pouze na webové stránce na výše uvedené adrese.

Následující přehled byl sepsán z dat nasbíraných k datumu 20. dubna 2006.

Aplikace steganografie

Do této kategorie napovídání spadají všechny metody, které využívají velikosti předávané informace. Předání výsledků touto cestou vyžaduje symetrickou komunikaci mezi studenty. Může se jednat například o jednoho studenta jako zdroje informací, který posílá řešení předem smluvenými signály. Přijímající studenti pouze odpovídají, zda zasílané řešení zachytili. Snahou studentů potom je, aby tato komunikace nebyla učitelem odhalena, signály proto musí být co nejstručnější a nenápadné, aby nebyly zpozorovány.

Pomocí smluvených signálů

Studenti si předem sestaví komunikační abecedu typu: jaký signál znamená odpověď A, jaký B atd. Dále mohou mít pomocné signály pro 'nerozumím', 'to je špatně', 'pochopil jsem', atp.

- *Nápověda zvukovými signály*

  Domluvené signály nepotřebují zrakový kontakt mezi studenty. Výsledek je snadno předatelný jedním studentem všem ostatním. Nevýhodou může být nemožnost zpětné odezvy k tomuto studentovi. Pokud by totiž začalo odpovídat několik studentů najednou, je vše prozrazeno.

  · vyťukávání řešení tužkou,
  · zvolání výsledku...

- *Nápověda posunky*

  Tato komunikace je omezená na dva komunikující subjekty. Umožňuje zpětnou odezvu a může být jen velmi těžko odlišitelná od přirozených gest. Nevýhodou tohoto způsobu komunikace je rychlost šíření informace po třídě.

  · mrkání,
  · kývání hlavou,
  · protahování se,
  · škrábání se ve vlasech, na zádech atp.
  · ukazování na prstech...

  V této kategorii mě zaujala metoda, kdy zadní student natáhl nohy k přednímu sousedovi a ten své nohy stočil pod sebe a přes podrážky bod si vyťukávali smluvené signály. Tato metoda je skvěle nenápadná.

- *Využitím učitele*

  Vhodným kandidátem pro předání výsledků se může stát i učitel a ani nemusí mít tušení, že k něčemu takovému přispěl. Stačí, když jeho reakce ponese potřebné informace pro studenty.

  · položením vhodné otázky učiteli,
  · v dohodnutý čas učiteli položit jakoukoliv otázku...

Využití prostředí

Zde mohou studenti vhodně pracovat s místem, ve kterém se nachází. Pomineme-li specifickou situaci, že jsou zkoušeni u počítačů, kde existuje nemalá šance komunikovat nezakázanou počítačovou sítí pomocí jednoho z mnoha programů typu NetSend, který je implementován v základní výbavě operačního systému, můžeme najít i zde originální triky.

· světla ve třídě,
· rozmístění lavic...

Aplikace šifrování

Tato kategorie napovídání zahrnuje metody, které počítají s možností odhalení nápovědy. Vyžaduje od studentů použít vhodné šifrování tak, aby nebylo možné rozpoznat, co zadržená informace znamená. Řešení může kolovat po třídě na zatím blíže nespecifikovaném taháku. Jeho existenci může učitel odhalit, ale pokud bude řešení správně utajené – zašifrované, nemusí zabavené řešení nutně vést k odhalení nápovědy. Někdy může studentům posloužit pouze vhodné zakódování odpovědí, a to v případě, že předpokládají, že takové kódování učitel nezná nebo neočekává, že může nějak souviset s testem. Hodit se může například hexadecimální kód popsaný v kapitole 3.2.1 Předání informace.

Vypůjčování si věcí

U studentů je běžné, že si navzájem půjčují různé učební pomůcky. Při zkoušení je tato praxe většinou zakázána, ale zvyk je železná košile, a tak i přes učitelův zákaz studenti zkouší své štěstí. Důvod půjčování pomůcek může však být i jiný, jak si uvedeme zde.

- *Povolené pomůcky*

  Zde je uvedeno několik věcí, které studenti mohou používat. Nezřídka se stává, že se ve třídě vyskytuje jen několik exemplářů těchto pomůcek. Využít je k předání informace je pak velmi snadné.

  · MFCH tabulky,
  · pravidla pravopisu,
  · slovník...

- *Pomůcky, které nelze zakázat*

  Školní pomůcky, které studenti každý den používají a potřebují je tedy i při zkoušení. Zde jde o bezděčné gesto: „Mohu si od tebe na chvíli vypůjčit ...? Jak lze uhlídat, aby takto nekoloval jeden předmět po celé třídě?“

  · guma,
  · kalkulačka,
  · prázdný list papíru, na kterém jsou protlačeny výsledky...

  a další.

5.2 Testování studentů

Pro testování studentů jsem si připravila sérii znalostních testů, ze kterých jsem chtěla získat data pro ověření následující hypotézy:

Jsou studenti schopní pomáhat si při psaní multiple-choice testů a zlepšit si tak své výsledky?

Testy v jednotlivých sériích měli být průměrné úrovně, tj. ne příliš těžké, aby je studenti nebyli schopni vyřešit, ale také ne příliš lehké, které by dokázal vyřešit každý a neměl by tak motivaci k napovídání. Rozhodla jsem se proto sestavit testy z prověřených otázek, u kterých je známa statistika úspěšnosti. Podklady mi byly srovnávací testy z deskriptivní geometrie a fyziky pro 2. ročníky v SPŠ ST Panská. Testovanou skupinou pak byly studenti 2. ročníků technického lycea na této škole.

5.2.1 Podoba testů

K testování jsem si připravila dva typy testů: znalostní a druhé, pro které budeme dále používat název „prázdné testy“. Podrobnosti k oběma testům jsou popsány v následujícím textu.

Znalostní test

Pro každý z testovaných předmětů byly sestaveny dva multiple-choice testy stejné úrovně: První pro úvodní test, druhý pro otestování, zda došlo ke zlepšení výsledků oproti testu prvnímu. Oba testy byly zhruba stejné úrovně, sestavené z původních – ekvivalentních – variant testů. Hodnocení testu bylo bráno jako součet bodů, které student získal v jednotlivých otázkách. Za správnou odpověď na otázku dostal student 1 bod (v testu z fyziky a deskriptivní geometrie) nebo 2 body (u vybraných otázek v deskriptivní geometrii). Za špatnou odpověď pak bylo 0 bodů. Body za špatné odpovědi se neodčítaly. Testy neobsahovaly žádné chytáky, ani v otázkách ani v sestavení, jako je například vzájemné přeházení otázek v jednotlivých exemplářích testů. Snažila jsem se tak usnadnit komunikaci mezi studenty. Není to sice standardní situace, ale pro můj účel tento model postačil. Důvodem byla úvaha, že vyškolení studenti mohou během 4 let, které společně studují, najít způsoby, jak obejít nástrahy, kterými se jim snaží tvůrci testů znesnadnit opisování.

