Jméno: ..... **Datum:** .....

Spolupracoval(a): ..... **Třída:** .....

Pracovní list: Protokol BB84

Šifry hrají v dějinách lidstva důležitou roli už od starověku. S rozvojem moderních technologií je však čím dál více potřeba zaručit bezpečnost některých dat. Pravděpodobně byste totiž nebyli rádi, kdyby měl kdokoliv přístup k vašim heslům, bankovním údajům a jiným citlivým informacím.

Klasické šifrování

Jednou z klasických šifer, která byla používána již za dob Julia Caesara (1. století př. Kr.) a která po něm byla i pojmenována, je Caesarova šifra.

Úkol 1.1 Napište zprávu a pomocí Caesarovy šifry ji zašifrujte **podle** písmene **E**.

Jak použít Caesarovu šifru?

1. Do prvního řádku tabulky napište zprávu.
2. Pomocí tabulky 1 převeďte písmena ze zprávy na čísla a ta napište do příslušných buněk v druhém řádku tabulky.
3. Pomocí tabulky 1 určete číslo, které odpovídá písmenu, podle něhož šifrujete.
4. Do buněk ve třetím řádku pište součet čísla z buňky nacházející se nad ní a čísla odpovídajícímu písmeni, podle něhož šifrujete (pokud je součet větší než 25, odečtěte od něj 26).
5. K číslům z buněk třetího řádku najděte odpovídající písmena pomocí tabulky 1 a napište je do odpovídajících buněk ve čtvrtém řádku – tato písmena tvoří šifru.

zpráva													
číslo z.													
kód													
šifra													

A	0
B	1
C	2
D	3
E	4
F	5
G	6
H	7
I	8
J	9
K	10
L	11
M	12
N	13
O	14
P	15
Q	16
R	17
S	18
T	19
U	20
V	21
W	22
X	23
Y	24
Z	25

Tabulka 1 Pomůcka k Caesarově šifře

Úkol 1.2 Jak hodnotíte neprolomitelnost použité šifry? Proč?

Odpověď 1.2: .....

.....

.....

Caesarova šifra v tomto provedení je však poměrně snadno prolomitelná, a to i bez použití počítačů. Chtělo by ji trochu vylepšit a zamezit například tomu, aby se dané písmeno vždy nahrazovalo stejným písmenem – díky tomu bychom případným špionům znemožnili použití frekvenční analýzy, což je metoda, která k prolomení šifry využívá různých četností písmen užívaných přirozeně v jazyce.

Úkol 1.3 Napište zprávu a pomocí uvedeného klíče ji zašifrujte podobně jako u Caesarovy šifry.

Jak šifrovat?

Postupujte podobně jako u předchozího šifrování s tím rozdílem, že tentokrát šifrujete pomocí klíče tvořeného z různých písmen, nikoliv jen E. Proto do čtvrtého řádku tabulky zapište čísla, která odpovídají jednotlivým písmenům v klíči, a pro získání kódu poté sčítejte čísla z odpovídajících si buněk ve druhém a čtvrtém řádku tabulky.

zpráva																
číslo z.																
klíč	K	D	Y	E	L	H	B	P	F	A	H	Z	Y	Q	E	D
číslo k.																
kód																
šifra																

S tímto vylepším jsme sice zamezili užití některých metod, jimiž by šlo naše tajné sdělení odhalit, ale aby bylo naše počínání opravdu úspěšné je třeba překonat ještě několik komplikací.

Pro ztížení prolomení šifry potřebujeme dostatečně silný klíč. Jeho síla spočívá jednak v délce, která by v ideálním případě měla mít stejná jako délka šifrované zprávy, jednak v jeho náhodnosti. Čím náhodnější posloupnost písmen budeme mít, tím složitější bude dešifrovat tajné sdělení.

