KRY – protokol k prvnímu projektu

Ondřej Koumar, xkouma02 (241550)

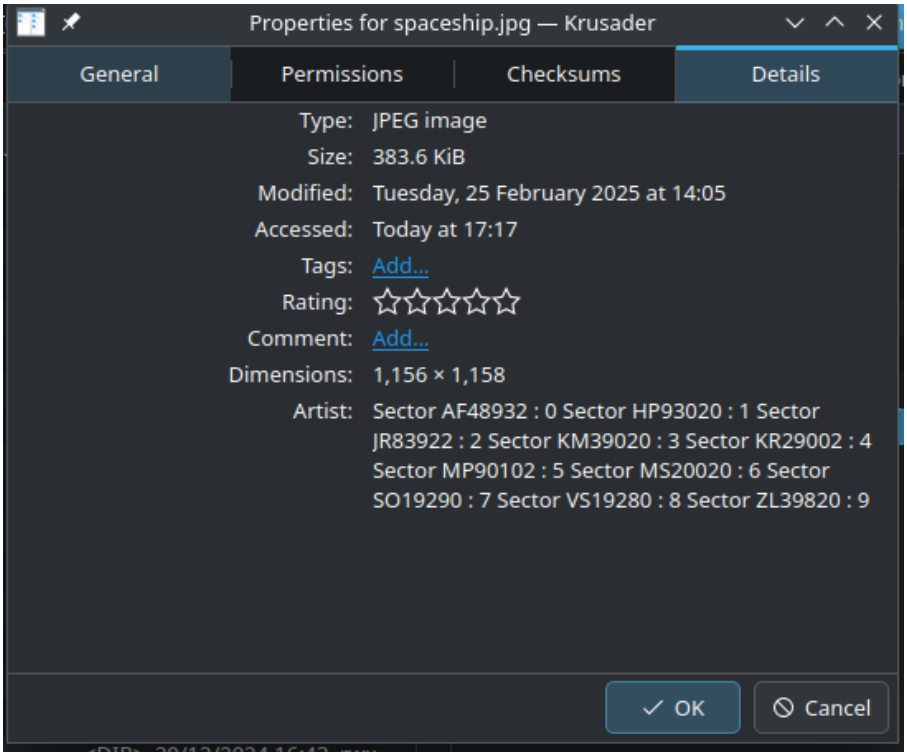
25. března 2025

1 Postup řešení

Jako první jsem potřeboval zjistit, jakou kódovou knihu použít pro dešifrování původních zpráv, které obsahovaly pouze znaky ve formátu `\xDD`, kde `D` je zástupný symbol pro libolnou číslici z množiny $\{0, \ldots, 9\}$. Na obrázku *spaceship.jpg* jsem si samozřejmě všimnul velkého nápisu *VUT ID MOD 10*. Naivně jsem si myslel, že jsem vyhrál a začal jsem dešifrovat, k čemuž jsem si napsal malý script v Pythonu. Disclaimer: asi to není nejčistší kód, ale svoji práci to dělá.

```
encryption = { # tento slovnik byl menen dle pouzivane kodove knihy
    "x08": "a",
    "x36": "b",
    "x54": "c",
          ⋮
    "x25": "zz"
}

i = 0
all_messages = ""
with open("../cipher.txt") as f:
    for line in f:
        decrypted_message = ""
        for encrypted_char in line.replace(',', '').strip().split():
            decrypted_char = encryption[encrypted_char]
            decrypted_message += decrypted_char
        print(f"ZP{i}: {decrypted_message}")
        all_messages += decrypted_message + "\n"
        i += 1
        decrypted_message = ""

list_of_messages = []
for message in all_messages.split('\n'):
    list_of_messages.append(list(message))

messages_csv_format = ""
for message in list_of_messages:
    for char in message:
        messages_csv_format += char + ';'
    messages_csv_format += '\n'

with open("output.csv", 'w') as f:
    f.write(messages_csv_format)
```

Po dešifrování zpráv kódovou knihou, kterou jsem vybral pomocí modulování mého VUT ID, jsem nedošel vůbec nikam. Dlouho mi trvalo, než jsem se přemluvil, abych přestal s dešifrováním zprávy a znovu se podíval, jestli jsem si vůbec vybral správnou kódovou knihu. Tento první pokus jsem prováděl metodou tužka-papír a snažil jsem se najít souvislosti mezi mezi písmenky – použil jsem



Obrázek 1: Schovaná přiřazení různých kódových knih podle zbytku VUT ID po dělení 10.

frekvenční analýzu a další metody, ze kterých jsem nic nezjistil. Bohužel už přesně nevím, co všechno jsem zkoušel, začínal jsem zhruba dva týdny před psaním této zprávy a nepamatuji si všechny své experimenty. Navíc, z frustrace jsem všechny papíry popsané neúspěšným prvním pokusem vyhodil.