Podoba testu v druhém kole se od prvního trochu lišila. Bylo v nich ponecháno více prostoru pro zaznamenání speciálních značek, které jsem potřebovala pro vyhodnocení. Studenti měli navíc na zaznačení správné odpovědi více sloupců.

Prázdný test

Na tomto typu testu si studenti mohli vyzkoušet účinnost svých metod napovídání. Použity byly při proškolování studentů v metodách napovídání. Test obsahoval 5 „otázek“, u kterých chyběl jakýkoliv kontext. Vyplnění prázdného testu záviselo pouze na tom, jaká informace se k danému studentu dostala nebo na náhodě – jak student daný test „natipoval“, pokud žádnou informaci nedostal, či neměl chuť spolupracovat. Ukázka nevyplněného testu následuje:

__ **Otázka č. 50:**

A) A) A) *****,

B) B) B) *****,

C) C) C) *****,

D) D) D) *****.

Při vyplňování testů měli studenti k dispozici tři sloupečky možností A, B, C a D. Důvod této úpravy je podrobněji popsán v sekci 5.2.2 Realizace prázdných testů. Smyslem tohoto testu bylo pomoci studentům ověřit si, jak dobrou metodu nápovědy zvolili. Pro mě ale bylo lákavé změřit na těchto testech změřit způsob šíření informace po třídě, je-li předem vybraný zdroj, od kterého bude informace vysílána. K detekci šíření informace mi studenti do testů zapsali značky k otázkám, pomocí kterých mi sdělili, odkud se k nim informace dostala. Podrobnosti tohoto měření jsou popsány v sekci Realizace testů.

5.2.2 Realizace

Testování studentů proběhlo ve dvou kolech s odstupem dvou týdnů. Mezi těmito dvěma koly proběhlo školení studentů v metodách napovídání, diskuzi o metodách, které sami vyzkoušeli nebo chtěli vyzkoušet atp. V rámci těchto diskuzí proběhlo i několik kol prázdných testů, ve kterých si mohli své napovídání procvičit.

Znalostní test

Studenti psali celkem 4 znalostní testy. Dva v prvním kole, každý z jiného předmětu – fyzika a deskriptivní geometrie – a obdobné dva v kole druhém. Při sestavení testů jsem využila toho, že třída při testech nebude dělená na oddělení. Použila jsem tak různé varianty původních testů pro různá kola. Docílila jsem tím toho, že testy z prvního i druhého kola byly vyvážené, přitom ale různé varianty obsahovaly různé úlohy.

Testy nebyly anonymní. Znalostní testy byly psány s vyučujícími jednotlivých předmětů a podle vlastního uvážení (a pro větší motivaci studentů) mohli testy vyhodnotit jako písemnou práci, kterou zahrnuli do své klasifikace. V principu pro mne však nebylo důležité, kdo konkrétní test napsal, pouze jsem potřebovala správně spárované vyhodnocení z obou kol.

První kolo testů nebylo z mé strany nijak ovlivněno. Test prvního kola vypadal jako klasický multiple-choice test. V druhém kole pak test obsahoval prostor pro značky, kterými mi proškolení studenti dávali zpětnou vazbu, jak si při testech dokázali napovídat. Podrobnosti značení jsou popsány v dalším odstavci, protože stejného značení bylo použito i v testech prázdných. Studenti se tak mohli se značkami sžít, aby se jejich vyplňováním v ostrém testu příliš nezdržovali.

Pro srovnání následuje ukázka testové otázky z fyziky v I. kole a v II. kole:

__ **Otázka č. 5:** (FY2055)
Účinnost stroje:

A) je rovna rozdílu mezi příkonem a výkonem,

...

__ **Otázka č. 9:** (FY2729)
Stabilita tělesa je určena:

A) A) A) těžištěm tělesa,

...

Prázdný test

Studentům byly rozdány prázdné testy popsané výše. Třída si vybrala dva dobrovolníky – zdroje, kteří obdrželi test vyplněný správnými odpověďmi. Oba tyto testy byly stejné. Pro každé kolo byly správné odpovědi náhodně vygenerovány. S těmito dobrovolníky si studenti před zahájením testu nebo během diskuze domluvili signály, pomocí kterých budou komunikovat. Mým úkolem bylo jednak v průběhu testu „hlídat“ jako učitel, ale také upozorňovat je na nedostatky jejich metody, na příliš výrazná gesta atp. Podle časových možností byly vyzkoušeny různé metody v několika kolech. Při tomto školení nesměli být přítomni vyučující předmětů, kteří studenty hlídali při psaní testů znalostních.

Správné odpovědi studenti označovali *kroužkem*, *zaškrtané* odpovědi znamenali, že považovali nabízenou možnost za jasný nesmysl. Z tohoto důvodu bylo nutné rozlišit, kdy student možnost zaškrtá proto, že si rozmyslel její zakroužkování a nebo ji zaškrtal, protože ji považoval za nesmysl. Na odpověď byly tedy připraveny tři sloupečky. Studenti již zaškrtnuté možnosti nesměli opravovat do stejného sloupečku, ale do dalšího. Za správnou odpověď se pak počítal vyplněný sloupeček *nejvíce vpravo*. Pokud se tedy student v prvním sloupečku spletl a chtěl svou odpověď opravit, zakroužkoval správnou možnost ve sloupečku druhém popř. již třetím.

Studenti do testu navíc vyplňovali značky, díky kterým bylo možné sestavit model šíření informace po třídě. Všichni obdrželi prázdný test, někteří měli na svých testech zaznačené odpovědi. Testy byly očíslované pořadovými čísly, jak seděli v lavici, kvůli zpětné rekonstrukci šíření informace po třídě. Směr číslování je z pohledu učitele: zleva doprava, odpředu dozadu. Pořadové číslo 1 má student v první lavici vlevo v nejlevějším oddělení, jeho soused je v pořadí druhý atd. Příklad rozmístění 30 studentů ve třídě ukazuje následující tabulka Tab. 3.