Velmi přirozeně tak vznikají nelehké otázky:

- Je možné takový klíč nějak efektivně vytvořit?
- Pokud by se nám podařilo nějakým způsobem takový klíč vytvořit, jakým bezpečným způsobem jej můžeme sdělit tomu, komu naši tajnou zprávu posíláme?
- A šlo by navíc nějak zjistit, zda jsme při tajném předávání vytvořeného klíče druhé straně nebyli náhodou odposlouchávání někým cizím?

Dobrá zpráva – ono to opravdu jde!

Kvantová kryptografie

S tímto problémem si poradili Charles H. **B**ennett a Gilles **B**rassard, kteří v roce 19**84** navrhli protokol BB84[1] a položili tak základy kryptografii, která využívá kvantovou fyziku. Abychom si i my mohli namodelovat vytvoření a předání klíče pomocí protokolu BB84, musíme nejdříve provést několik úmluv.

Od teď nadále budeme nazývat toho, kdo šifrovanou zprávu odesílá, **Alice** a toho, kdo zprávu od Alice přijímá, **Bob**. Kromě těchto dvou se pak ještě někdy objevuje „slídilka“ **Eva** snažící se Alici s Bobem odposlouchávat. Zároveň začneme písmena převádět na čísla ve dvojkové soustavě, tedy na sekvence nul a jedniček.

Přenos informace pomocí fotonu

Způsob zajišťující bezpečný přenos dat, kterého využijeme v protokolu BB84, je přenos pomocí fotonů. Každý foton může nést jeden bit informace, který je zakódován do směru polarizace fotonu. Jelikož jsou směry polarizace v jedné bázi navzájem kolmé, mohou být snadno rozlišeny.

Obdobně je možné v protokolu BB84 použít místo fotonů elektrony. V tomto případě bychom místo směru polarizace fotonu měřili průmět spinu elektronu do vybraných směrů, do něhož by byla zakódována informace.

báze	polarizace	bit
$+$	$\vert\updownarrow\rangle$	1
$+$	$\vert\leftrightarrow\rangle$	0
$\times$	$\vert\swarrow\!\!\nearrow\rangle$	1
$\times$	$\vert\nwarrow\!\!\searrow\rangle$	0

Tabulka 2 Přiřazení hodnot bitu jednotlivým polarizacím v obou bázích, které budeme používat

V našem měření ovšem využijeme fotony. Mějme tedy dvě báze. První z nich, kterou budeme označovat jako $+$, má směry polarizace $|\updownarrow\rangle$ a $|\leftrightarrow\rangle$, a druhá báze označená jako $\times$ má směry polarizace $|\swarrow\!\!\nearrow\rangle$ a $|\nwarrow\!\!\searrow\rangle$. Směrům polarizace v obou bázích přiřadíme hodnoty bitu 0 a 1 dle tabulky 2.

Úkol 2.1 Přepište sérii směrů polarizace $|\updownarrow\rangle\ |\swarrow\!\!\nearrow\rangle\ |\nwarrow\!\!\searrow\rangle\ |\updownarrow\rangle\ |\leftrightarrow\rangle\ |\nwarrow\!\!\searrow\rangle$ do posloupnosti nul a jedniček podle tabulky 2.

Řešení 2.1: .....

Úkol 2.2 Přepište sérii bitů 1 0 0 1 0 1 alespoň do dvou různých posloupností směrů polarizace podle tabulky 2.

