MASARYKOVA
UNIVERZITA

FAKULTA INFORMATIKY

Analýza a predikce herních informací

Diplomová práce

BARBORA ELIÁŠOVÁ

Brno, jaro 2023

MASARYKOVA
UNIVERZITA

FAKULTA INFORMATIKY

Analýza a predikce herních informací

Diplomová práce

BARBORA ELIÁŠOVÁ

Vedoucí práce: doc. RNDr. Aleš Horák, Ph.D.

Katedra strojového učení a zpracování dat

Brno, jaro 2023


FACULTAS ARTIS INFORMATICÆ
UNIVERSITAS MASARYKIANA

Prohlášení

Prohlašuji, že tato diplomová práce je mým původním autorským dílem, které jsem vypracovala samostatně. Všechny zdroje, prameny a literaturu, které jsem při vypracování používala nebo z nich čerpala, v práci řádně cituji s uvedením úplného odkazu na příslušný zdroj.

Barbora Eliášová

Vedoucí práce: doc. RNDr. Aleš Horák, Ph.D.

Poděkování

Chtěla bych poděkovat příteli a rodině za neustálou podporu a trpělivost. Dále společnosti Cryptomania za poskytnutá data, pochopení a prostor pro práci. Doc. RNDr. Aleši Horákovi, Ph.D. za cenné rady a poznámky. A nakonec organizátorům šifrovacích her, kteří zveřejňují použité šifry, a tak se z nich mohou učit hráči i predikční modely.

Shrnutí

Práce představuje nástroj pro predikci využití nápovědy na trase šifrovací hry společnosti Cryptomania s.r.o. V rámci práce byla vytvořena neuronová síť, která na základě informací o týmu, hře a šifře určí, zda tým během řešení následující šifry požádá o nápovědu. Pro vytvoření této predikce slouží primárně klasifikátor obtížnosti šifry, který obrazovému zadání přiřadí vektorovou reprezentaci zohledňující obtížnost. Výsledný nástroj je prezentován ve formě webové aplikace, která zobrazí dosavadní průchod týmu a pravděpodobnost, že na následující šifře využije nápovědu. Zároveň dokáže vizualizovat obecné trendy během řešení šifer.

Klíčová slova

šifrovací hra, predikce nápovědy, neuronová síť, predikce obtížnosti úlohy

Obsah

Seznam tabulek

Seznam obrázků

Seznam zkratek

C5 Czech Colossal Clean Crawled Corpus 14

CTDC Czech Text Document Corpus 15

DCGAN Deep Convolutional Generative Adversarial Network 12, 13, 39, 57

FERNET Flexible Embedding Representation NETwork 14

GAN Generative Adversarial Network 13

MLM Masked Language Modeling 14

NSP Next Sentence Prediction 14

RTP Recent temporal patterns 5, 6

SVM Support vector machine 5, 6, 13

Úvod

Práce se věnuje tématu šifrovacích her. Konkrétně se zaměřuje na využití nápovědy během nich. Tyto hry jsou velmi specifickou formou zábavy kombinující prvky orientačního běhu a bojovky známé z dětských táborů. Obvykle mají hráči za úkol projít předem neznámou trasu a dostat se co nejrychleji do cíle. Polohu následujícího stanoviště se vždy dozví až po vyřešení šifry, kterou mají právě před sebou.

Nejstarší šifrovací hrou v České republice je noční brněnská TMOU[1], pořádaná spolkem Instruktoři Brno[2] od roku 2000 [1]. Ti se pro její tvorbu inspirovali závodem *Open Blood*, který probíhá od konce 90. let. Závod je nicméně primárně koncipován jako orientační běh po Vysočině a šifry v něm hrají jen malou roli [2]. TMOU se následně inspirovala řada dalších her, např. brněnská DNEM[3] či pražská Bedna[4] a MATRIX[5].

Ve světě se zdá být nejstarší *MIT Mystery Hunt*[6], který probíhá od roku 1981 v kampusu Massachusetts Institute of Technology. Hra typicky trvá 48 hodin a úkolem týmů je nalézt „minci“ (*coin*) schovanou někde v prostoru kampusu. Některé ročníky obsahovaly až 200 šifer (TMOU má obvykle 15-20 úkolů a trvá 19 hodin) a týmy čítají jednotky až stovky hráčů (oproti tomu české hry mají většinou striktní omezení na maximálně pět hráčů v týmu [3]) [4]. *Mystery Hunt* je pořádán studenty univerzity primárně pro ostatní studenty univerzity, šifry a úkoly tedy mohou využívat odborné znalosti, které jsou na univerzitě běžné. České šifrovací hry oproti tomu zpravidla znalosti na takové úrovni nevyžadují, to ovšem neznamená, že hráči nemusí informace dohledávat nebo že nejsou ve výhodě, pokud mají vědomostí více.

Popsané šifrovací hry se všechny řadí do kategorie tzv. „velkých her“. Hra se vždy koná v konkrétní, předem daný, čas a je odstartována jako závod, trvá déle než osm hodin, obtížnost šifer není příliš omezována, dokonce se výjimečně mohou vyskytnout šifry, které je

1. `https://www.tmou.cz/`
2. `https://www.instruktori.cz/`
3. `https://www.chameleonbrno.org/dnem/`
4. `https://www.bedna.org/`
5. `https://matrix.velkyvuz.cz/archiv`
6. `http://puzzles.mit.edu/`

nemožné vyluštit. Hráči často nemají možnost požádat o nápovědu a většina týmů hru nedokončí (např. TMOU 23, která proběhla na začátku listopadu 2022 dokončily 4 týmy z 263, které odstartovaly [5]). Hráči těchto her chtějí většinou překonat sami sebe a účastní se kvůli silnému zážitku [6].

Dalším typem her jsou ty vytvářené pro komerční využití. Ty tvoří poměrně malé odvětví, kde hra má být výzva, nicméně zároveň musí být příjemná a v porovnání s „velkými hrami“ rychlá (přibližně do tří hodin herního času). Autoři těchto her se snaží zanechat v hráčích pozitivní dojem ze hry, protože hráči jsou zároveň klienty firmy [7]. Šifry, ze kterých se tyto komerční hry skládají, mají výrazně nižší obtížnost. Hry zároveň obvykle obsahují několik nápověd ke každé šifře, každý tým má tedy možnost projít celou hru. Oproti „velkým hrám“ je možné odstartovat téměř kdykoliv a během hry není na trase žádný z organizátorů, celá je řízena online herním systémem.

Vzhledem k tomu, že organizátoři nemají možnost sledovat náladu hrajícího týmu a v případě potřeby mu poskytnout nápovědu, bylo by vhodné, aby tuto roli zastal herní systém. Pokud tým požádá systém o nápovědu, pravděpodobně vyčerpal své možnosti a neví si s šifrou rady, což snižuje zážitek ze hry. Pokud by systém dokázal tuto událost predikovat, mohl by nápovědu nabídnout o něco dříve a potenciálně zabránit zaseknutí týmu. Na druhou stranu, vyřešení šifry bez nápovědy je otázka intelektuální hrdosti hráčů a nabídka nápovědy by některé týmy mohla urazit.

Zda tým nápovědu využije, závisí na mnoha proměnlivých či subjektivních faktorech, jako je například počasí nebo únava hráčů. Nicméně na potřebu nápovědy má přímý vliv i obtížnost šifry. Spolehlivě určit obtížnost šifry lze pouze testováním. Šifra je obecně považována za obtížnou, pokud výraznému množství týmů trvá dlouho ji vyřešit nebo pokud výrazné množství týmů požádá o nápovědu. Co znamená „výrazné množství týmů“ a „dlouhá doba řešení“ však záleží na autorech šifry a jejím zamýšleném použití. Pro „velkou šifrovací hru“ je hodina řešení přijatelná [5], šifra s komerčním využitím by neměla překročit dvacet minut. Stejně tak tolerance k počtu týmů, které šifru samy nevyřeší, je odlišná. Například TMOU obvykle žádné nápovědy neposkytuje [6] a jejich testovací týmy jsou pravidelně složeny z tvůrců vlastních šifer a zkušených hráčů, pro které není obtížnost šifry překážkou (jedním z testerů bývá například Martina Pomikálková, která je

momentálně (květen 2023) 16. nejlepší hráč podle statistik na stránce Šifrovačky.cz) [5][8]. Pokud šifru vyřeší alespoň jeden testovací tým, může být do hry zařazena. Oproti tomu, pokud mají dva testovací týmy z pěti problém se stejným krokem řešení komerční šifry, autoři mají tendenci ji upravit [7].

Cílem práce je na základě předchozího chování týmu a informací o šifře predikovat, zda tým využije nápovědu během hraní šifrovací hry společnosti Cryptomania. K tomu bude využita automatická klasifikace obtížnosti zadání šifry, záznam chování ostatních týmů a dosavadní postup daného týmu hrou. Výsledný model bude prezentován formou webového systému, který vizualizuje chování týmů během hry a následně pro zvolený tým a šifru určí pravděpodobnost, že tým o nápovědu požádá.

První kapitola se věnuje přehledu řešených projektů na podobné téma a následně pokročilým nástrojům, které by mohly být pro predikci vhodné. V kapitole 2 jsou podrobně popsána využitá data a jejich zdroje. Tato data jsou poté v další kapitole využita ke klasifikaci obtížnosti obrazového zadání šifry a tato klasifikace následně spolu s popsanými daty slouží jako vstup modelu, který predikuje, zda tým nápovědu využije. Výsledky vzniklých modelů jsou poté v následující kapitole analyzovány. Kapitola 6 popisuje webové rozhraní, které prezentuje chování týmů na trase hry, a zároveň slouží jako nástroj pro zobrazení predikce využití nápovědy modelu prezentovaného dříve. Nakonec jsou v kapitole 7 popsány nástroje a knihovny využité při tvorbě modelů a rozhraní. Vzhledem k tomu, že názvosloví běžně používané komunitou je v anglickém jazyce, byla pro lepší srozumitelnost většina termínů uvedena v českém i anglickém jazyce.

1 Rešerše

O odhadu obtížnosti hry bylo publikováno mnoho různých studií, nicméně princip těchto her a metriky, které lze měřit, jsou rozdílné. Například van Kreveld [9] použil vlastní webovou implementaci logických her Flow[1] (cílem je propojit body stejné barvy tak, aby se jednotlivé barevné dráhy neprotínaly), Move (několik bodů různých barev, hráč určuje směr, kam se vždy všechny naráz pohnou, cílem je každý z nich dopravit na pole odpovídající barvy) a Lazors[2] (nastavování zrcadel laserovému paprsku tak, aby prošel zadaným bodem). Pro odhad obtížnosti úkolů u tohoto druhu her byla měřena například velikost území, které má hráč k dispozici, počet barev, kterými operuje, nebo počet tahů potřebných k vyřešení. U zadání šifry lze kvantitu měřit také, nicméně je nejasné jakou veličinu měřit. Nabízí se využití délky textu v šifře, nicméně se nezdá, že by tato tato metrika byla rohodující. Například hra Sendvič obsahuje každý rok šifru s názvem Mlha [10]. Tato šifra měla v roce 2021[3] i 2023[4] čtyři řádky textu (51 a 34 slov). Starší zadání bylo vyřešeno jedním procentem týmů, zatímco novější variantu překonalo 83% týmů [10]. Oproti tomu šifru Steganosaurus[5] ze hry TMOU, která obsahuje 635 slov, úspěšně překonaly všechny týmy, které ji řešily [11].