24	25	26	27	30	×
×	21	22	23	×	×
16	17	×	18	19	20
10	11	12	13	14	15
7	×	8	9	×	×
1	2	3	4	5	6

Tab. 3: Příklad rozmístění 30 studentů ve školních lavicích.

Při psaní testů směli mít studenti při ruce pomocný papír s pokyny, jaké postranní informace mi mají předat. Tyto pokyny měli k dispozici i při druhém kole znalostních testů, ale s podmínkou, že s jejich obsahem nejsou seznámeni vyučující, kteří na studenty dohlíželi při znalostních testech v této či jiné třídě. Příklady možného vyplnění prázdné testové otázky je vidět v následující ukázce:

N Otázka č. 1:

A) A) A) *****,
B) B) B) *****,
C) C) C) *****,
D) D) D) *****,

VILS Otázka č. 1:

A) A) A) *****,
B) B) B) *****,
C) C) C) *****,
D) D) D) *****,

V levé ukázce student sděluje, že si svou odpověď dvakrát rozmyslel a pak na ni odpověděl náhodně (N = nevím nebo náhodně tipuji) poté, co vyloučil možnosti C a D. V pravé ukázce student ví správnou odpověď a ještě dostal informaci od svého levého souseda (V = vím, I = informace, LS = levý soused), který nějakým způsobem informaci dostal. Podrobnosti budou ve značce u stejné odpovědi tohoto souseda. Stejně jako v levé ukázce, i zde student vyloučil možnosti C a D.

Kompletní tabulka značek je následující:

Značka	Pozn.	Zkratka za	Význam
N		nevím/náhodně tipuji	Odpověď nevím, nedostala se ke mě.
V		vím	Odpověd vím i bez napovídání.
I		informace	Došla ke mě informace od spolužáků o správné odpovědi.
	LS	levý soused	Informaci jsem získal od levého souseda.
	PS	pravý soused	Informaci jsem získal od pravého souseda.
	RS	pRední soused	Informaci jsem získal od souseda přede mnou.
	ZS	zadní soused	Informaci jsem získal od souseda za mnou.
Z	*A*	informace od zdroje A	Dostal jsem informaci od zdroje A.
	B	informace od zdroje B	Dostal jsem informaci od zdroje B.

Tab. 4: Značky, které používali studenti k zaznačení, odkud se k nim dostala informace o správné odpovědi.

Jak je vidět z této tabulky a předchozího příkladu, značky se mohou různě kombinovat. Není tedy nutné uvádět pouze I, ale v kombinaci $V\ I$, popřípadě $V\ I\ RS$ nastává velmi příznivá možnost pro tohoto studenta a dost jasná stopa pro mě.

Kapitola 6
Výsledky

V této kapitole jsou uvedeny výsledky testů a naměřených dat. Výsledky jsou rozděleny do těchto oblastí:

- *Ověření hypotézy*, v níž jsme chtěli prokázat, že si studenti zlepší výsledky při psaní testů, budou-li vhodně využívat tajnou komunikaci a množství předávané informace.
- *Šíření informace*, ve které jsme zjišťovali, jestli se informace šíří mezi studenty a v jaké míře.

6.1 Výsledky testů

Studenti z dvou vybraných tříd psali ve dvou kolech multiple-choice testy z fyziky a deskriptivní geometrie. První test proběhl jako standardní test bez vědomí studentů, že jsou testováni. V druhém kole byly instruováni k tomu, aby spolupracovali. Výsledky těchto testů jsou uvedeny v tabulce Tab. 5 a Tab. 6.

DG – Body studentů

1. vzorek	I. kolo	5	6	6	3	6	7	4	6	7	7	7	7	7	5	6	7	7	7	5	7	5	5	5	6	4
1. vzorek	II. kolo	7	7	7	7	7	7	7	7	7	7	5	7	7	5	7	7	7	7	6	7	7	4	7	7	7
2. vzorek	I. kolo	7	6	4	7	2	4	5	7	5	5	7	7	5	7	7	5	7	4	7	6	7	3	7	7	7
2. vzorek	II. kolo	7	3	3	3	3	5	7	7	7	3	6	7	5	7	5	3	7	5	5	3	5	7	7	7	3

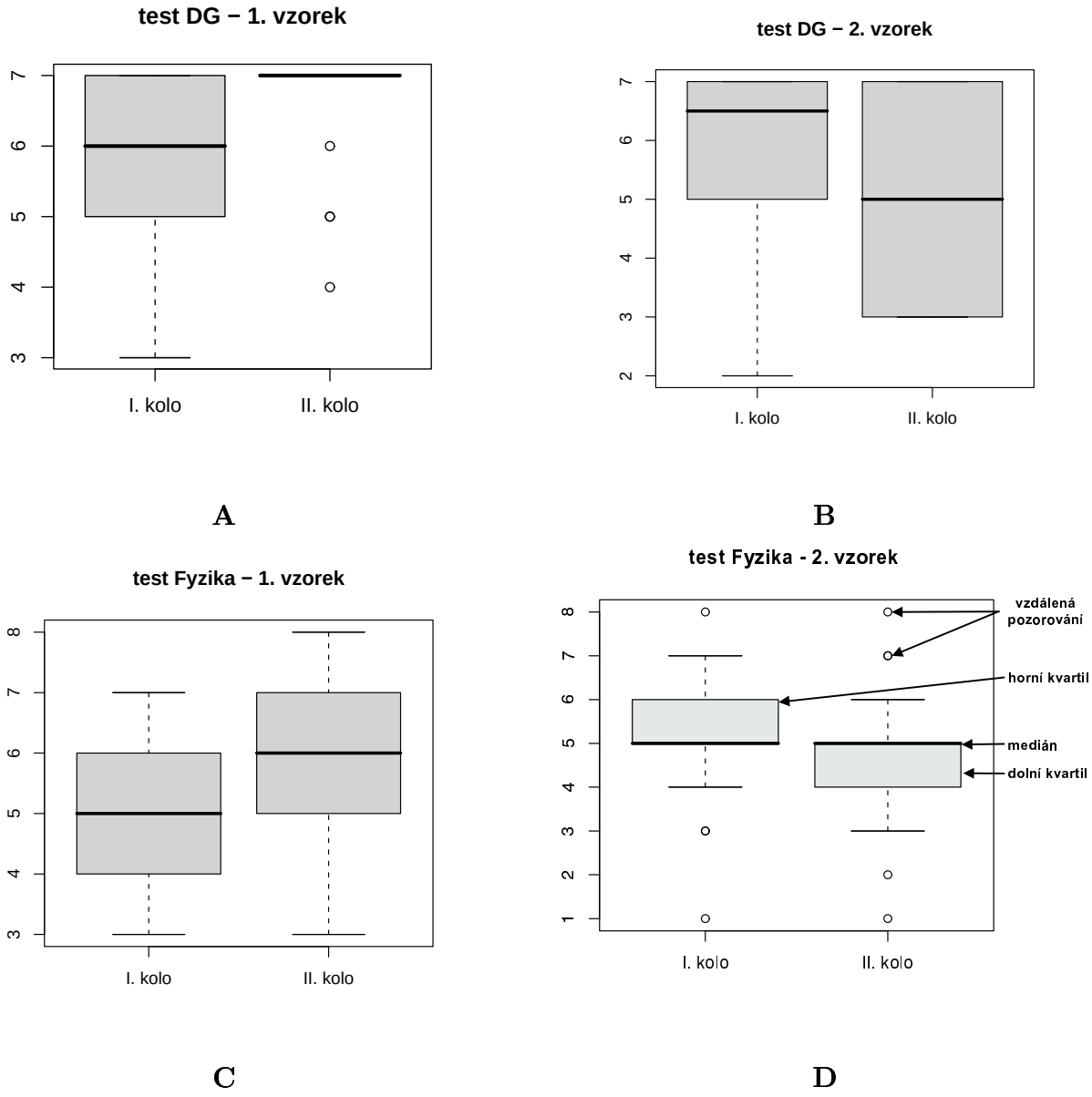
Tab. 5: Body získané v testech z deskriptivní geometrie. První dva řádky patří výsledkům první třídy v prvním a druhém kole testů, třetí a čtvrtý řádek patří druhé třídě.