Začal jsem se na situaci dívat *jinak*. Přesněji, na obrázek *spaceship.jpg* jsem se začal dívat jinak. Bylo mi jasné, že v něm musí být schované něco, co bych mohl využít. Po pár minutách jsem usoudil, že samotné hledání detailů na obrázku nemá smysl a zkusil jsem se podívat do vlastností samotného souboru. Co jsem našel je ukázáno na Obrázku 1.

Bylo mi tedy jasné, že musím opravdu svoje VUT ID vydělit 10, ale poté vybrat kódovou knihu, na základě zbytku po dělení, z rozdělení definovaného v sekci *Artist*. Protože zbytek po dělení mého VUT ID 10 je 0, vybral jsem kódovou knihu *Sector AF48932*. Zprávy po dešifrování kódovou knihou jsou v Tabulce 1.

Číslo zprávy	**Dešifrovaná zpráva**
ZP0	rmxesxzoxvaotyhntaaolsntvienaiernovsceolaviptemppbztnnoueelr
ZP1	nixctxisxajxattirecovziiaeieaemdtnpltackikobeunlaaxtaxszxnta
ZP2	vxapmxrixeakkimurhopixruave2nv0edmanrtlcttyiiksemnlnmeaaciye
ZP3	dlxyyxbvxnexsyacaeesdvvsnecdckykehdkoknynpnaareaspvavltoevao
ZP4	unvosxtaaieaeulaedknockierlattniompfollvkptsapeizninjreuprer
ZP5	vexhdxaaxorxoanmnlrvaflyckzanneaeaiofntjaranoloehietyaotdebp
ZP6	eznimxvainaleirranptendettolcreibikaaanjosstankaspaeditebert
ZP7	ikxiuxnnxlcxrhyratolupitznctpaiinavobcoatmriroofnccuaxohenaa

Tabulka 1: Zprávy po prolomení substituční šifry pomocí kódové knihy.

Tímto momentem jsem se dostal do fáze lámání zašifrovaného textu. Druhá část projektu šla mnohem rychleji než první. Když se podíváte na skript, který jsem si pro potřeby řešení tohoto

projektu vytvořil, zjistíte, že všechny dešifrované zprávy ukládám bez jakýchkoliv dalších informací do *.csv* souboru. Tento *.csv* soubor jsem si otevřel v tabulkovém procesoru s myšlenkou, že se mi v něm bude lépe pracovat než na papíře. Trvalo mi jen pár minut zjistit, že to byl lepší nápad, než jsem původně očekával. To díky možnosti hýbat s celými sloupci v tabulkových procesorech (možná je to čtenáři dlouho známý fakt, ale pro mě to byla úplná novinka), navíc šifra byla postavená tak, že se dala vyřešit přeskupováním sloupců a postupným doplňováním slov tak, aby dávaly smysl. Jak to v tabulkovém procesoru vypadalo je ukázáno na Obrázku 2.

	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	AA	AB	A
1	r	m	x	e	s	x	z	o	x	v	a	o	t	y	h	n	t	a	a	o	l	s	n	t	v	i	e	n	a
2	n	i	x	c	t	x	i	s	x	a	j	x	a	t	t	i	r	e	c	o	v	z	i	i	a	e	i	e	a
3	v	x	a	p	m	x	r	i	x	e	a	k	k	i	m	u	r	h	o	p	i	x	r	u	a	v	e	2	n
4	d	l	x	y	y	x	b	v	x	n	e	x	s	y	a	c	a	e	e	s	d	v	v	s	n	e	c	d	c
5	u	n	v	o	s	x	t	a	a	i	e	a	e	u	l	a	e	d	k	n	o	c	k	i	e	r	l	a	t
6	v	e	x	h	d	x	a	a	x	o	r	x	o	a	n	m	n	l	r	v	a	f	l	y	c	k	z	a	n
7	e	z	n	i	m	x	v	a	i	n	a	l	e	i	r	r	a	n	p	t	e	n	d	e	t	t	o	l	c
8	i	k	x	i	u	x	n	n	x	l	c	x	r	h	y	r	a	t	o	l	u	p	i	t	z	n	c	t	p