Hry, které studuje Szabó a spol. [12], jsou edukativního charakteru a v podstatě představují gamifikovaný kvíz. Autoři popisují vlastní hru, kde hráči za správné odpovědi sbírají cihličky své barvy a staví z nich zeď. Obtížnost úlohy je měřena poměrem počtu úspěšných a neúspěšných řešení, což se zdá být šifrovací hře blízké. Edukativní hry však úkol ukončí při zadání jakékoliv odpovědi, oproti tomu při řešení šifry tým zadává své odpovědi do té doby, než objeví tu správnou. Vzhledem k tomu, že informace o špatných odpovědích není v datasetu dostupná, nelze s touto veličinou pracovat.

Popsané výzkumy se zabývají odhadem obtížnosti, nicméně tyto hry mají se šifrováním jen velmi málo společného. Na druhou stranu, čím vzdálenější jsou šifrovací hry od her v běžném slova smyslu, tím

1. https://www.bigduckgames.com/flowfree
2. https://pyrosphere.net/lazors/
3. https://www.hrasendvic.cz/2021/data/sada4.pdf
4. https://www.hrasendvic.cz/2023/data/sada4.pdf
5. https://archiv.tmou.cz/_media/2018/sifry/1-51-steganosaurus.pdf

více se blíží intelektuálním problémům, se kterými se setkávají například studenti matematiky, či informatiky.

1.1 Predikce doby řešení úlohy

Predikcí úspěchu studentů při řešení úlohy se zabývá Radek Pelánek [13]. Na základě předchozích výkonů daného studenta a jeho kolegů predikuje čas, který student stráví řešením konkrétního problému. Jeho model tak spojuje schopnost studenta řešit problémy a čas, který k tomu potřebuje.

Pravděpodobnost, že student vyřeší daný problém v logaritmu času t, definuje normálním rozdělením se střední hodnotou $b + a\theta$ a rozptylem c^2, je tedy definována takto:

$$f_{a,b,c,\theta}(\ln t) = \mathcal{N}(a\theta + b, c)(\ln t) = \frac{1}{\sqrt{2\pi}c} e^{-\frac{(\ln t - (a\theta+b))^2}{2c^2}},$$

kde θ je schopnost studenta řešit problém. Pro správnou funkci modelu zavedli normalizaci: pro množinu parametrů problému a_i, b_i, c_i a studentské parametry θ_j musí platit, že střední hodnota θ_j je 0 a střední hodnota a_i je -1. Počet neznámých parametrů Pelánek iterativně odhaduje a upřesňuje podobně jako při sdružené metodě maximální věrohodnosti pro teorii odpovědi na položku(*item response theory*).

Základní úroveň (*baseline*) byla stanovena jako průměrný čas potřebný k vyřešení úkolu a představený model dokázal tento odhad překonat o 5–80% v závislosti na obtížnosti úlohy – čím jednodušší úloha (např. bludiště), tím menší zlepšení. Cílem autorů bylo primárně předložit studentovi zadání s adekvátní obtížností (kterou definují jako čas, který student úlohou stráví). Systém neposkytuje nápovědy, student tedy úlohu buď dokončí, nebo vzdá.

1.2 Predikce úspěchu a potřeby asistence

Další pohled na predikci úspěchu studentů představuje Ye Mao [14]. Ta využívá dolování častých vzorců (*Recent temporal patterns* (*RTP*) [15]) v kombinaci se *Support vector machine* (*SVM*) [16] a logistickou regresí, aby predikovala úspěch studentů a to, zda budou mít potíže

během plnění programovacích úloh. Pro tyto predikce využívá data z kurzu „*introduction to computers*“ v letech 2016 a 2017 na North Carolina State University, které zaznamenalo prostředí *iSnap* [17]. To umožňuje sledovat postup studentů při řešení úlohy, pravidelně zaznamenává studentův zdrojový kód a zároveň nabízí nápovědu. Ta je automaticky generována pomocí algoritmu *SourceCheck* [18] na základě dat studenta.

Pro účely predikce je úspěch studenta definován jako „dokončení úlohy za hodinu či méně a zisk plného počtu bodů“. Model má k dispozici prvních n minut studentova řešení (záznam vývoje kódu) a predikuje, zda bude práce úspěšně dokončena kdykoliv mezi n-tou a 60. minutou.

Vzhledem k tomu, že studenti často neumí požádat o pomoc, nebo neví, že ji potřebují, nelze potíže definovat na základě této žádosti. Namísto toho jsou potíže studenta definovány jako stav, kdy „v kterémkoliv okamžiku neučiní žádný pokrok na svém nedokonalém, či chybném řešení po dobu pěti minut“. Na základě záznamu o aktivitě studenta během prvních n minut model predikuje zda se student během následujících pěti minut dostane do potíží. Záznam je pak tvořen sérií kliknutí, která jsou převedena na seznamy fixních rysů (*features*). Tyto rysy byly definovány experty (*expert-based feature set* – EF) a na základě jejich definic vznikla další sada, která je generována automaticky (*data-driven feature set* – DDF).

Při dolování vzorců (RTP) jsou nejprve binární časové řady (záznam práce studenta) převedeny na sekvence časových intervalů, z nichž jsou extrahovány časté vzorce pro třídy dat (uspěl/neuspěl). Každý záznam studenta x_i je převeden na binární vektor fixní délky v_i, kde délka vektoru odpovídá počtu častých vzorců získaných dříve. Nakonec je vytvořen model pro predikci na základě binární matice složené z jednotlivých vektorů v.

Při evaluaci predikce úspěchu byly porovnány výsledky klasických modelů strojového učení (lineární regrese, SVM a KNN), neuronové sítě LSTM modelu a modelů založených na RTP v kombinaci s jedním ze zmíněných klasických modelů. Všechny modely pracují s okénkem dat, které je typicky nastaveno na jednu minutu, vstup je tedy relativně malý. Modely byly vyhodnocovány porovnáním přesnosti, pokrytí, F-míry a AUC (plochy pod ROC křivkou). Zároveň byl porovnáván zdroj seznamu rysů. Modely založené na RTP dosáhly hodnot přes 95% na

všech měřených veličinách, a jediný výsledek, který je převyšuje, je pokrytí modelu LSTM. Modely využívající seznamy rysů definované odborníky dosáhly nepatrně lepších výsledků a nejvyšší přesnosti ze všech modelů dosáhly kombinace RTP s SVM a RTP s lineární regresí, které oba dosáhly 97%.

Při predikci potíží studenta byly testovány stejné modely, jako při predikci úspěchu. S daty z první minuty práce studenta dosáhly nejlepších výsledků modely RTP s KNN a RTP s lineární regresí (shodně přesnost 99,4%. Modely s DDF dosahují velmi podobných výsledků jako ty s EF, například RTP s lineární regresí dosáhl s EF přesnosti 99,4% a s DDF 98,8%.

1.3 Detekce problémů na trase šifrovacích her

Tématu šifrovacích her se podrobně věnuje předchozí práce autorky [19]. Tato práce popisuje velké šifrovací hry a šifry během nich využívané, vysvětluje také rozdíly mezi hrami společnosti Cryptomania tvořenými pro veřejnost a jejich firemními kurzy.

Dále popisuje základní principy zašifrování (substituce, transpozice, grafická šifra, steganografie a logické hádanky) a předkládá i alternativní klasifikaci šifer podle způsobu myšlení, který je k vyřešení třeba použít. Šifru lze buď vyřešit analytickým myšlením a testováním hypotéz, nebo je nutné využít kreativní myšlení a testovat netradiční přístupy. Předkládá také parametry šifry, které mají přímý vliv na dobu řešení šifry:

složitost: objektivní stav šifry, přímo závisí na počtu kroků, které vedou ke správnému řešení,

obtížnost: subjektivní veličina, závisí na zkušenosti hráčů, jejich stylu myšlení a mnoha dalších faktorech (např. vzdělání),

pracnost: kolik práce je třeba vykonat k získání hesla, i pokud hráči vědí, co mají při řešení dělat, množství kroků se nezmění, pracnost úzce souvisí s dobou řešení.

Práce předkládá řadu vizualizací včetně *nejpravděpodobnějšího průchodu hrou*, který demonstruje nejčastější dobu řešení každé z šifer během jedné hry. Toto zobrazení bylo následně využito autory hry

k úpravě šifry, která vykazovala časové anomálie oproti zbytku hry. Dále byly definovány metriky pro porovnání jednotlivých šifer a jejich nápověd: nejčastější doba řešení šifry, užitečnost nápovědy (tedy zda tým po žádosti o nápovědu šifru vyřeší, nebo požádá ještě o další) a souhrnné ohodnocení šifry, které obě předchozí veličiny spojuje do jedné.

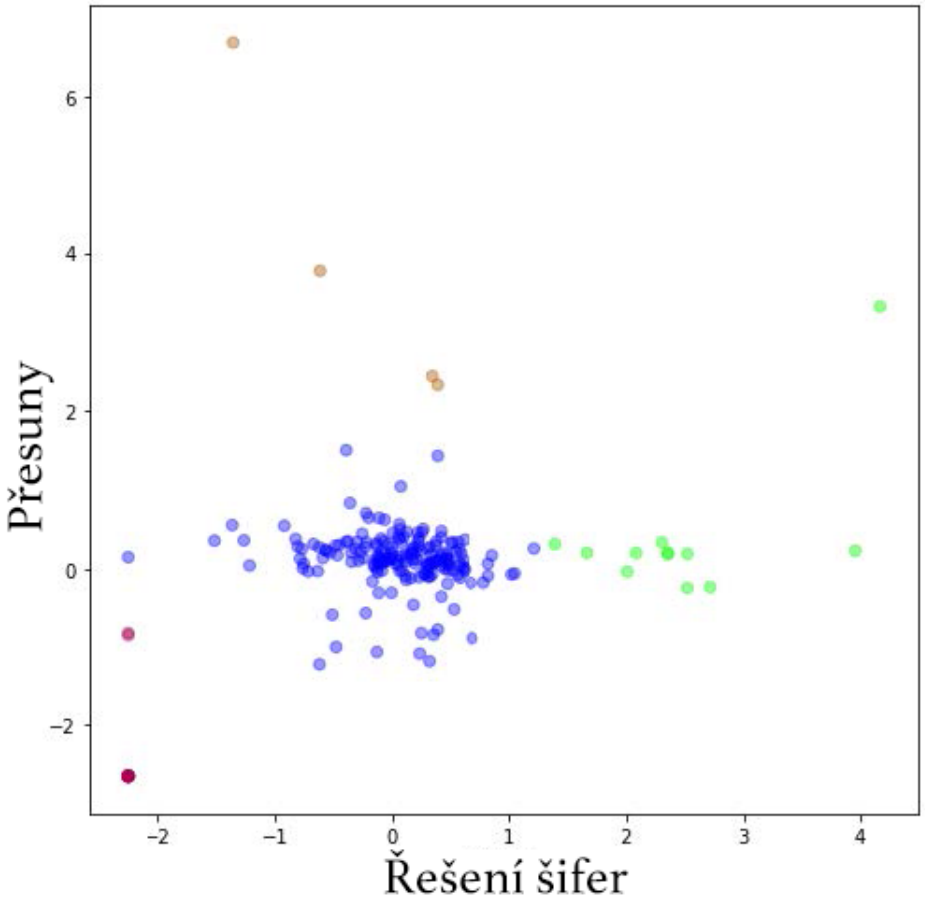
Navrženy jsou také metriky pro definování schopností jednotlivých týmů. Výkon týmu na n-té šifře je definován pomocí poměru doby, kterou tým strávil řešením šifry vzhledem k ostatním týmům, a bodů, které za vyřešení získal. Celkové ohodnocení výkonu týmu je pak definováno jako průměr všech těchto dílčích ohodnocení.