Fyzika – Body studentů

1. vzorek	I. kolo	5	7	5	5	4	5	5	5	5	5	6	4	6	5	3	6	6	4	6	4	3	4	6	4	
1. vzorek	II. kolo	5	7	7	5	6	8	5	5	8	3	8	6	5	6	6	7	6	5	4	6	8	6	7	4	
2. vzorek	I. kolo	5	7	7	7	6	5	6	4	7	6	3	3	4	5	4	5	8	6	7	6	5	6	5	5	1
2. vzorek	II. kolo	5	5	4	5	5	5	4	2	5	6	4	5	3	5	5	7	6	5	7	5	4	8	1	5	6

Tab. 6: Body získané v testech z fyziky. První dva řádky patří výsledkům první třídy v prvním a druhém kole testů, třetí a čtvrtý řádek patří druhé třídě.

Grafické znázornění dat pomocí krabicových diagramů je na obrázku Obr. 2. Výsledky byly zpracovány programem pro statistické výpočty R (volně ke stažení na http://www.r-project.org). Pro grafické znázornění výsledků byl použit graf box-plot (nebo-li krabicový diagram).



Obr. 2: Grafické znázornění získaných dat pomocí krabicových diagramů. Zobrazují rozložení výsledků kolem mediánu jednotlivých měření – test z deskriptivní geometrie pro první (A) a druhý (B) vzorek studentů a test z fyziky pro první (C) a druhý (D) vzorek studentů.

Dospěli jsme k závěru, že první vzorek studentů dosáhl vzhledem k prvnímu kolu zlepšení v obou testech druhého kola. Naopak druhý vzorek studentů lepších výsledků nedosáhl, případně se zhoršil. V případě prvního vzorku studentů byla hypotéza potvrzena, v případě druhého vzorku byla potvrzena negovaná hypotéza.

Znalosti a opsané odpovědi v testech

Ze znalostních testů druhého kola jsou v tabulce Tab. 7 zde vybrány údaje, které ukazují počet odpovědí v jednotlivých kategoriích a průměrný počet na kolik otázek každý student odpověď zná a v kolika otázkách mu někdo k odpovědi pomohl. Některé odpovědi zůstaly neoznačené.

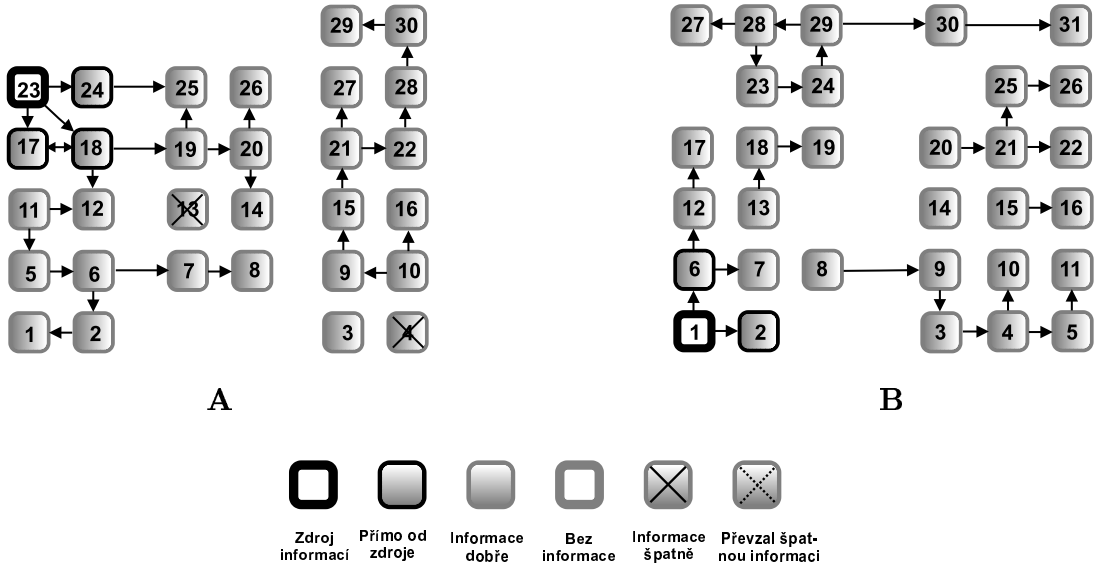
DG	1. vzorek	2. vzorek
V*	37,8%	40,5%
VI*	24,1%	4,3%
I*	37,0%	33,6%
N*	0%	18,1%
Znal odpověď	**62,9%**	**44,8%**
Opsal	**37,0%**	**33,6%**
Napověděl	**11,9%**	**4,8%**