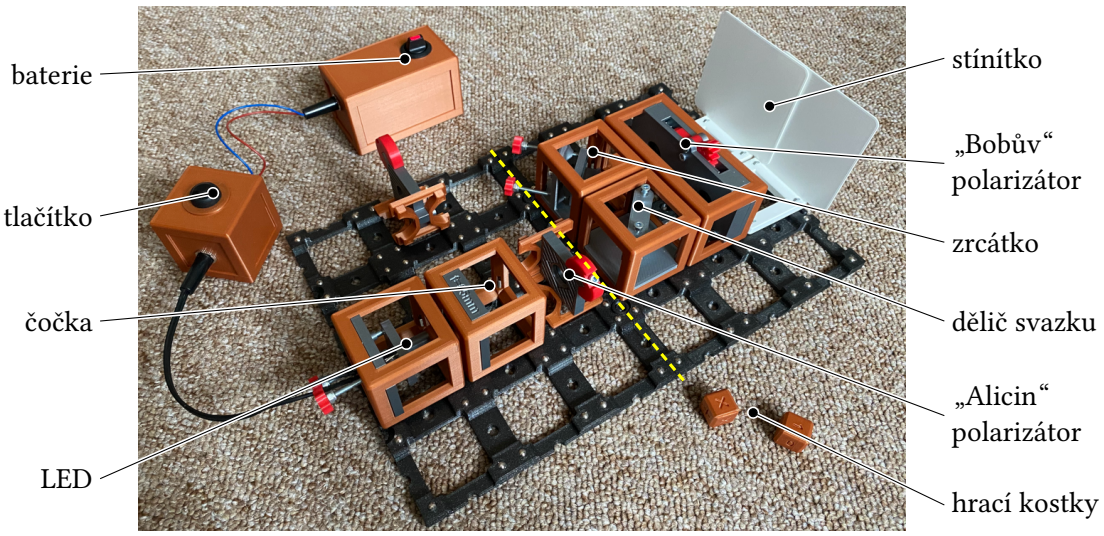
Řešení 2.2: .....

.....

V protokolu BB84 je náhodný výběr báze klíčový pro zajištění bezpečnosti. Proto je důležité, aby se používala co nejlepší metoda pro náhodný výběr, a zabránilo se tak předvídatelnosti – my použijeme hrací kostky.

Na následujících stránkách je sepsán detailní návod k provedení protokolu BB84. Za účelem tohoto úkolu pracujte ve dvou skupinách. Jedna skupina bude zastávat roli Alice (instrukce najdete na dvou následujících stránkách) a druhá roli Boba (další dvě stránky následující po Alici).

[1] Slovo protokol má v informatice význam způsobu komunikace nebo přenosu dat mezi dvěma body.

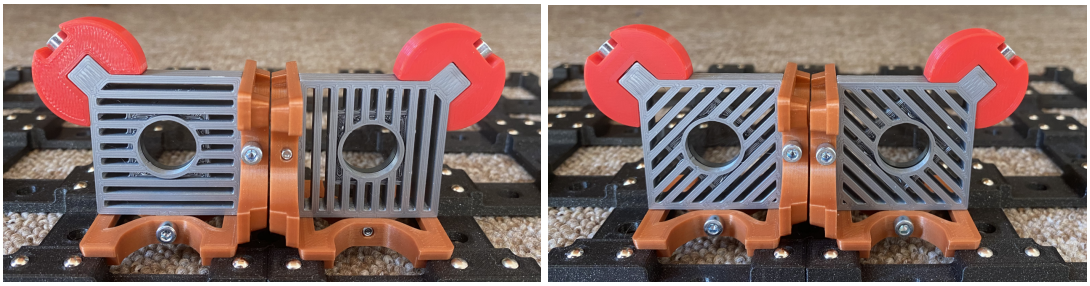


Obrázek 1 Fotografie sestavené aparatury (Alici patří část vlevo a Bobovi část vpravo)

Kromě stávajícího komunikačního kanálu s jednotlivými fotony jako nosiči informace, tedy aparatury z obrázku 1, je pro fungování protokolu zapotřebí ještě druhého kanálu. Tento kanál je veřejný a nemá žádné zvláštní technické požadavky. Ve skutečnosti by se mohlo jednat například o komunikaci prostřednictvím internetu nebo telefonické spojení. V našem modelu si však budeme příslušné informace jednoduše říkat.

Úkol 2.3 Podle obrázku 1 sestavte aparaturu. Následně postupně plňte úkoly 2.3–A1 a 2.3–A2 v roli Alice za současné spolupráce s Bobem plnícím úkoly 2.3–B1 a 2.3–B2, čímž provedete protokol BB84, při němž vygenerujete šifrovací klíč.