Shluková analýza celkového ohodnocení týmů nakonec ukázala čtyři skupiny s podobným chováním na trase venkovní hry:

- týmy, které se přesouvají obvyklou rychlostí a jsou úspěšné při řešení šifer (modrý shluk na obrázku 1.1),
- týmy, které se také přesouvají obvyklou rychlostí, nicméně při řešení šifer dosahují slabších výsledků (zelený shluk),
- týmy, jejichž výsledky při řešení šifer jsou srovnatelné s ostatními, ale při pohybu jsou výrazně zpomaleny (hnědý shluk),
- týmy s výrazně lepším ohodnocením při řešení i při pohybu (červený shluk), vzhledem k jejich množství jsou tyto týmy pravděpodobně testovací a fyzicky trasu možná vůbec neabsolvovaly.

Z analýzy vyplývá, že rychlost, jakou se tým přesunuje, nemá na jeho výkon zásadní vliv a pro analýzu úspěšnosti řešení šifer lze tuto metriku zanedbat.

Na základě tohoto zjištění se současná práce nezabývá přesuny týmů mezi stanovišti a místo toho přímo využívá zadání šifry a doprovodný text.



Obrázek 1.1: Shluky týmů podle celkového ohodnocení [19]

1.4 Extrakce textu z obrázků

Vzhledem k tomu, že některé šifry jsou čistě textové (viz např. výše zmiňovaná šifra Mlha[6]), mohlo by být užitečné z obrázků tento text extrahovat a využít během další analýzy.

Rozpoznání a následnou extrakci textu z obrázků nabízí *Tesseract*[7]. Tento nástroj byl původně vyvinut společností HP, která ho v roce 2005 poskytla jako *open source* projekt. Jeho funkčnost následně shrnul Ray Smith [20].

Tesseract přijímá vstup ve formě binárních obrázků, volitelně s definovanými oblastmi textu. Provede analýzu spojených komponent, čímž získá obrysy textu a ty spojí do tzv. *blobů*. Ze skupin textu jsou vytvořeny řádky a ty jsou rozděleny na slova podle toho, jaké mezery mezi nimi jsou. Texty s fixním prostorem na znak mohou být rozděleny rovnou, proporcionální text je rozdělen na základě jistých a nejistých mezer (*definite spaces and fuzzy spaces*).

Rozdělený text následně projde dvojnásobnou detekcí. Při prvním průchodu textem se nástroj snaží rozpoznat každé ze slov. Když se slovo podaří rozpoznat, je předáno adaptivnímu klasifikátoru (aktuální verze využívá LSTM neuronovou síť [21]) jako součást trénovacích dat. Klasifikátor se tedy během průchodu průběžně vylepšuje a text níže na stránce rozpoznává lépe. Již vylepšený klasifikátor následně text zpracuje podruhé, aby získaná data využil i na začátku textu na dříve nerozpoznaná slova. Nakonec upřesní nejisté mezery a určí velikost písma (zda jsou písmena malá, či velká).

1.5 Detekce objektů na obrázcích

Pro zvýšení množství informací, které model analyzující šifru využívá, by bylo vhodné mu poskytnout obrázek i v předzpracované formě. Tato informace může být tvořena například objekty, které byly na obrázku detekovány.

Detectron2 je knihovna vyvíjená společností Facebook, která „poskytuje *state-of-the-art* detekční a segmentační algoritmy“ [22]. Knihovna nabízí množství modelů trénovaných na datasetu COCO [23]

6. `https://www.hrasendvic.cz/2021/data/sada4.pdf`
7. `https://github.com/tesseract-ocr/tesseract`

(konkrétně na sadě `train2017`, validace pak na `val2017`). Základní tři typy nabízených modelů jsou tvořeny kombinací sítě s reziduálními spojeními (*ResNet*) a dalších prvků:

***ResNet* a FPN** se standardní konvolucí a plně propojenými hlavami, který dosahuje nejlepšího poměru rychlosti a přesnosti,

***ResNet* conv4** s conv5 hlavou, původně popsaný v [24],

***ResNet* s mezerami v conv5** se standardní konvolucí a plně propojenými hlavami.

Pyramidové sítě rysů (*FPN*) přijímají jednorozměrné obrázky libovolné velikosti a vrací proporcionální mapy rysů nezávisle na základní konvoluční architektuře [25]. Pyramidy jsou složeny z průchodů zdola-nahoru (*bottom-up*) a shora-dolů (*top-down*) a z příčných propojení.

Cesta zdola-nahoru je představována dopředným průchodem základní konvoluční sítí, která definuje mapy rysů (*feature maps*) několika velikostí (*scales*) se škálovacím krokem rovným 2 (každá mapa má dvojnásobnou velikost, než ta předchozí). Výstup poslední vrstvy každého rozměru je použit jako součást referenční mapy rysů.

Cesta shora-dolů generuje rysy s většími rozměry pomocí převzorkování rysů z vyšších úrovní pyramidy, poté je vylepšuje propojením s patry průchodu zdola-nahoru. Model byl trénován na COCO datasetu (80 tisíc trénovacích obrázků a 35 tisíc testovacích, ze setu `trainval35k` s validací na `minival` sadě s 5 tis. obrázky). Základní sítě jsou předtrénovány na ImageNet1k klasifikační sadě (ResNet-50 a ResNet-101) a následně dotrénovány na detekční datové sadě. Faster R-CNN model předtrénovaný na ResNet-101 dosáhl při prahové hodnotě 0,5 průměrné přesnosti 58,2%.

1.6 Generování obrázků

Datová sada obrázků dostupných k analýze není příliš rozsáhlá. Jako jedna z možností jejího rozšíření se nabízí generování nových šifer na základě těch stávajících.

Alec Radford a spol. představují architekturu konvoluční sítě, která dosahuje silných výsledků při učení bez učitele (*unsupervised learning*).

Tuto architekturu nazvali *Deep Convolutional Generative Adversarial Network* (*DCGAN*) [26].

Autoři navrhují jako základ pro generování kvalitních reprezentací obrázků síť generativního soupeření (*Generative Adversarial Network, GAN*). Ta se skládá ze dvou částí: *generátoru* a *diskriminátoru*, které jsou oba tvořeny neuronovou sítí. Tyto sítě mezi sebou během učení navzájem „soupeří". *Generátor G* na základě sady vstupních obrázků generuje obrázky. *Diskriminátor D* takto vytvořené obrázky klasifikuje do dvou tříd (původní obrázek/obrázek vytvořený generátorem). Původní soupeřící síť (*GAN*) je definována pomocí vícevrstvých perceptronů G a D. Tyto perceptrony „hrají minimax hru dvou hráčů s následující funkcí $V(G, D)$:

$$V(G, D) = \min_G \max_D \mathbb{E}_{x \sim p_{\text{data}}(x)}[\log D(x)] + \mathbb{E}_{z \sim p_z(z)}[1 - \log D(G(z))],$$

kde $G(z; \theta_g)$ je diferencovatelná funkce reprezentovaná vícevrstvým perceptronem, která mapuje do datového prostoru a $D(x; \theta_d)$ je perceptron, který má na výstupu jednu skalární hodnotu." [27] Z této základové *GAN* jsou později využity části *generátoru* a *diskriminátoru* jako extraktory rysů pro učení s učitelem.

Zmíněná *GAN* architektura tvořená konvoluční sítí je do podoby DCGAN upravena pomocí následujících změn:

- všechny sdružovací (*pool*) vrstvy jsou nahrazeny krokovanými (*strided*) konvolucemi u diskriminátoru a *fractional-strided* variantou konvoluční metody u generátoru, díky čemuž si síť vytvoří vlastní převzorkování,

- normalizace dávky (*batch normalisation* [28]) je využívána v generátoru i diskriminátoru, díky čemuž je učení stabilnější,

- plně propojené vrstvy uvnitř sítě jsou maximálně omezeny, přímé propojení vstupu generátoru a výstupu diskriminátoru s nejvyššími vrstvami je zachováno,

- generátor využívá aktivační funkci ReLU ve všech vrstvách kromě výstupu, který implementuje funkci Tanh, model se díky tomu rychleji učí vyplnit barevný prostor trénovací sady,

- diskriminátor využívá aktivační funkci *Leaky ReLU* ve všech vrstvách (oproti maxout funkci v původním Generative Adversarial Network (GAN) modelu).

Během evaluace byl vzniklý model DCGAN trénován na datasetu *ImageNet-1k*. Následně byly využity konvoluční rysy (*features*) všech vrstev diskriminátoru. Pomocí maxpoolingu byla reprezentace každé vrstvy transformována do mřížky 4×4 a tyto mřížky byly následně využity jako vstup regularizovaného lineárního L2-SVM klasifikátoru. Takto natrénovaný klasifikátor dosáhl při klasifikaci datasetu CIFAR-10 přesnosti 82,8%, čímž překonal všechny přístupy založené na K-means.

1.7 Rukou kreslené obrázky

Quick Draw Dataset je poskytován společností Google [29]. Jedná se o sadu přibližně 50 milionů kreseb z 345 kategorií pocházejících ze hry *Quick, draw!*[8]. Ve hře mají hráči v minutovém časovém limitu za úkol nakreslit zadaný objekt (například auto, letadlo, ponorku, žábu, ...), v reálném čase se neuronová síť pokouší jejich kresbu rozpoznat.

Dataset je tvořen obrázky ve formě vektorové grafiky společně s metadaty obsahujícími kategorii, kterou měl hráč nakreslit, zemi, ve které se nacházel, zda byl obrázek rozpoznán modelem, časovou známku a unikátní identifikátor dané kresby. Jsou poskytovány různě předzpracované varianty datasetu: čistá neupravená data, zjednodušená data s normalizovanými kresbami, binární data a obrázky ve formě bitových map.

1.8 Analýza sentimentu a multi-label klasifikace českých jazykových modelů

Jan Lehečka a Jan Švec porovnávají české transformery na úlohách klasifikace textu [30]. Pro porovnání si zvolili tyto modely:

8. `https://quickdraw.withgoogle.com/`

MultiBERT [31]: vícejazyčná varianta modelu BERT [32] poskytnutá společností Google, která byla trénována na exportu ze stránek Wikipedia[9] ve 104 jazycích včetně češtiny,

SlavicBERT [33]: model BERT trénovaný na exportu ze stánek Wikipedia ve čtyřech slovanských jazycích (čeština, ruština, bulharština a polština), tento model využil váhy modelu MultiBERT,

XLM-RoBERTa [34]: model předtrénovaný společností Facebook na stovce jazyků včetně češtiny, tato data pocházela z Common Crawl datasetu [35], pro tento model existují dvě varianty: *base* s 270 miliony parametrů a *large* s 550 miliony parametrů,

Czert [36]: monolingvní český model BERT předtrénovaný na kombinaci českého národního korpusu [37], stránek z Wikipedia a novinových textech, které si autoři exportovali sami,

RobeCzech [38]: model RoBERTa předtrénovaný na českém národním korpusu [37], datasetu Czes [39], dokumentech z české části webového korpusu W2C [40] a exportu ze stránek Wikipedia.

Autoři předkládají dvě varianty vlastního modelu Flexible Embedding Representation NETwork (FERNET), které s těmito modely porovnávají. Modely se liší datovou sadou, na které byly předtrénovány: *News Corpus*, který si autoři vytvořili vlastním nástrojem ([41]) a *Czech Colossal Clean Crawled Corpus* (*C5*), což je česká varianta anglického datasetu C4. Podle zdroje dat jsou modely nazvány FERNET-News, respektive FERNET-C5. Oba modely byly trénovány na úlohách *Masked Language Modeling* (*MLM*), kdy je úkolem modelu doplnit vymaskovaná slova v textu, a *Next Sentence Prediction* (*NSP*), kde model rozlišuje zda jsou dvě věty fragmentem textu, nebo byly zvoleny náhodně. Takto předtrénované modely byly testovány na dvou úlohách: analýze sentimentu a multi-label klasifikaci tématu.