Obrázek 2: Náhled na práci se zašifrovanými zprávami v tabulkovém procesoru. Část šifer je uříznuta, aby se obrázek pohodlně vlezl na šířku stránky a zároveň byl čitelný.

Když se podíváme na zprávu *ZP2*, najdeme v ní, jako jediné, čísla. Jsou to stejná čísla, která mám v xloginu, proto jsem svoji práci začal sestavením xloginu tak, aby písmena v jiných řádcích také dávala smysl, což se po pár pokusech podařilo. Prozatím jsem jej ponechal na začátku řádku s tím, že v případě potřeby jej přehodím jinam, nicméně nakonec tam zůstal, před něj už žádný sloupec nešel.

Postupně jsem zprava skládal sloupce, dokud jsem se na chvíli nezasekl, protože jsem měl vícero možností, které by dávaly smysl. Abych zredukoval počet těchto možností, začal jsem skládat od konce. Všiml jsem si, že v každém řádku je několik písmenek `x`, v jednom sloupci byly dokonce ve všech řádcích. Napadlo mě, že sloupec s `x` na konci by mohl značit konec řádku nebo něco podobného a zkusil jsem jej dát na konec. Poté jsem si všiml sloupců, ve kterých bylo písmenek `x` dost, i když ne všechny. Dospěl jsem k tomu, že každý řádek bude jinak dlouhý a `x` na konci budou výplní, aby všechny zprávy byly stejně dlouhé. Po pár minutách zkoušení a přehazování jsem se dostal do fáze, kdy písmenka na koncích řádků začala vypadat jako části slov. V tu chvíli už skládání šlo opět rychle. Tímto způsobem jsem pokračoval, dokud jsem celou šifru neměl poskládanou tak, aby dávala smysl. Pokud v ní byl nějaký sofistikovanější systém, který se dal najít, já ho nenašel.

1.1 Shrnutí

Pří řešení projektu jsem dešifroval původní zprávy ve dvou krocích. V prvním kroku jsem překonal substituční šifru, která byla realizována kódovou knihou. Druhý krok byl lámání transpoziční šifry. Během řešení jsem nepřišel na přesný systém, kterým jsou sloupce přeházeny, projekt jsem vyřešil pomocí posouvání sloupců doleva a doprava, dokud písmenka začala dávat smysl a postupným přidáváním dalších sloupců ke zprávě zprava. Paralelně jsem skládal zprávu od konce, protože jsem si všiml spousty písmenek `x`, pomocí kterých se mi povedlo dát dohromady části slov na koncích řádků. Mezi těmito dvěma částmi jsem přeskakoval, když jsem měl vícero možností, jak pokračovat.

2 Dešifrované zprávy v plaintextové podobě

Číslo zprávy	**Dešifrovaná zpráva po prolomení transpoziční šifry**
ZP0	`stanovenecilepotvrzenyotviramepalbunamosthlasenipotvrzenoxxx`

Číslo zprávy	**Dešifrovaná zpráva po prolomení transpoziční šifry**
ZP1	zacinameutoknastanicitorpedanabitazajistitvelitelcekaxxxxxxx
ZP2	xkouma02krycimanevrpripravenstitynamaximumihnedvelitelcekaxx
ZP3	vsechnydronyvstandbyvysadekcekanapovelvysadekcekanapovelxxxx
ZP4	cekamenapotvrzeniutokunepritelskenujenasilodflotilapripravax
ZP5	formacealfajehotovahlavnikanonnabityreadynalozenetorpedaxxxx
ZP6	nepritelnasjestenevidtaktickatorpedazamerenaobranastabilnix
ZP7	prorazitobrannouliniihlavnipocitachacknutyutocnaformacexxxxx

Tabulka 2: Dešifrované zprávy po prolomení substituční šifry (kódová kniha) a transpoziční šifry.