Alicina úloha



(a) Báze $+$, vlevo $|\leftrightarrow\rangle$ (bit 0) a vpravo $|\updownarrow\rangle$ (bit 1) **(b)** Báze $\times$, vlevo $|\swarrow\!\!\nearrow\rangle$ (bit 1) a vpravo $|\nwarrow\!\!\searrow\rangle$ (bit 0)

Obrázek 2 Všechny varianty nastavení „Aliciných“ polarizátorů

Úkol 2.3–A1 Pošlete Bobovi 20 bitů.

Jak poslat jeden bit?

1. Hoďte dvěma kostkami a vyberte tak náhodně bázi (buď $+$, nebo $\times$) a hodnotu bitu odpovídající jednomu z příslušných směrů polarizace (buď 0, nebo 1) dle tabulky 2.
2. Poznamenejte si do tabulky bázi a hodnotu bitu, které padly na kostkách
3. Podle toho, co padlo na kostkách umístěte odpovídající polarizátor ve správném směru na aparaturu.
4. Počkejte na Bobovo znamení a stisknutím tlačítka, které rozsvítí LED, pošlete „foton“.

měření	1	2	3	4	5	6	7	8	9	10
báze										
bit										
měření	11	12	13	13	15	16	17	18	19	20
báze										
bit										

Úkol 2.3–A2 Zapište klíč z vašeho měření.

Jak najít klíč?

1. Porovnejte s Bobem použité báze.
2. Pokud se báze pro dané měření neshodují, měření vyškrtněte. Pokud se shodují, měření ponechte.
3. Klíč, který tvoří posloupnost nul a jedniček (hodnot zaslaného bitu) u ponechaných měření, si zapište.

Klíč: . . . . . .

A	00001	1	J	01010	10	S	10011	19
B	00010	2	K	01011	11	T	10100	20
C	00011	3	L	01100	12	U	10101	21
D	00100	4	M	01101	13	V	10110	22
E	00101	5	N	01110	14	W	10111	23
F	00110	6	O	01111	15	X	11000	24
G	00111	7	P	10000	16	Y	11001	25
H	01000	8	Q	10001	17	Z	11010	26
I	01001	9	R	10010	18	Φ	11011	27

Tabulka 3 Kódování písmen do čísel ve dvojkové soustavě a převod do desítkové soustavy

Úkol 2.4–A Pomocí klíče[2] vygenerovaného protokolem BB84 zašifrujte zprávu. Následně ji zašifrovanou sdělte Bobovi.

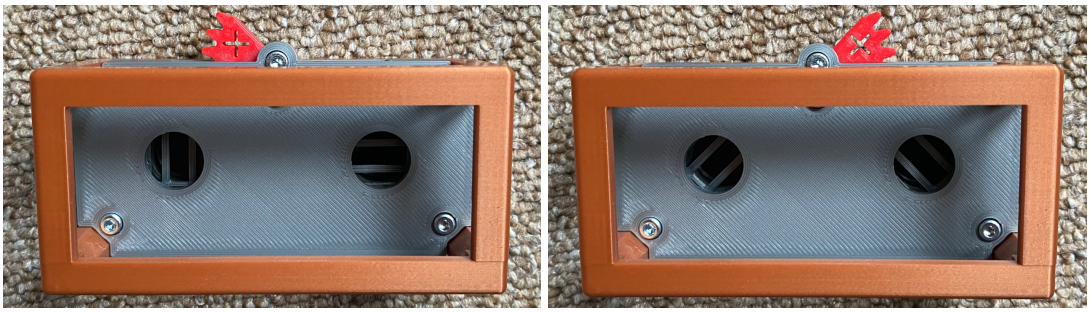
Jak zašifrovat zprávu?