Pro analýzu sentimentu byly využity datasety CSFD (91 tisíc filmových recenzí ze stránky ČSFD[10] rozdělených na pozitivní, negativní a neutrální kategorii), MALL (145 tisíc produktových recenzí ze stránek prodejce MALL.cz[11], opět pozitivní, negativní a neutrální

9. `https://www.wikipedia.org/`
10. `https://www.csfd.cz/`
11. `https://www.mall.cz/`

Tabulka 1.1: Porovnání F1-míry modelů pro analýzu sentimentu

Model	CSFD	MALL	FCB
FERNET-C5	85,36	79,75	81,07
RobeCzech	85,01	78,18	79,12
XLM-RoBERTa-large	**86,03**	**79,94**	**82,23**

Tabulka 1.2: Porovnání F1-míry modelů pro multi-label klasifikaci

Model	CTDC	CN
FERNET-C5	**91,25**	82,13
FERNET-News	90,85	82,94
RobeCzech	90,47	81,20
XLM-RoBERTa-large	91,18	**82,78**

sentiment) a FCB (10 tisíc příspěvků vybraných z několika stránek na Facebooku[12] rozdělených podle návrhu autorů datasetu [42]). Kvalita modelů byla měřena pomocí F1-míry, model FERNET-C5 na zmíněných třech datasetech překonal všechny ostatní modely kromě XLM-RoBERTa-large, nicméně FERNET-News byl u všech datasetů překonán minimálně modelem RobeCzech, porovnání zmíněných modelů je shrnuto v tabulce 1.1.

Klasifikace tématu byla evaluována na datasetech Czech Text Document Corpus (CTDC) (12 tisíc novinových článků s přiřazeným tématem, pro evaluaci bylo vybráno 37 nejčastějších kategorií) [43] a CN (250 tisíc článků s přiřazeným tématem, získaných autory ze serveru `ceskenoviny.cz`). Na datasetu CTDC dosáhl nejvyššího F1-skóre model FERNET-C5, který překonal i XLM-RoBERTa model, pro dataset CN dosáhl lepšího výsledku model FERNET-News, nicméně model XLM-RoBERTa byl ještě úspěšnější. Porovnání výsledků modelů shrnuje tabulka 1.2.

12. `https://www.facebook.com/`

2 Využívaná data a jejich zdroje

Pro predikci využití nápovědy jsou využívány informace o týmech a šifrách, které řeší. Dále je předávána informace o hře, ve které se daná šifra nachází. Největší část dat pochází z her pro veřejnost společnosti Cryptomania. Tyto hry jsou řízeny online herním systémem, který tým celou hrou provází a zároveň zaznamenává jeho průchod. Z tohoto záznamu dostal predikční model informace o týmu a o hře. Dále tento model používá obrazová a textová data.

2.1 Data z průchodů hrami Cryptomania

Šifrovací hry společnosti Cryptomania jsou řízeny online herním systémem [44]. Tento systém hráče provází celou hrou. Předkládá jim zadání jednotlivých šifer (části zadání obsahuje také herní brožura, kterou mají týmy fyzicky s sebou) a následně vyhodnocuje heslo, které hráči vyluštili z šifry a do systému zadali. Pokud je heslo správné, zobrazí polohu dalšího stanoviště (u venkovní hry), případně rovnou ukáže zadání dalšího úkolu (u her na doma). Systém také nabízí ke každé šifře jednu nebo více nápověd jak ji řešit (jejich zobrazení snižuje potenciální bodový zisk, kterého mohou hráči vyřešením dosáhnout) a kompletní řešení (hráči za danou šifru nezískají žádné body, ale mohou se ve hře posunout dále, to bez zadání správného hesla není možné). Pro potřeby predikce modelu je za využití nápovědy považována jakákoliv žádost týmu o pomoc (nezáleží tedy na tom, zda tým požádal o jednu nápovědu k vyřešení, či si zobrazil všechny dostupné nápovědy i řešení šifry). U her, které probíhají venku, je dostupná i nápověda k přesunu, která tým připraví o dva body a zobrazí polohu následujícího stanoviště. Tyto nápovědy nejsou v modelu uvažovány, protože jsou odlišnou událostí v datech a o schopnosti týmu mnoho nevypovídají, jak bylo zmíněno v sekci 1.3 (tým zpravidla žádá o nápovědu, pokud je na trase nějaký problém, se kterým autoři nepočítali, například zmizí obchod, jehož výlohu využívali v přesunu). Tato nápověda obsahuje především přístupový kód, kterým hráči odemknou samotné zadání šifry, díky tomuto kódu je v datech délka luštění oddělena od času, který hráči potřebovali na přesun na dané místo.

Každá interakce hráčů s herním systémem (zadání hesla, zobrazení nápovědy, ...) je zaznamenávána spolu s časovou známkou a typem události. Kompletní ukázka datového exportu je v příloze F.

2.2 Obrazová data

Zdroje obrazových zadání lze rozdělit do dvou kategorií: šifry, které vytvořila společnost Cryptomania a volně dostupná zadání z veřejných šifrovacích her (přesné počty a rozdělení je rozepsáno v tabulce 2.1). Data od firmy Cryptomania jsou chráněna autorským zákonem a vzhledem k tomu, že jsou hlavním artiklem firmy, je nelze najít volně dostupná a nesmí se šířit. Nelze je tedy předat spolu s prací. Tato data se skládají ze zadání her pro veřejnost a z šifer, které Cryptomania používá na firemní kurzy.

Hry pro veřejnost jsou vždy motivovány příběhem. Šifry jsou jeho součástí, proto neobsahují jen samotné zadání, ale často i prvky doplňující atmosféru hry (např. šifra leží na stole, viz obrázek A.1).

Oproti tomu šifry pro firemní kurzy mají velmi jednoduchý styl a kromě samotné šifry obsahují pouze logo firmy, název šifry a copyright v patičce (viz obrázek A.2). To bylo odstraněno během předzpracování dat, zbylo tedy čistě zadání úkolu.

Volně dostupná data byla převzata z archivu šifrovací hry DNEM[1]. Tato hra je neobvyklá tím, že v rámci jednoho ročníku vytvoří tři varianty každé šifry – pro děti, dospělé a experty. Tyto kategorie mají odlišnou složitost, nicméně základ šifry je ve většině případů stejný. Tím lze získat porovnání jak vypadá lehká (dětská) a těžká (pro experty) varianta téže šifry (např. obrázek A.4 a obrázek A.3). Všechny šifry obsahují logo a název kategorie obtížnosti, obojí bylo odstraněno při přípravě dat.

Po odstranění loga, názvu, copyrightu a kategorie byly obrázky zmenšeny na čtverec o rozměru 512 na 512 pixelů. Následně byla zadání rozdělena na lehké a těžké šifry. U her vytvořených společností Cryptomania pro veřejnost byla využita data z průchodů – pokud nadpoloviční většině týmů trvá vyřešení přes 18 minut, je šifra klasifikována jako těžká (viz tabulka E.1). Zbytek šifer byl anotován ručně.

1. `https://www.chameleonbrno.org/dnem/`

Za lehkou jsou považovány např šifry na obrázcích A.1 a A.2, oproti tomu těžká šifra je například na obrázku A.3.

Jako další zdroj zadání šifer se nabízí ostatní veřejné šifrovací hry (například brněnská TMOU[2]). Nicméně tyto hry jsou vytvářeny pro zkušené hráče a v porovnání s těmi od Cryptomania neobsahují žádnou lehkou šifru. Například počáteční šifra z 20. ročníku šifrovací hry TMOU (A.5) je jedna z nejjednodušších z celé hry [45], i tak je obtížnější, než většina šifer vytvořených ve firmě Cryptomania pro veřejnost.

2.3 Textová data

Textová část dat pochází z legend k jednotlivým šifrám. Jedná se o část příběhu, který motivuje hry pro veřejnost od Cryptomania. Zpravidla se jedná o krátký text, který uvádí do děje, vysvětluje prvky obrázku, které nutně nemusí být součástí šifry (například text hovoří o šifře ležící na stole v kavárně, viz obrázek A.1, hráči tedy ví, že stůl a káva nejsou součástí šifry). Zároveň tento text může obsahovat drobnou nápovědu jak šifru řešit, například poukazuje na skutečnost, která nemusí být na první pohled zřejmá. K šifře na obrázku A.1 vidí hráči ještě tento text:

> Sedíš společně se Šárkou v kavárně U Zmateného netopýra. Místností se line vůně kávy a Šárka hledá v knihovně knihu Saturnin. První šifru jste zvládli vcelku rychle, a tak se těšíte, co Tomáš vymyslel dalšího. Během chvilky v knize nacházíte list papíru.
>
> Tentokrát je na něm několik jednoduchých obrázků a z druhé strany připsaná krátká poznámka: Tohle je tvoje druhá šifra Šárko. Výsledkem je opět jedno slovo. Můžeš se odrazit od toho, kde jsi šifru našla. Zajdi si na zmrzlinu do té skvělé cukrárny u řeky a obsluze řekni heslo, které ti vyjde. Dostaneš se zase o kousek blíž k cíli [46].

První odstavec textu navazuje na předchozí šifru, která hrdiny dovedla k současnému zadání. Následně dostávají hráči nápovědu, že se

2. `https://www.tmou.cz/`

Tabulka 2.1: Zdroje obrazových dat pro klasifikaci obtížnosti šifry

Sada/label	Zdroj dat a jejich počet			
	DNEM	firemní kurzy	hry pro veřejnost	celkem
train/easy	79	55	35	169
train/hard	84	52	35	171
valid/easy	21	14	9	43
valid/hard	23	11	9	43
celkem/easy	100	69	43	212
celkem/hard	107	63	44	214

mají *„odrazit od toho, kde šifru našli“*, tedy od knihovny. Hráči následně přijdou na to, že obrázky v šifře představují názvy známých knih.

Hry, které fyzicky prochází městem, mají příběh rozdělen na dvě části: první hráči dostanou na cestu mezi úkoly a druhý k samotné šifře. Pro potřeby modelu byly tyto části spojeny do jedné. Přehled délek těchto textů a jejich rozdělení je dostupný v příloze B.

3 Predikce využití nápovědy

Veškerá dostupná obrazová data byla použita pro trénink a následné vyhodnocení modelu, který predikuje obtížnost šifry (lehká, nebo těžká). Výstup předposlední vrstvy tohoto modelu následně slouží jako jeden ze vstupů pro síť predikující využití nápovědy během hry.

3.1 Predikce obtížnosti šifry

Do modelu pro predikci obtížnosti šifer vstupují jednak samotné obrázky (zadání šifer), jednak text, který byl z těchto obrázků extrahován pomocí nástroje Tesseract[1] (ukázky extrahovaných textů viz příloha C) [20]. Vzhledem k tomu, že zadání šifer pro tuto predikci byla převzata z více různých zdrojů (viz zdroje dat v kapitole 2), nelze pro tuto predikci přidat další vstupy (například doprovodné texty), protože tento typ dat je dostupný jen pro Cryptomania hry pro veřejnost, které jsou zde zastoupeny minimálně (viz tabulka 2.1, pro zkrácení zápisu jsou uváděny názvy v sad anglickém jazyce: *train* – trénovací, *val* – validační, *easy* – lehká, *hard* – těžká). Nicméně pro vylepšení výsledků predikce se nabízí využití předtrénovaného modelu pro detekci objektů v obrázku a vytvoření jejich vektorové reprezentace.

Jako výchozí hodnoty pro porovnání přesnosti modelů byly použity výsledky náhodné predikce (přesnost 0,48 na validační množině) a jednovrstvé konvoluční sítě s 16 neurony, která využívala pouze obrazový vstup (přesnost 0,54 na validační množině, tyto hodnoty jsou shrnuty v tabulce 3.4).