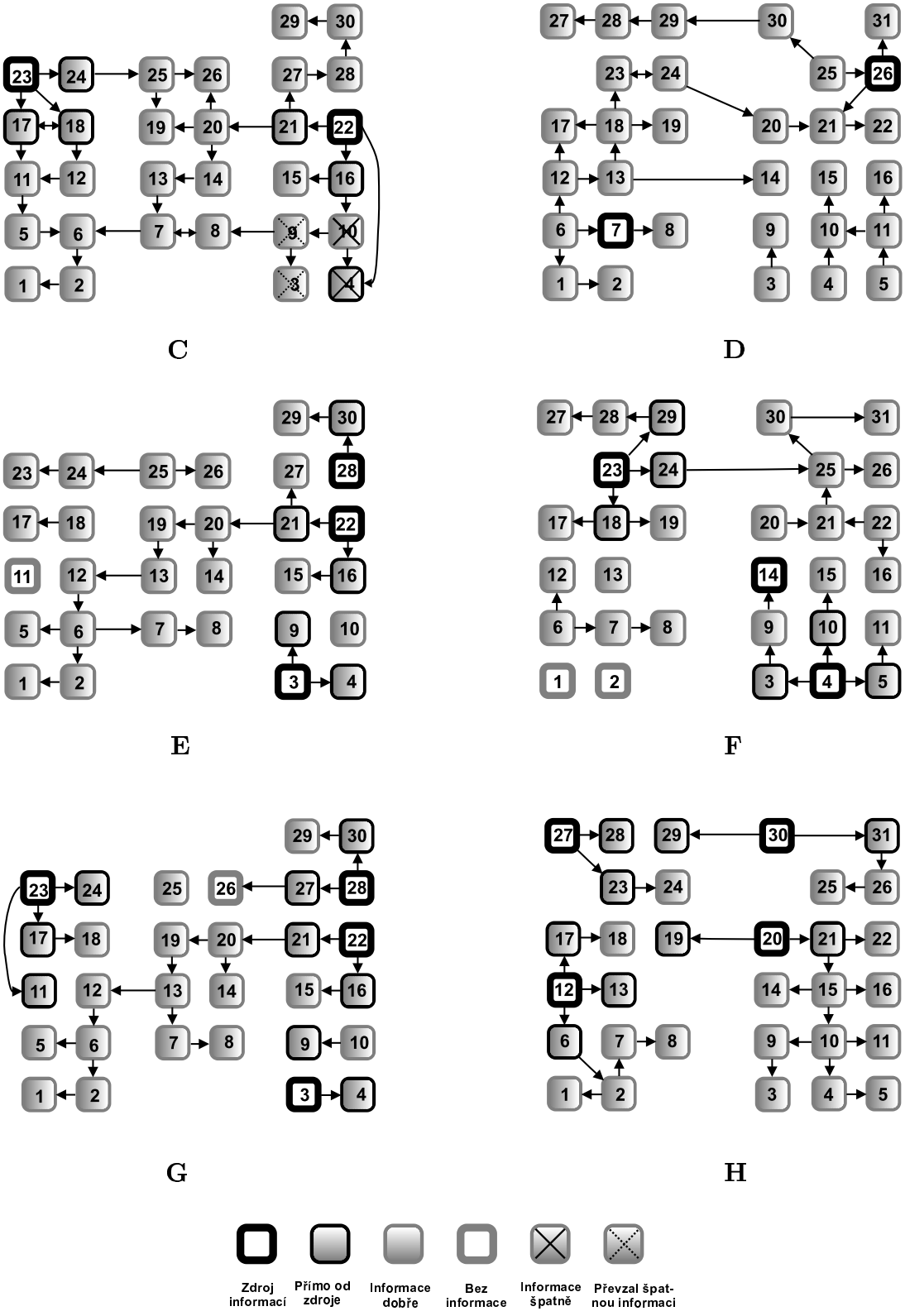
Fyzika	1. vzorek	2. vzorek
V*	26,7%	51,3%
VI*	14,7%	0,3%
I*	46,7%	21,0%
N*	3%	6,6%
Znal odpověď	**36,7%**	**51,4%**
Opsal	**46,7%**	**21,0%**
Napověděl	**7,6%**	**0,2%**

Tab. 7: Tabulky popisují průměrný počet odpovědí jednoho studenta, které opsal, věděl, nevěděl nebo věděl a zároveň dostal nápovědu v testech z deskriptivní geometrie a fyziky.

6.2 Šíření informace

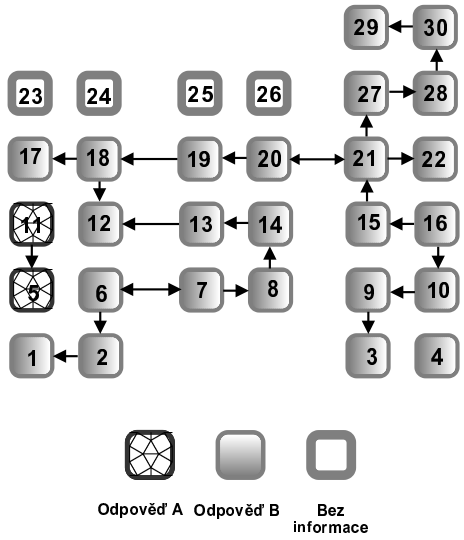
Pro zmapování cesty, jak se informace šířila po třídě, bylo provedeno měření na tzv. prázdných testech, které jsou popsány v kapitole 5.2 Testování studentů. Z výsledků byly sestaveny následující grafy, které znázorňují předávání informace od studenta ke studentovi. Došlo ke ztrátě informace o šíření, a to díky studentům, kteří nevyplnili značku, jak se k nim informace dostala.





Obr. 3: Grafy šíření informace. Grafy A, C, E a G odpovídají 1. vzorku studentů, grafy B, D, F, H 2. vzorku studentů, pro různý počet zdrojů správných odpovědí (A a B pro 1 zdroj, C a D pro 2 zdroje, E a F pro 3 zdroje, G a H pro 4 zdroje).

Nakonec je uveden graf šíření informace po třídě, aniž by někdo měl k dispozici správné řešení. Všichni studenti, kteří odpověděli na tuto otázku, označili shodně odpověď B kromě dvou studentů. Zdroj této klamné informace se nepodařilo zjistit.



Obr. 4: Šíření odpovědi na jednu otázku mezi studenty bez zdroje správné odpovědi.