1. Vyberte si čtyři písmena (to bude vaše zpráva), zapište je do prvního řádku tabulky.
2. Kódy písmen z tabulky 3 si poznamenejte do druhého řádku (vznikne vám 20členná posloupnost složená z nul a jedniček).
3. Do třetího řádku tabulky vpisujte opakovaně číslice klíče, dokud jej celý nezaplníte.
4. Do buněk čtvrtého řádku vpisujte číslice podle následujících pravidel: $0+0=0$, $1+0=0+1=1$ a $1+1=0$. U každé buňky přitom použijte dvě buňky nacházející se nad ní.

zpráva																				
kód																				
klíč																				
šifra																				

[2]Aby bylo možné jeden znak zašifrovat bezpečně, je třeba 5 bitů (alespoň v případě použití naší kódovací tabulky). Při 20 poslaných bitech a 50% pravděpodobnosti shody báze u Alice i Boba pak průměrně bude k dispozici 10 bitů. Pro pochopení principu tyto počty bitů postačují, v praxi by se však mělo přenést mnohem více bitů, aby byla délka klíče dostatečná (ideálně stejná jako délka zpráva).

Bobova úloha



(a) Báze $+$, vlevo $|\updownarrow\rangle$ (bit 1) a vpravo $|\leftrightarrow\rangle$ (bit 0) **(b)** Báze $\times$, vlevo $|\swarrow\!\nearrow\rangle$ (bit 1) a vpravo $|\nwarrow\!\searrow\rangle$ (bit 0)

Obrázek 3 Všechny varianty nastavení Bobova polarizátoru

Úkol 2.3–B1 Přijměte od Alice 20 bitů.

Jak přijmout bit?

1. Hoďte kostkou s bázemi a vyberte tak náhodně bázi (buď $+$, nebo $\times$).
2. Poznamenejte si do tabulky příslušnou variantu báze, která padla na kostce.
3. Nastavte „Bobův“ polarizátor podle toho, jakou bázi jste hodem kostky zvolili.
4. Dejte Alici znamení, aby stisknutím tlačítka odeslala bit.
5. Pokud je výsledek jednoznačný, zaznamenejte si do tabulky příslušnou hodnotu bitu dle tabulky 2. Pokud výsledek není jednoznačný a na stínítku vidíte dvě stejně jasné stopy, vyberte bit hodem kostky a zaznamenejte si jej do tabulky.

měření	1	2	3	4	5	6	7	8	9	10
báze										
bit										

měření	11	12	13	14	15	16	17	18	19	20
báze										
bit										

Úkol 2.3–B2 Zapište klíč z vašeho měření.

Jak najít klíč?

1. Porovnejte s Alicí použité báze.
2. Pokud se báze pro dané měření neshodují, měření vyškrtněte. Pokud se shodují, měření ponechte.
3. Klíč, který tvoří posloupnost nul a jedniček (hodnot zaslaného bitu) u ponechaných měření, si zapište.

Klíč: . . . . . .

A	00001	1	J	01010	10	S	10011	19
B	00010	2	K	01011	11	T	10100	20
C	00011	3	L	01100	12	U	10101	21
D	00100	4	M	01101	13	V	10110	22
E	00101	5	N	01110	14	W	10111	23
F	00110	6	O	01111	15	X	11000	24
G	00111	7	P	10000	16	Y	11001	25
H	01000	8	Q	10001	17	Z	11010	26
I	01001	9	R	10010	18	Φ	11011	27

Tabulka 4 Kódování písmen do čísel ve dvojkové soustavě a převod do desítkové soustavy

Úkol 2.4–B Pomocí klíče[3] vygenerovaného protokolem BB84 dešifrujte zprávu, kterou jste dostali od Alice.

Jak dešifrovat zprávu?

1. Do prvního řádku tabulky zapište zašifrovanou zprávu, kterou jste obdrželi od Alice.
2. Do druhého řádku tabulky postupně vpisujte klíč, dokud jej celý nezaplníte.
3. Do buněk třetího řádku vpisujte číslice podle následujících pravidel: $0 + 0 = 0$, $1 + 0 = 0 + 1 = 1$ a $1 + 1 = 0$. U každé buňky přitom použijte dvě buňky nacházející se nad ní.
4. Převeďte číselné kódy ze třetího řádku na písmena (vždy pětice číslic na písmeno), která zapište do čtvrtého řádku tabulky.