Základní model vychází z architektury popsané v [47]. Textový vstup prochází enkodérem a následně jednorozměrnou konvoluční a poolingovou vrstvou. Obrázky zmenšené na 512 $\times$ 512 px jsou nejprve zpracovány vlastním klasifikátorem (v tomto případě třemi konvolučními vrstvami) a následně zpracovány společně s textem, schéma tohoto modelu je zobrazeno na obrázku 3.1 a jeho parametry pak v tabulce 3.1.

1. `https://github.com/tesseract-ocr/tesseract`

Jako aktivační funkce poslední vrstvy byl použit softmax:

$$\sigma(z_i) = \frac{e^{z_i}}{\sum_{j=1}^{K} e^{z_j}} \quad pro\ i = 1, 2, \ldots, K$$

a jako ztrátová funkce slouží binární křížová entropie:

$$H(p) = -(y \log(p) + (1 - y) \log(1 - p)),$$

kde p je predikce modelu a y je skutečná třída. K optimalizaci byl využit algoritmus Adam[2] a jako rozhodující veličina byla měřena přesnost (*accuracy*) na validační množině:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN},$$

kde TP odpovídá počtu *true positive*, tedy správně predikovaných pozitivních příkladů, TN *true negative* (počet správně predikovaných negativních příkladů), obdobně FP respektive FN – *false positive*, resp. *false negative* (počet špatně predikovaných příkladů).

Skryté vrstvy obrazového klasifikátoru využívají aktivační funkci ReLU:

$$ReLU(z) = max(0, z)$$

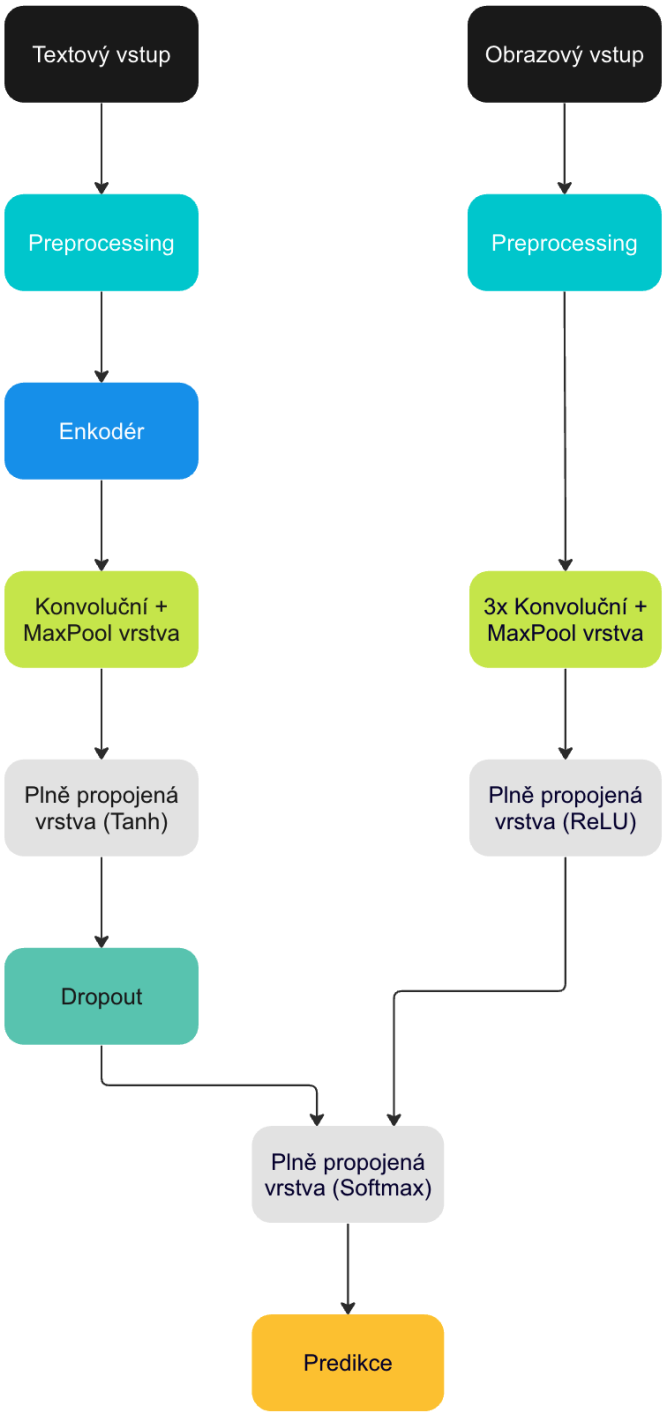
a pro text je aplikován hyperbolický tangens:

$$tanh(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}} = \frac{1 - e^{-2x}}{1 + e^{-2x}}.$$

3.1.1 Zpracování textového vstupu

Textové zadání je před vstupem do konvoluční vrstvy předzpracováno jazykovým modelem. Z dostupných multilingvních modelů byly porovnány enkodéry BERT[3] a XLM-RoBERTa[4].

2. `https://keras.io/api/optimizers/adam/`
3. `https://tfhub.dev/tensorflow/bert_multi_cased_preprocess/3` a `https://tfhub.dev/tensorflow/bert_multi_cased_L-12_H-768_A-12/4`
4. `https://tfhub.dev/jeongukjae/xlm_roberta_multi_cased_L-12_H-768_A-12/1` a `https://tfhub.dev/jeongukjae/xlm_roberta_multi_cased_preprocess/1`



Obrázek 3.1: Schéma modelu pro predikci obtížnosti šifry

Tabulka 3.1: Parametry vrstev modelu na obrázku 3.1 pro predikci obtížnosti šifry

Vrstva	Počet neuronů	Aktivační funkce
1. Conv2D	16	ReLU
2. Conv2D	32	ReLU
3. Conv2D	16	ReLU
Plně propojená	128	ReLU
Conv1D	16	ReLU
Plně propojená	32	tanh

Tabulka 3.2: Porovnání multilingvních jazykových modelů a jejich dalšího učení

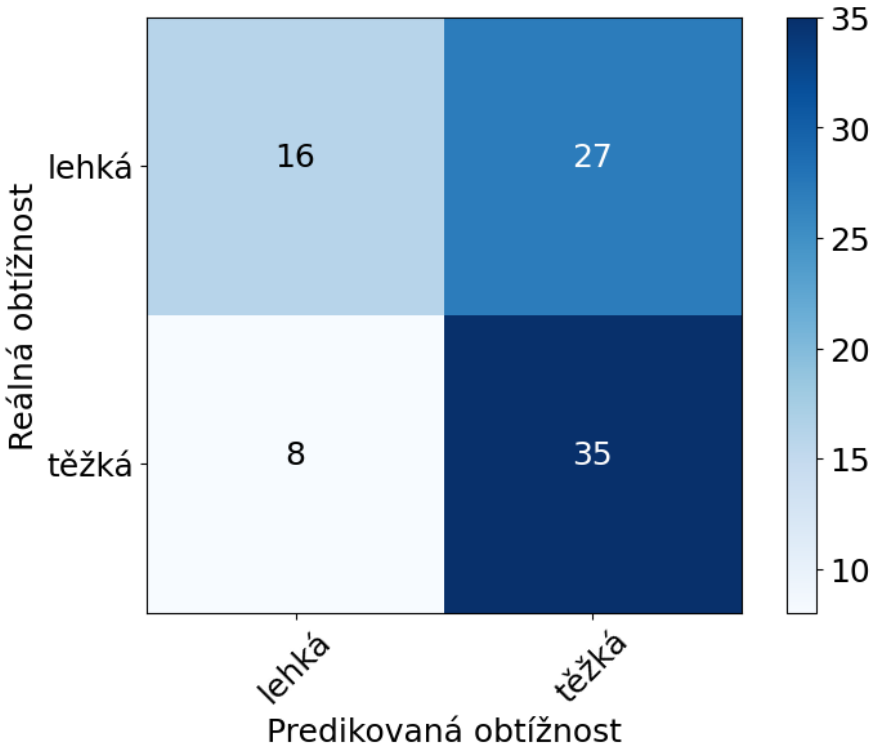
Jazykový model	Dále učený	Train acc	Val acc
BERT	ne	0,67	0,55
BERT	**ano**	**0,97**	**0,59**
RoBERTa	ne	0,63	0,58
RoBERTa	ano	0,63	0,58

Vzhledem k tomu, že zadání šifer často neobsahují žádný smysluplný text (viz např. obrázek A.2), se nabízí předtrénovaný jazykový model dále učit, aby se netradičnímu vstupu přizpůsobil. Tento přístup však přesnost predikce na validační sadě příliš nezvýšil. Výsledky jednotlivých modelů se zafixovaným i dále učeným enkodérem jsou shrnuty v tabulce 3.2 (pro zkrácení zápisu je v tabulce používána *Train acc* pro přesnost modelu na trénovací sadě a *Val acc* pro přesnost na validační sadě).

Model, který během 18 epoch dosáhl nejlepšího výsledku, je silně přizpůsoben trénovací sadě. K přeučení dochází i přesto, že již v základní architektuře je na textovou část aplikován dropout 0,1 (10% matice je nahrazeno 0). Výsledky predikce tohoto modelu na validační sadě zachycuje matice záměn na obrázku 3.2.

3.1.2 Vektorová reprezentace obrazových zadání

Pro zvýšení přesnosti predikce se nabízí použití vektorové reprezentace i pro obrazový vstup. K tomu je využit model pro detekci ob-



Obrázek 3.2: Matice záměn základního modelu predikce obtížnosti šifry na validační sadě

Tabulka 3.3: Výsledky modelů predikce obtížnosti šifry využívající pouze vektorovou reprezentaci, nebo i původní obrázky

Jazykový model	I původní obrázky	Train acc	Val acc
BERT	ne	0,63	0,65
RoBERTa	ne	0,63	0,61
BERT	ano	0,73	0,65
RoBERTa	**ano**	**0,74**	**0,67**

Tabulka 3.4: Porovnání modelů pro predikci obtížnosti šifry

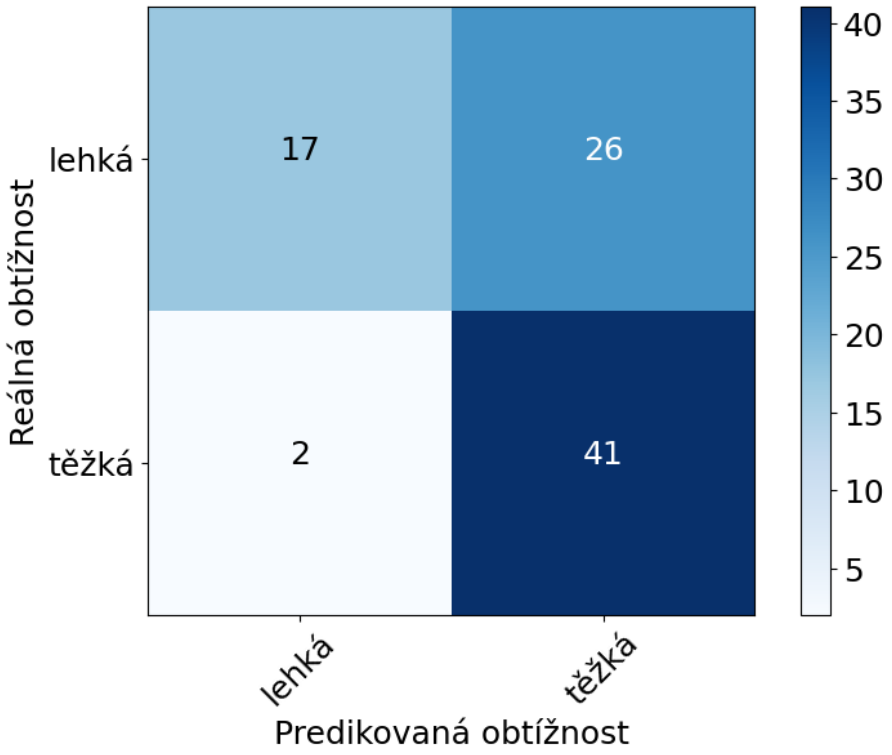
Model	Train acc	Val acc
Náhodná predikce	0,49	0,48
Jednovrstvá CNN	0,62	0,54
Model pro text a obrázky, dále přizpůsobovaný j. m. BERT	0,97	0,59
Model pro text, obrázky a jejich vekt. rep., dále přizpůsobovaný j. m. RoBERTa	**0,74**	**0,67**

jektů v obrázku, konkrétně *Detectron2* [22] předtrénovaný na datasetu COCO[5]. Obrázky v původní velikosti jsou zpracovány modelem, který je zmenší na rozměr 800 × 1300 px, převede do formátu BRG (*blue – red – green*) a následně vygeneruje vizuální vektorovou reprezentaci zahrnující 10 nejpravděpodobnějších objektů.