Kapitola 7
Závěr

Výsledky testů

Z naměřených výsledků jsem zjistila, že studenti v prvním vzorku si výrazně zlepšili své průměrné výsledky v testech, při kterých si měli předávat informace. V druhém vzorku došlo oproti prvnímu kolu testů k poklesu průměrného počtu bodů. Studenti v těchto dvou vzorcích byli vybráni tak, aby měli stejné předpoklady pro úspěšné řešení testů, výběr se tak omezil na dvě paralelní třídy 2. ročníku technického lycea na SPŠ ST Panská v Praze. Již při školení byl patrný různý přístup studentů k probíhajícímu testování vzhledem k tomu, že výsledky testů byly započítávány do hodnocení jen první skupině studentů.

Tuto domněnku podpořil i jeden ze studentů z druhé skupiny se svým názorem:

> „Ten systém funguje, problém je v naprosté nefunkčnosti naší třídy. Navrhuji pro příště žáky nějak více přimět, aby spolupracovali a nebylo jim to fuk."

Předpokládám, že takový rozdíl způsobila naprostá ztráta motivace studentů a pravděpodobně i skutečnost, že v této třídě vyučuji.

Vzhledem k výsledkům testů na prvním vzorku je možné učinit závěr, že při zkoušení multiple-choice testem si studenti dokáží velice efektivně předávat informace bez vědomí učitele. Opačný výsledek v druhém vzorku byl pravděpodobně způsoben demotivací a laxního přístupu studentů při druhých testech, proto tento výsledek nemůže být započítán do hodnocení.

Vzhledem ke kvalitativně rozdílným výsledkům testů obou vzorků by nemělo smysl provádět testování hypotézy. Její závěr by neměl dostatečnou vypovídací hodnotu k celkové populaci studentů. Pro relevantní závěr by výzkum musel proběhnout na větším počtu vzorků.

Pro potvrzení výsledků z testování prvního vzorku by bylo vhodné zopakovat analogický test na větším počtu tříd s důrazem na zajištění stejných podmínek při testování tak, aby byla systematická chyba měření co nejmenší. Doporučuji, aby testy neprobíhaly mezi studenty, ke kterým má školitel nebo testující nějaký profesní vztah.

Šíření informace

Tato část testování bavila studenty nejvíce. Vyzkoušeli si na ní různé způsoby předávání informací bez vědomí učitele a byli upozorňováni na případné nedostatky a viditelné projevy komunikace. Zajímavá je rychlost, s jakou jsou studenti schopni si informaci předat. Čas potřebný k distribuci správných řešení po třídě byl ve všech případech maximálně 10 minut. Pro zajímavost, v jednom testu, kde dva byly dva zdroje informací, stačily pouhé 3 minuty na to, aby každý ve třídě získal správné řešení.

Pokud uvážíme, že by při psaní testů měli studenti několik minut zbývajícího času, mohou své výsledky velmi rychle zkonzultovat s ostatními. Tato práce by měla být přínosem do diskuze o vhodnosti používání multiple-choice testů. Je třeba zvážit, zda použití multiple-choice testů je vhodný prostředek pro získání informace o skutečných vědomostech studentů a nebo je vzhledem k malému množství přenášené informace studenti mohou lehce obejít.

Náměty pro další práci

Vzhledem k aktuálnosti tohoto tématu ve vztahu k celostátní maturitě by bylo zajímavé podobné měření uskutečnit na jedné či více třídách, které by byly sledovány po co nejdelší dobu, aby byl zaznamenán vývoj kolektivu studentů a jejich spolupráce.

Literatura

[1] Ekert, A., K.: *Quantum cryptography based on Bell's theorem*, Physical Review letters **67** (1991).

[2] Hála, V.: *Kvantová kryptografie*, Aldebaran bulletin, http://aldebaran.cz/bulletin/2005_14_kry.php, 20. 3. 2006.

[3] Jones, G. A., Jones, J. M.: *Information and coding theory*, Springer-Verlag, Londýn, 2000.

[4] Poe, E. A.: *Vraždy v ulici Morgue*, Mladá Fronta, nakladatelství ČSM, Praha, 1964.

[5] Shannon, A., D.: *A mathematical theory of communication*, The Bell System Technical Journal **27** (1948), 349–423, 623–656.

[6] Singh, S.: *Kniha kódů a šifer*, Dokořán, Praha, 2003.

[7] Tůma, J. a kol.: *Úvod do klasických a moderních metod šifrování*, Texty k přednášce na MFF UK, kód ALG082, 2004.

[8] The RSA Challenge Numbers, RSA Security, http://www.rsasecurity.com/rsalabs/node.asp?id=2093, 20. 3. 2006.

Dodatky

Dodatek A

Frekvenční analýza

Písmeno	Čeština	Slovenština	Angličtina	Francouzština	Němčina
A	8,99	9,49	7,96	7,68	5,52
B	1,86	1,9	1,60	0,80	1,56
C	3,04	3,45	2,84	3,32	2,94
D	4,14	4,09	4,01	3,60	4,91
E	10,13	9,16	12,86	17,76	19,18
F	0,33	0,31	2,62	1,06	1,96
G	0,48	0,4	1,99	1,10	3,60
H	2,06	2,35	5,39	0,64	5,02
I	6,92	6,81	7,77	7,23	8,21
J	2,1	2,12	0,16	0,19	0,16
K	3,44	3,8	0,41	0,00	1,33
L	4,2	4,56	3,51	5,89	3,48
M	2,99	2,97	2,43	2,72	1,69
N	6,64	6,34	7,51	7,61	10,20
O	8,39	9,34	6,62	5,34	2,14
P	3,54	2,87	1,81	3,24	0,54
Q	0	0	0,17	1,34	0,01
R	5,33	5,12	6,83	6,81	7,01
S	5,74	5,94	6,62	8,23	7,07
T	4,98	5,06	9,72	7,30	5,86
U	3,94	3,7	2,48	6,05	4,22
V	4,5	4,85	1,15	1,27	0,84
W	0,06	0,06	1,80	0,00	1,38
X	0,04	0,03	0,17	0,54	0,00
Y	2,72	2,57	1,52	0,21	0,00
Z	3,44	2,72	0,05	0,07	1,17

Tab. 8: Frekvence písmen v textech vybraných jazyků.

Dodatek B

Vigenèrův čtverec

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
26	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

Tab. 9: Šifrovací pomůcka pro Vigenèrovu šifru.