šifra																			
klíč																			
kód																			
zpráva																			

[3]Aby bylo možné jeden znak zašifrovat bezpečně, je třeba 5 bitů (alespoň v případě použití naší kódovací tabulky). Při 20 poslaných bitech a 50% pravděpodobnosti shody báze u Alice i Boba pak průměrně bude k dispozici 10 bitů. Pro pochopení principu tyto počty bitů postačují, v praxi by se však mělo přenést mnohem více bitů, aby byla délka klíče dostatečná (ideálně stejná jako délka zpráva).

Odhalení odposlechu v protokolu BB84

Poslední z otázek, které jsme si položili ještě před vstupem do kvantové kryptografie, byla zaměřena na odhalení Evy odposlouchávající Alici s Bobem. Nyní když už známe, jak při protokolu BB84 postupovat, pojďme přidat do celého procesu ještě Evu a pozorujme, jak se její snaha o získání klíče projeví.

Dejme tomu, že Eva zvládá zachytit fotony, které vysílá Alice Bobovi, ještě před tím, než dorazí k Bobovi a pomocí polarizačního filtru (u něhož stejně jako Bob nastavuje náhodně bázi) změří polarizaci fotonu. Jelikož však nechce být odhalena tím, že k Bobovi už žádný foton nedoletí, použije navíc svůj vlastní zdroj fotonů, na němž nastaví vždy takový směr polarizace, jaký právě naměřila.

Úkol 2.5 Alice Bobovi odeslala foton s polarizací $|\swarrow\nearrow\rangle$, tedy bit 1 v bázi $\times$, ten však zachytila Eva. Doplňte do tabulky s jakou pravděpodobností P naměří Eva jednotlivé směry polarizace, pokud měří v bázi $\times$, resp. $+$?

Eva dostala foton $\|\swarrow\nearrow\rangle$ a měří s bází $\times$			Eva dostala foton $\|\swarrow\nearrow\rangle$ a měří s bází $+$		
polarizace	**bit**	P	**polarizace**	**bit**	P
$\|\swarrow\nearrow\rangle$	1		$\|\updownarrow\rangle$	1	
$\|\nwarrow\searrow\rangle$	0		$\|\leftrightarrow\rangle$	0	

Úkol 2.6 Alice Bobovi odeslala foton s polarizací $|\swarrow\nearrow\rangle$, tedy bit 1 v bázi $\times$, ten však zachytila Eva, která měřila v bázi $+$. Eva změřila polarizaci $|\updownarrow\rangle$, tj. bit 1. Takto polarizovaný foton poslala dále Bobovi. Doplňte do tabulky s jakou pravděpodobností P změří Bob jednotlivé hodnoty bitu, měří-li v bázi $\times$?

Bob dostal foton $\|\updownarrow\rangle$ a měří s bází $\times$		
polarizace	**bit**	P
$\|\swarrow\nearrow\rangle$	1	
$\|\nwarrow\searrow\rangle$	0	

Na základě tohoto pozorování lze dojít k závěru, že pro kontrolu, zda nedošlo k odposlouchávání, porovnají Alice a Bob (veřejným kanálem) několik náhodně vybraných číslic ze svého klíče. Odposlech vede k rozdílům v obou klíčích a toto porovnání klíčů tedy umožňuje odhalení případného odposlechu. I v případě, že k odhalení nedošlo, se sdělené číslice z klíče odeberou, jelikož byly zveřejněny, a ze zbytku tak vznikne nový, zaručeně bezpečný klíč. V případě, že byl odhalen odposlech, je potřeba se odposlechu zbavit a provést celý přenos znovu.

Úkol 2.7 Jakou lze očekávat chybovost při porovnání klíčů Alice a Boba, pokud všichni tři (Alice, Eva a Bob) volí bázi pro každý foton naprosto náhodně?

Odpověď 2.7: . . . . . .

. . . . . .