Na vstupu jsou pak buď jen takto upravené šifry, nebo jsou k nim přidány i původní obrázky. Výsledky jednotlivých modelů shrnuje tabulka 3.3. Nejvyšší přesnosti dosáhl návrh kombinující původní obrazová zadání šifer s jejich vektorovou reprezentací a využívající jazykový model XLM-RoBERTa, který byl dále přizpůsobován vstupu. Matice záměn tohoto modelu je na obrázku 3.3.

Tabulka 3.4 shrnuje přístupy k predikci a srovnává výsledky modelů. Nejvyšší přesnosti dosáhl model spojující vektorovou reprezentaci obrázků a jejich původní zadání zmenšené na 512 × 512 px. Textový vstup je předzpracován multilingvním modelem RoBERTa, který se dále přizpůsoboval vstupu. Tento model je používán v dalších výpočtech.

5. `https://cocodataset.org/#home` s konfigurací `COCO-InstanceSegmentation/mask_rcnn_R_101_FPN_3x.yaml`



Obrázek 3.3: Matice záměn modelu využívajícího obrázky i jejich vektorovou reprezentaci pro predikci obtížnosti šifry na validační sadě

3.2 Model predikce využití nápovědy

Pro predikci, zda si tým t vezme nápovědu během řešení šifry c, využívá model tato vstupní data:

Poměr dosavadního využití nápověd udává obecnou tendenci týmu o nápovědu požádat.

$$h_t = \sum_{i=1}^{c} \frac{h_i}{c}, \text{ kde } h_i = \begin{cases} 1, & \text{pokud si tým na šifře } i \\ & \text{zobrazil libovolnou nápovědu} \\ 0, & \text{jinak.} \end{cases}$$

Průměrný čas strávený na šifře během řešení každé z předchozích šifer na trase hry.

$$d_t = \sum_{i=1}^{c} \frac{d_i}{c}, \text{ kde } d_i \text{ je čas, který tým } t \text{ strávil řešením šifry } i.$$

Poměrné pořadí šifry ve hře, které může přibližně naznačit autory zamýšlenou obtížnost. Vzhledem k tomu, že hry jsou tvořeny zkušenými organizátory zážitkových akcí, mají pečlivě promyšlenou dramaturgii (lehká šifra na začátku, postupně zvyšovaná obtížnost až k šifře přibližně v polovině hry, snížení obtížnosti a nové postupné zvyšování až k předposlední šifře, zakončené poslední lehkou šifrou) [2, 6]. Tato veličina je následně zakódována pomocí kódování *one-hot-encoding*

$$o_c = \frac{c}{N}, \text{ kde } N \text{ je počet všech šifer ve hře.}$$

O jakou hru se jedná: hry mají různé cílové skupiny a tedy i odlišnou obtížnost šifer (nejtěžší šifra pro děti je nesrovnatelná s nejtěžší šifrou pro dospělé). Je tedy možné, že během hry pro děti budou nápovědy využívány méně, protože dětem mohou poradit dospělí.

Hra je určena umělým indexem, který je zakódován pomocí *one-hot-encoding*.

Informace o obrazovém zadání šifry, tedy výstup předposlední vrstvy modelu predikce obtížnosti šifry popsaného v sekci 3.1 (tj. vektorová reprezentace obrázku).

Příběh k šifře, který může obsahovat nápovědu k řešení šifry, popsaný v sekci 2.3. Tento text je předzpracován některým z jazykových modelů popsaných níže.

Rozdělení dat z modelu predikce obtížnosti zůstává zachováno. Pokud bylo tedy obrazové zadání v trénovací sadě, všechny týmy, které šifru řešily, jsou také součástí trénovací sady.

Vzhledem k tomu, že data nejsou vyvážená (68% pozitivních příkladů z celkových 39936 v trénovací sadě a 71% z 4230 ve validační), jsou třídám přiřazeny váhy, které jsou následně předány trénovanému modelu. Tyto váhy byly stanoveny podle následujícího vzorce:

$$\text{váha třídy } j = \frac{\text{celkový počet prvků}}{\text{počet tříd} \times \text{počet prvků třídy } j}.$$

Takto byla stanovena váha 1,58652471 pro třídu 0 (týmy, které nápovědu nevyužily) a 0,73009141 pro třídu 1 (týmy, které ji využily). U validační sady takový krok není nutný, nicméně je třeba správně stanovit hranici, kdy je model považován za lepší, než náhodný. V tomto případě je hranice stanovena na 0,71.

Poměr využití nápověd a průměrný čas strávený na šifře byly spojeny do dvouprvkového pole ([*Poměr využití nápověd*, *Průměrný čas strávený na šifře*], konkrétní ukázka vstupu je v příloze D) a následně byly všechny vstupy převedeny na tensory.

3.2.1 Využití multilingvních jazykových modelů

Základní model predikce využívá pro zpracování textového vstupu předtrénovaný model RoBERTa[6], který dosahoval nejlepších výsledků při predikci obtížnosti šifry u modelu popsaného v kapitole 3.1.

Takto připravený vstup je zpracován jednou vrstvou se 128 neurony a aktivační funkcí *ReLU* a následně je spojen se zbytkem vstupů a předložen zbytku modelu, jehož struktura je popsána v tabulce 3.5

Základní verze modelu byla trénována na 50 epochách a využívala optimalizační algoritmus Adam s rychlostí učení (*learning rate*) 0,001. Tento model dosáhl přesnosti 0,68 na validační sadě a nepřekročil tedy

6. `https://tfhub.dev/jeongukjae/xlm_roberta_multi_cased_preprocess/1` a `https://tfhub.dev/jeongukjae/xlm_roberta_multi_cased_L-12_H-768_A-12/1`

Tabulka 3.5: Struktura modelu predikce nápovědy s modelem RoBERTa

Vrstva	Počet neuronů	Aktivační funkce
dense 1	128	ReLU
dense 2	32	ReLU
dense 3	64	ReLU
dense 4	128	ReLU
dense 5	16	ReLU
dense 6	32	ReLU
dense 7	2	softmax

Tabulka 3.6: Výsledky predikce využití nápovědy s využitím multilingvních modelů

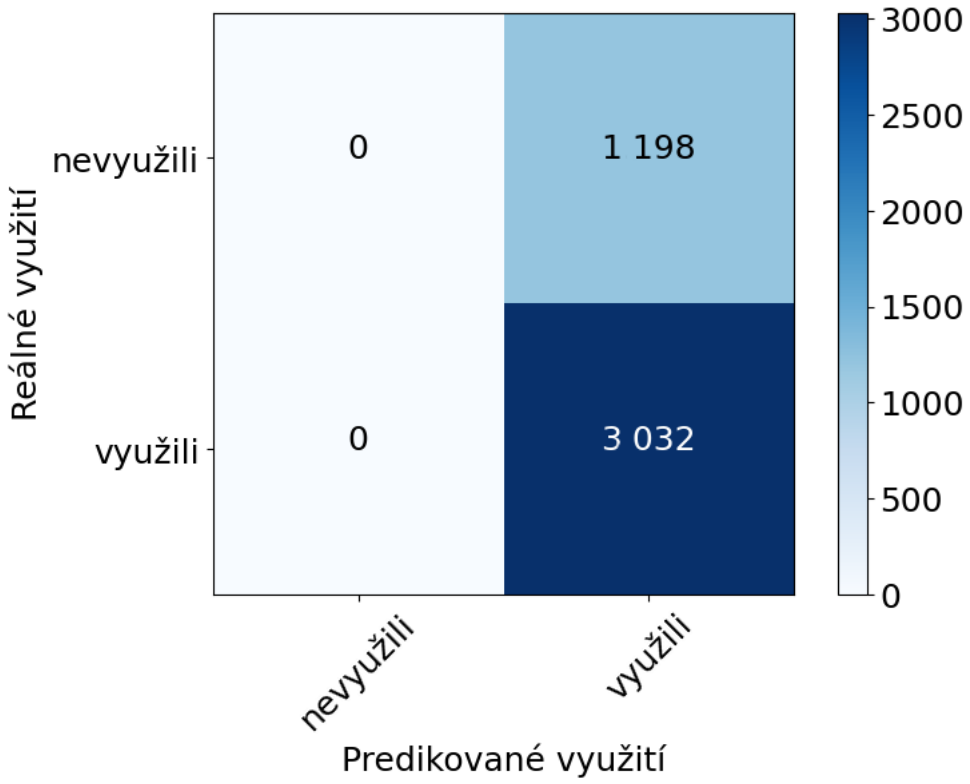
Jazykový model	Rychlost učení	Val acc
RoBERTa	0,001	0,68
RoBERTa	0,0001	0,697
RoBERTa	0,0001	0,685
RoBERTa	0,00015	**0,71**
BERT[a]	0,00015	0,70

a. `https://tfhub.dev/tensorflow/bert_multi_cased_preprocess/3` a `https://tfhub.dev/tensorflow/bert_multi_cased_L-12_H-768_A-12/4`

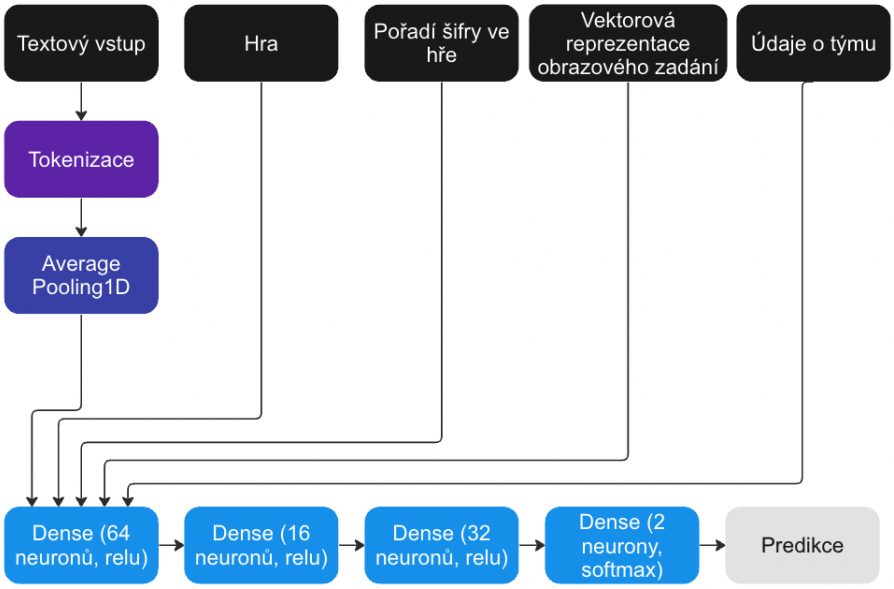
definovanou hranici úspěchu (0,71). Následné úpravy hyperparametrů a opětovné učení modelu dosáhly nejvyšší přesnosti 0,71 a tedy konstantní predikce jedné třídy (že tým nápovědu využije). Konkrétní výsledky (včetně dvakrát provedeného trénování se stejnou rychlostí učení, které dosáhlo různých výsledků) shrnuje tabulka 3.6 a matice záměn na validační sadě (obrázek 3.4).