Dodatek C

Základní ASCII tabulka

	0	1	2	3	4	5	6	7	8	9
0	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT
1	LF	VT	FF	CR	SO	SI	DLE	DC1	DC2	DC3
2	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS
3	RS	US	SP	!	”	#	$	%	&	’
4	(	)	*	+	,	-	.	/	0	1
5	2	3	4	5	6	7	8	9	:	;
6	¡	=	¿	?	@	A	B	C	D	E
7	F	G	H	I	J	K	L	M	N	O
8	P	Q	R	S	T	U	V	W	X	Y
9	Z	[	\	]	ˆ	_	‘	a	b	c
10	d	e	f	g	h	i	j	k	l	m
11	n	o	p	q	r	s	t	u	v	w
12	x	y	z	{	—	}	˜	DEL		

LF = nový řádek	CR = konec řádku	ESC = escape
BEL = pípnutí	BS = backspace	TAB = tabulátor

Tab. 10: Prvních 128 znaků ASCII tabulky. Netisknutelné znaky jsou vyjádřeny zkratkami (velkými písmeny). Nejvýznamnější jsou uvedeny ve vysvětlivkách. Ostatní lze nalézt například na http://www.lookuptables.com/.

Přílohy

V této části budou především testy, které dostávali studenti středních škol ke zpracování.

- ukázka prázdného testu,
- ukázka znalostního testu 1. kola,
- ukázka znalostního testu 2. kola,
- pokyny studentům,

Test č. X

Tento test je k procvičení šíření informace po třídě. (Připraven 20. dubna 2006)

____ Otázka č. 1:

A A A *****,
B B B *****,
C C C *****,
D D D *****,

____ Otázka č. 2:

A A A *****,
B B B *****,
C C C *****,
D D D *****,

____ Otázka č. 3:

A A A *****,
B B B *****,
C C C *****,
D D D *****,

____ Otázka č. 4:

A A A *****,
B B B *****,
C C C *****,
D D D *****,

____ Otázka č. 5:

A A A *****,
B B B *****,
C C C *****,
D D D *****,

KONEC

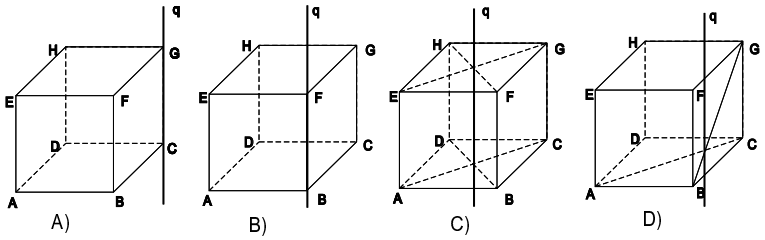
Test č. I – 1. kolo

Tento test je určen pro 2. ročníky. – Stereometrie. (Připraven 11. března 2006)

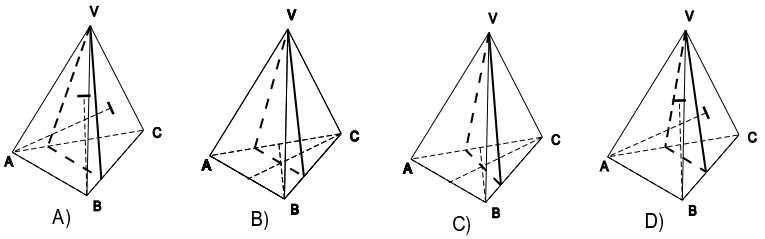
Otázka č. 1: (DG2ST1A)
Jsou dány mimoběžky a, b. Jakou polohu mají roviny $\rho,\ \sigma$, platí-li: $a \subset \rho \parallel b, b \subset \sigma \parallel a$? Proveďte důkaz. (2 body)

A) Roviny jsou různoběžné.
B) Roviny jsou kolmé.
C) Roviny jsou rovnoběžné.
D) Roviny jsou mimoběžné.

Otázka č. 2: (DG2ST2A)
Jsou dány přímky a, b, c z nichž každé dvě jsou mimoběžné. Přímkou a je vedena rovina α a přímkou b rovina β tak, aby $\alpha \cap \beta = q \parallel c$. Která z konstrukcí je správně, je-li dáno: $a =$ AC, $b =$ BG, $c =$ DH? (2 body)

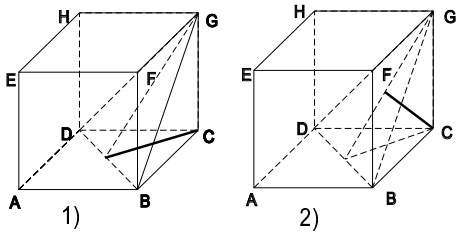


Otázka č. 3: (DG2ST4A)
Je dán jehlan VABC a težiště T stěny ABC. Přímkou VT je vedena rovina ρ tak, aby byla rovnoběžná s AB. Která z možností zobrazuje správně její průsek s jehlanem? (1 bod)



Otázka č. 4: (DG2ST5A)
Je dána krychle ABCDEFGH. Určete správnou konstrukci a vzdálenost vrcholu C od roviny BDG. Strana krychle $a = 4$. (2 body)

A) Vzálenost je $4\sqrt{\frac{1}{3}}$, konstrukce 2.
B) Vzálenost je $4\sqrt{\frac{1}{3}}$, konstrukce 1.
C) Vzálenost je $\sqrt{14}$, konstrukce 2.
D) Vzálenost je $\sqrt{14}$, konstrukce 1.



KONEC

Test č. III – 2. kolo

Tento test je určen pro 2. ročníky. – Fyzika. (Připraven 11. března 2006)

__ **Otázka č. 1:** (FY2721)
Rovnoměrně zrychlený pohyb přímočarý je definován:

A) A) A) konstantní rychlostí,
B) B) B) zrychlením konstantní velikosti a směru,
C) C) C) zrychlením u něhož je konstantní pouze směr,
D) D) D) zrychlením, u něhož je konstantní pouze velikost.

__ **Otázka č. 2:** (FY2722)
Jakou rychlostí dopadne na zem těleso padající volným pádem z výšky 10 m?

A) A) A) $10\,\mathrm{m}\cdot\mathrm{s}^{-1}$,
B) B) B) $98,1\,\mathrm{m}\cdot\mathrm{s}^{-1}$,
C) C) C) $1,02\,\mathrm{m}\cdot\mathrm{s}^{-1}$,
D) D) D) $14,1\,\mathrm{m}\cdot\mathrm{s}^{-1}$.