3.2.2 Využití modelu předtrénovaného na českých textech

Texty, které model zpracovává, jsou smysluplné (narozdíl od modelu predikce obtížnosti v kapitole 3.1, který dostal data automaticky extrahovaná, a tím pádem často nesmyslná), predikci by tedy mohlo prospět využití modelu předtrénovaného čistě pro české texty. Za tímto účelem byl použit model *RobeCzech* popsaný v [38].



Obrázek 3.4: Matice záměn modelu predikujícího jednu třídu



Obrázek 3.5: Schéma predikčního modelu s využitím předtrénovaného modelu RobeCzech

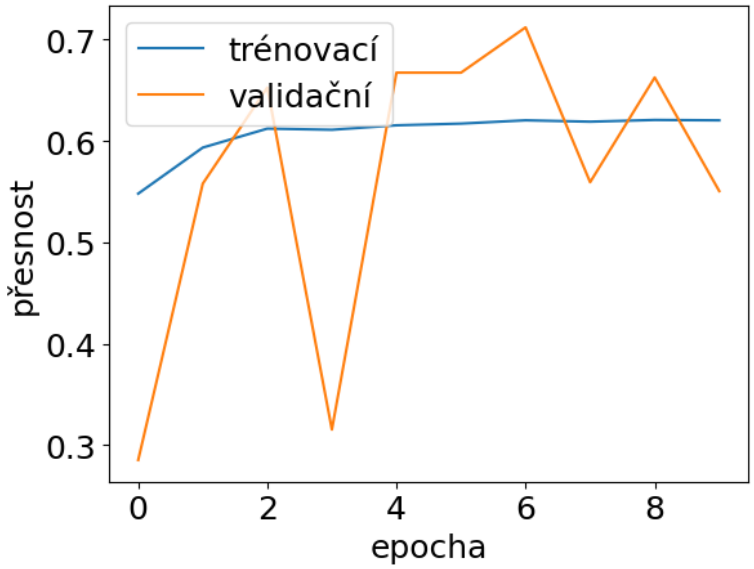
Texty příběhů k šifrám byly tokenizovány pomocí BPE (*byte pair encoding*) algoritmu a následně byly vektorizovány modelem *ufal/robeczech-base*. Takto předzpracované byly předloženy predikčnímu modelu spolu se zbytkem vstupních dat, ukázka vstupu je v příloze D. Struktura tohoto modelu je popsána v tabulce 3.7 a na obrázku 3.5. Vzhledem k rozsáhlosti předtrénovaného modelu není z paměťových důvodů možné zvýšit množství vrstev konečného modelu (při velikosti dávky rovné 1, zabírá model 12 GB paměti a jedna epocha průměrně trvá 80 minut).

K optimalizaci učení byl nejprve použit algoritmus Adam s počáteční rychlostí učení (*learning rate*) 10^{-5}. Tento model se učil deset epoch a po prvních pěti epochách začal střídavě predikovat vždy pouze jednu z tříd (tj. s přesností 0,7168, nebo 0,2832).

Následně byla rychlost učení snížena na 5×10^{-6}. Vývoj přesnosti během prvních deseti epoch zobrazuje obrázek 3.6, nejvyšší dosažená přesnost byla 0,712, pohled na matici záměn (obrázek 3.7) ukazuje že model predikuje téměř výhradně prvky jedné třídy, nicméně ještě zcela nezkonvergoval. Proto byly použity váhy modelu s nejlepším nastavením a model byl učen dalších deset epoch s rychlostí učení

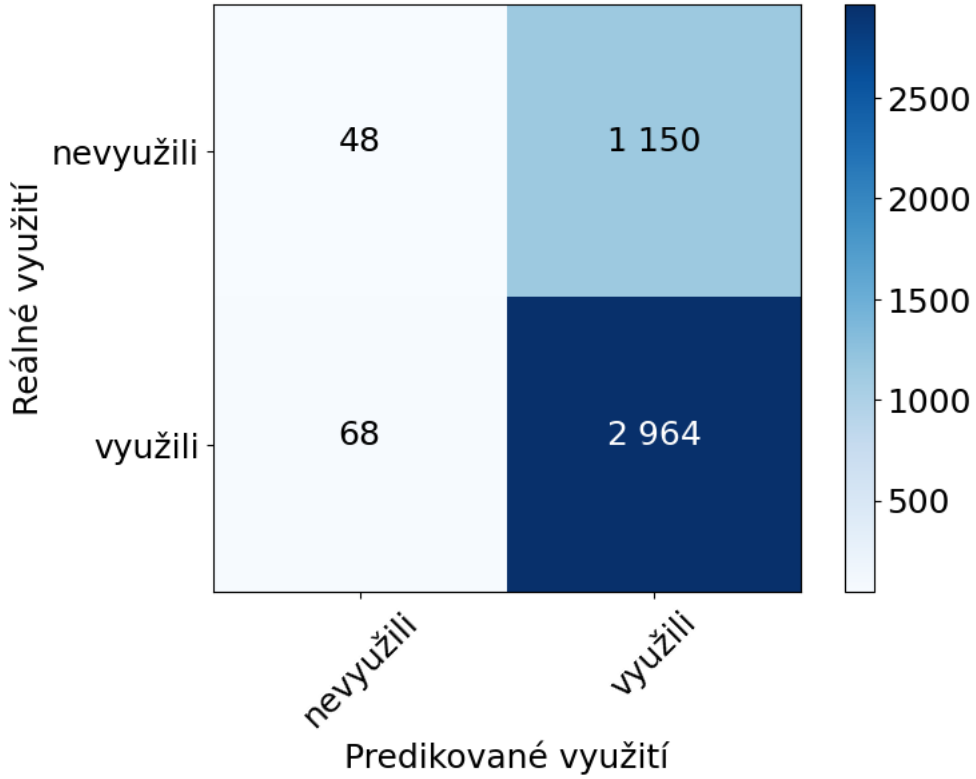
Tabulka 3.7: Struktura modelu predikce nápovědy s využitím předtrénovaného modelu RobeCzech

Vrstva	Počet neuronů	Aktivační funkce
dense 1	128	ReLU
dense 2	64	ReLU
dense 3	16	ReLU
dense 4	32	ReLU
dense 5	2	softmax

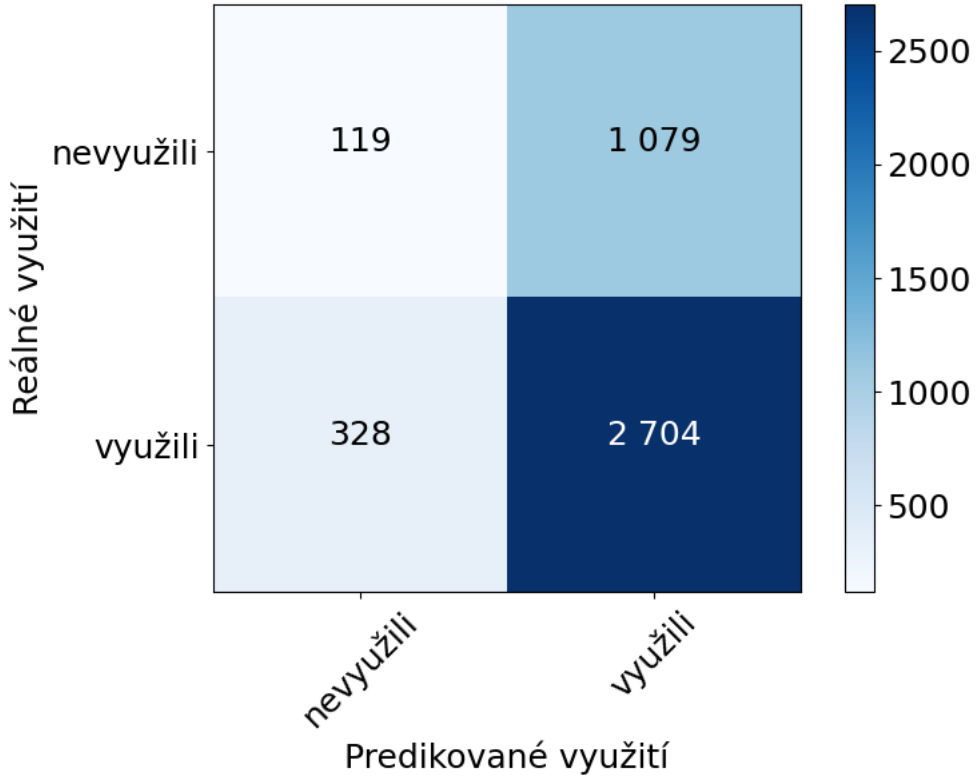


Obrázek 3.6: Vývoj přesnosti během prvních 10 epoch učení modelu využívajícího předtrénovaný model RobeCzech

sníženou na 10^{-6}. Matice záměn (obrázek 3.7) ukazuje, že výsledný model predikuje méně prvků dominantní třídy, nicméně o to více vrací *false negative* výsledků, jeho nejvyšší přesnost je 0,653.



Obrázek 3.7: Matice záměn modelu využívajícího předtrénovaný model RobeCzech po 10 epochách



Obrázek 3.8: Matice záměn modelu využívajícího předtrénovaný model RobeCzech po 20 epochách

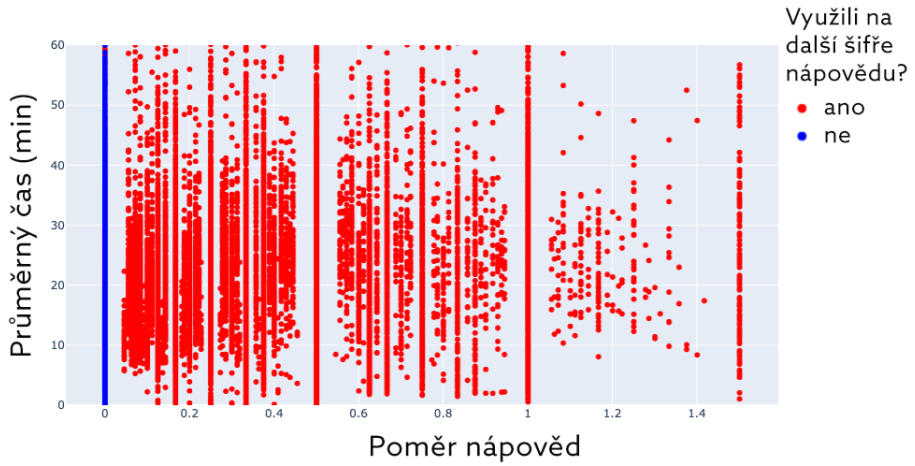
4 Úprava datové sady

Datová sada pro predikci využití nápovědy vychází ze sady pro predikci obtížnosti šifry (popsaný v sekci 3.1). Nejprve byla tedy obrazová zadání rozdělena na trénovací a validační část tak, aby každá z nich obsahovala stejné množství lehkých a těžkých šifer. Toto rozdělení je přenášeno do jakékoli další tvorby datových sad. Díky tomu jsou všechny týmy, které řešily danou šifru, zařazeny do stejné části (trénovací, nebo validační). K takto rozděleným týmům je vygenerován zbytek informací popsaných na začátku kapitoly 3.2 (dosavadní výkon týmu, informace o hře a šifře, vektorová reprezentace obrazového zadání a vektorová reprezentace příběhu k šifře).