__ **Otázka č. 3:** (FY2723)
Síla o velikosti 5 N uděluje jistému tělesu zrychlení o velikosti $4\,\mathrm{cm}\cdot\mathrm{s}^{-2}$. Zvětší-li se velikost síly na 15 N, bude velikost zrychlení:

A) A) A) menší než $4\,\mathrm{m}\cdot\mathrm{s}^{-2}$,
B) B) B) $4\,\mathrm{m}\cdot\mathrm{s}^{-2}$,
C) C) C) mezi $4\,\mathrm{m}\cdot\mathrm{s}^{-2}$ a $8\,\mathrm{m}\cdot\mathrm{s}^{-2}$,
D) D) D) větší nebo rovna $8\,\mathrm{m}\cdot\mathrm{s}^{-2}$.

__ **Otázka č. 4:** (FY2724)
Cyklista i s kolem má tíhu o velikosti 800 N. Součinitel smykového tření mezi silnicí a pneumatikami kola je 0,01 a odporová síla vzduchu má velikost 5 N. Jede-li po vodorovné silnici rovnoměrně přímočaře, musí vyvinout sílu o velikosti:

A) A) A) 813 N,
B) B) B) 5 N,
C) C) C) 23 N,
D) D) D) 8 N.

__ **Otázka č. 5:** (FY2725)
Výkon výtahu, který zvedá zátěž o hmotnosti 400 kg do výšky 16 m za dobu 16 s je:

A) A) A) 322 W,
B) B) B) 16 kW,
C) C) C) 4 kW,
D) D) D) 160 kW.

__ **Otázka č. 6:** (FY2726)
Družice o hmotnosti m_{D} obíhá po kružnici kolem planety o hmotnosti m_{P} ve vzdálenosti h od jejího povrchu. Planetu považujte za kouli o poloměru R. Velikost oběžné rychlosti družice kolem planety je dána vztahem:

A) A) A) $v = \sqrt{\dfrac{\kappa m_{\mathrm{P}}}{R+h}}$,

B) B) B) $v = \sqrt{\dfrac{\kappa m_{\mathrm{D}}}{R+h}}$,

C) C) C) $v = \sqrt{\dfrac{\kappa m_{\mathrm{P}}}{R}}$,

D) D) D) $v = \sqrt{\dfrac{\kappa m_{\mathrm{D}}}{h}}$.

__ **Otázka č. 7:** (FY2727)
Kámen byl vržen svisle vzhůru rychlostí o velikosti $40\,m \cdot s_{-1}$. Za jakou dobu se vrátí zpět do místa, odkud byl vržen?

A) A) A) 2 s, B) B) B) 4 s.
C) C) C) 6 s, D) D) D) 8 s.

__ **Otázka č. 8:** (FY2728)
Fyzikální veličina moment setrvačnosti určuje:

A) A) A) rozložení hmoty v tuhém tělese vzhledem k ose otáčení,

B) B) B) míru otáčivých účinků síly na tuhé těleso,

C) C) C) polohu těžiště tuhého tělesa,

D) D) D) typ rovnovážné polohy tuhého tělesa.

__ **Otázka č. 9:** (FY2729)
Stabilita tělesa je určena:

A) A) A) těžištěm tělesa,

B) B) B) prací, jež je třeba vykonat k překlopení tělesa z rovnovážné polohy stabilní do labilní,

C) C) C) momentem tíhové síly vzhledem ke zvolené ose rotace,

D) D) D) momentem setrvačnosti tělesa.

__ **Otázka č. 10:** (FY27210)
Těleso ponořené v nestlačitelné kapalině je nahrazeno jiným tělesem o stejném objemu, ale jiné hmotnosti. Druhé těleso bude nadlehčováno:

A) A) A) touž silou, pouze pokud těžiště obou těles budou ve stejné hloubce,

B) B) B) silou přímoúměrnou tíze druhého tělesa,

C) C) C) silou přímoúměrnou tíze druhého tělesa a hloubce ponoření,

D) D) D) touž silou, nezávislou na tíze a hloubce ponoření druhého tělesa.

KONEC

Pokyny studentům k testům II. kola

Tyto pokyny si **pozorně** pročtěte nejméně jednou. Přečtěte si je také před začátkem každého testu. *Mějte je u sebe položené na lavici při psaní testů jako pomůcku.* Vyučující Vám nesmí tyto pokyny vzít, ani si je číst. Mohla by se tím narušit jejich objektivita při hodnocení testu.

Pokyny k vyplňování testu

Správnou odpověď **zakroužkujte** v nejlevějším sloupečku, odpověď, kterou považujete za *nesmyslnou*, **můžete zaškrtat** v nejlevějším sloupečku. **Zakroužkování neopravujte do stejného sloupečku!** Pokud budete odpověď měnit, kroužkujte/škrtejte do dalšího sloupečku v pořadí (celkem máte sloupečky tři). Dále mi ke každé otázce napište, jak jste k té konkrétní odpovědi dospěli a to pomocí níže navržených značek. Pro tyto značky je u každé otázky vyhrazeno místo před číslem otázky:

____ Otázka č. 50: ...

V následující tabulce jsou vyjmenované všechny značky, které používejte. Pokud otázku nestihnete zpracovat nebo ji přeskočíte, žádné značky neuvádějte.

Značka	Pozn.	Zkratka za	Význam
N		nevím/náhodně tipuji	Odpověď nevím, nedostala se ke mě.
V		vím	Odpověd vím i bez napovídání.
I		informace	Došla ke mě informace od spolužáků o správné odpovědi.
	*LS**	levý soused	Informaci jsem získal od levého souseda.
	*PS**	pravý soused	Informaci jsem získal od pravého souseda.
	*RS**	pRední soused	Informaci jsem získal od souseda přede mnou.
	*ZS**	zadní soused	Informaci jsem získal od souseda za mnou.
*Z**	*A**	informace od zdroje A	Dostal jsem informaci od zdroje A.
	*B**	informace od zdroje B	Dostal jsem informaci od zdroje B.

Vzor vyplnění jedné otázky testu:*

V, I RS **Otázka č. 50:**

ⓐ	A	ⓐ	*****
B	ⓑ	✗	*****
✗	C	C	*****
✗	✗	D	*****

U této otázky je řečeno, že odpověď víte (V), ale i tak jste dostal informaci (I) o správném výsledku a to od předního souseda (RS). Dále, že odpověď D, C a nakonec i B považujete za nesmyslnou a správně je odpověď A, ačkoliv jste se rozmýšlel mezi B a A.

* **Tuto značku v testu již nepoužívejte!**