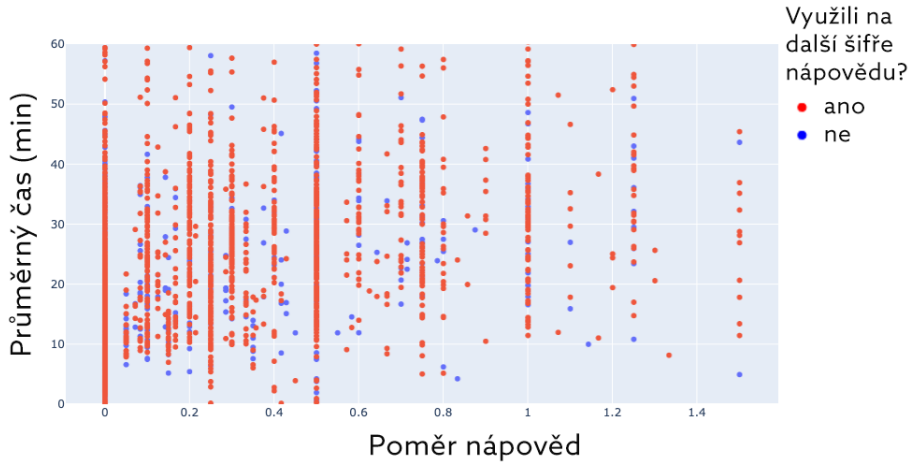
Vzhledem k vysokému množství *false positive* výsledků predikčních modelů v kapitole 3 se zdá, že takto vytvořená datová sada není pro predikci využití nápovědy vhodná. Snaha zachovat oddělená trénovací a validační data od samého počátku vedla k velké nevyváženosti v pozdějších krocích. Obrázek 4.1 zachycuje rozložení statistik týmů v trénovací sadě pro průměrné řešení šifry menší než 60 minut, ukazuje poměr nápověd a časů jednotlivých týmů. Všechny úspěšné týmy jsou zřejmě v jedné kategorii, čímž se tato veličina stává pro model neužitečnou. Pohled do validační sady (4.2) ukazuje i úspěšné týmy, které v minulosti nápovědu využily. Zdá se tedy, že změna tohoto poměru by mohla predikce vylepšit. Proto je třeba oddělit trénovací a validační sady modelu obtížnosti šifry a modelu predikce nápovědy.

4.1 Přerozdělení trénovací a testovací sady

V celém datasetu je 68,79% (30381) pozitivních příkladů (týmy, které na další šifře nápovědu využily), původní trénovací sada (obsahující 68,48% (27350) pozitivních příkladů) tedy tento poměr úspěšně udržela. Původní trénovací sada obsahuje 12586 týmů, které na následující šifře nevyužily nápovědu, nicméně všechny mají dosavadní průměr využití nápovědy roven nule. Oproti tomu nově rozdělený dataset obsahuje jen 10987 týmů bez nápovědy na následující šifře, 285 z nich však nápovědu využilo někdy v minulosti. Tento počet odpovídá poměru zastoupení týmů s podobným chováním. Celý dataset



Obrázek 4.1: Původní rozdělení týmů v trénovací sadě



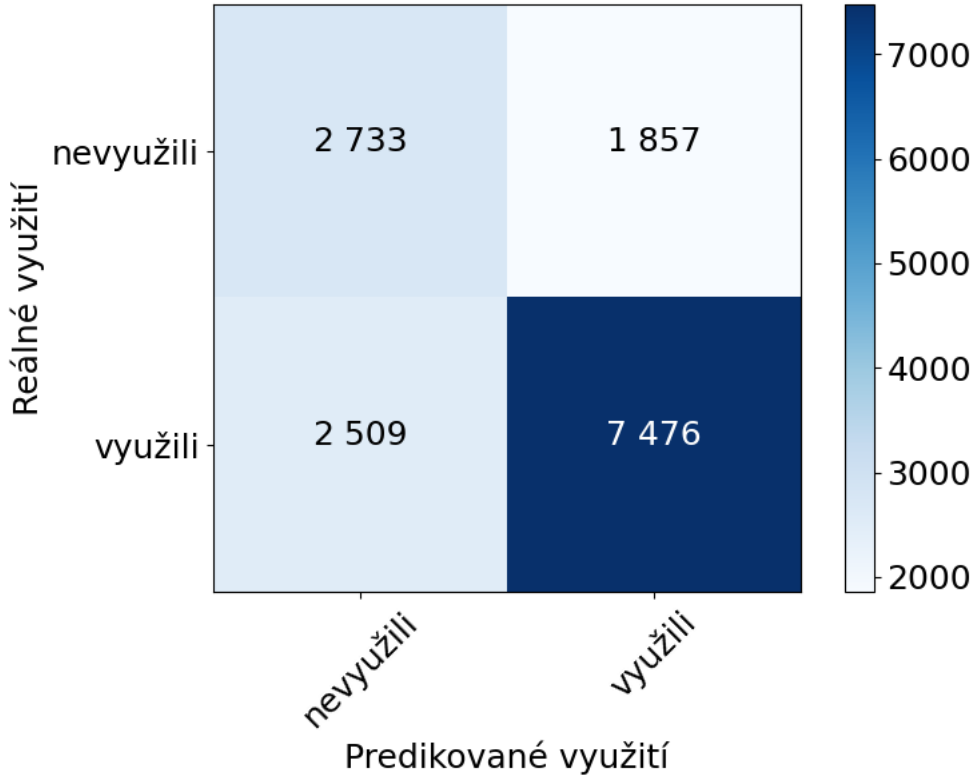
Obrázek 4.2: Původní rozdělení týmů ve validační sadě

takovýchto záznamů o týmech obsahuje 358 z 44166 řádků, jednotlivé počty jsou rozepsány v tabulce 4.1. Zároveň je v nově rozděleném datasetu stejný poměr pozitivních příkladů v trénovací i validační sadě (68% pozitivních).

Vzhledem k trvající nevyváženosti trénovací sady, byly opět třídám přiřazeny váhy (1,6 a 0,72). Následně byl s touto novou sadou a váhami natrénován predikční model popsaný v podsekci 3.2.1 s rychlostí učení 0,00015 a jazykovým modelem RoBERTa. Tento model dosáhl během

Tabulka 4.1: Počty záznamů vzhledem k využití nápovědy v minulosti a na další šifře

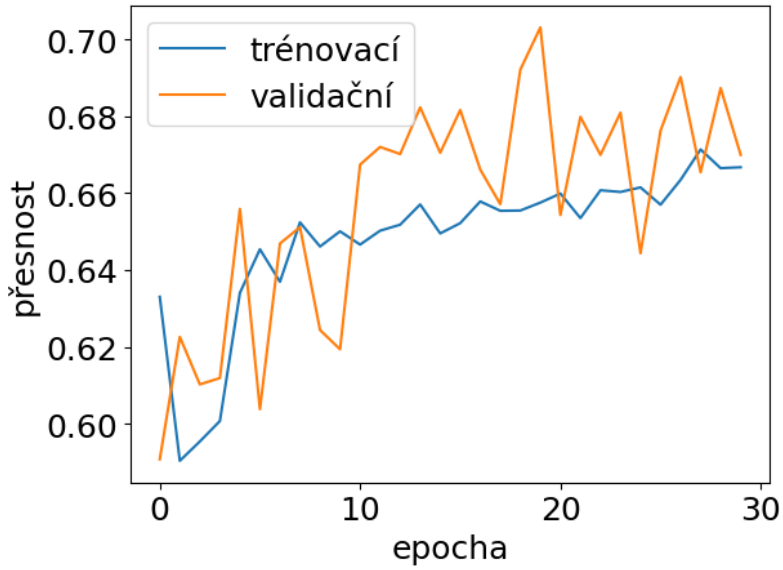
Sada dat	Nápověda na další šifře	Nápovědy v minulost	Počet záznamů
celá sada	ne	ano	358
celá sada	ne	ne	13426
celá sada	ano	ano	17000
celá sada	ano	ne	13382
původní trénovací	ne	ano	0
původní trénovací	ne	ne	12586
původní trénovací	ano	ano	15693
původní trénovací	ano	ne	11657
nová trénovací	ne	ano	285
nová trénovací	ne	ne	10702
nová trénovací	ano	ano	13662
nová trénovací	ano	ne	10683



Obrázek 4.3: Matice záměn modelu s přerozdělenými daty a jazykovým modelem RoBERTa

30 epoch na validační sadě nejlepší přesnosti 0,7. Pohled na matici záměn na obrázku 4.3 ukazuje, že model stále tíhne k predikci jedné třídy, nicméně vrací prvky obou tříd (narozdíl od modelu s výsledky na obrázku 3.7). Vzhledem k rostoucímu průběhu přesnosti modelu (obrázek 4.4) se zdá, že by dalším trénováním mohla přesnost ještě vzrůst. Výsledky dalšího učení však tento předpoklad nepotvrdily a přesnost modelu se nezměnila.

S využitím tokenizace, jazykového modelu RobeCzech a rychlosti učení 5×10^{-6} bylo během deseti epoch (každá přibližně 80 minut) dosaženo přesnosti 0,68. Matice záměn na obrázku 4.5 ukazuje, že tento model tíhne k predikci jedné třídy.



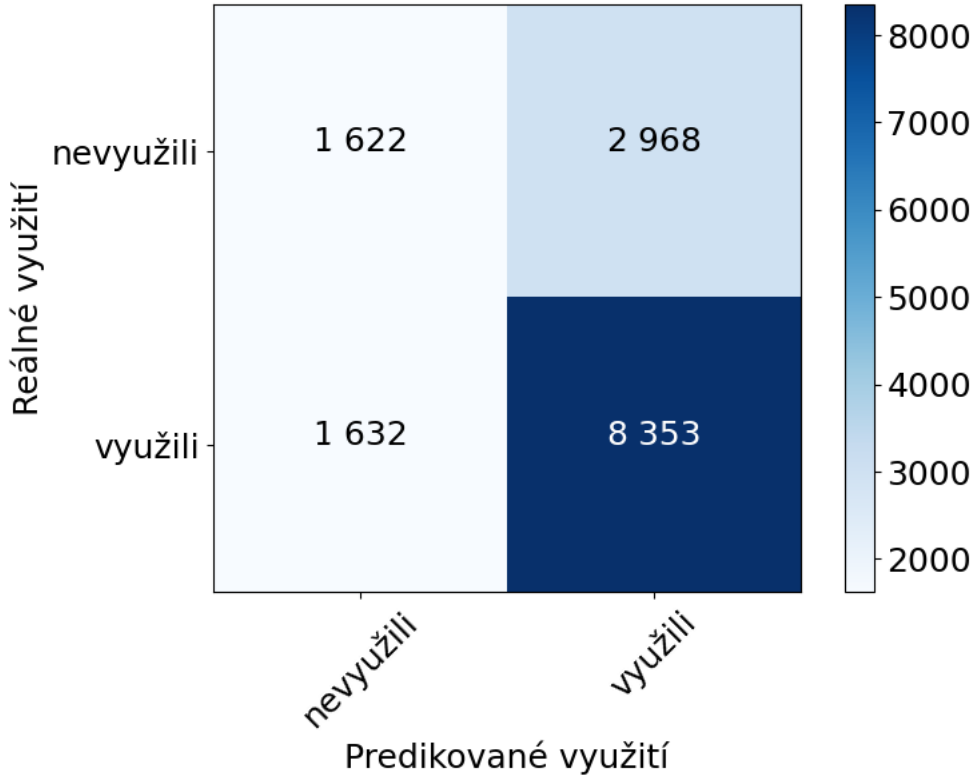
Obrázek 4.4: Vývoj přesnosti predikčního modelu s přerozdělenými daty a jazykovým modelem RoBERTa během prvních 30 epoch

4.2 Generování nových dat

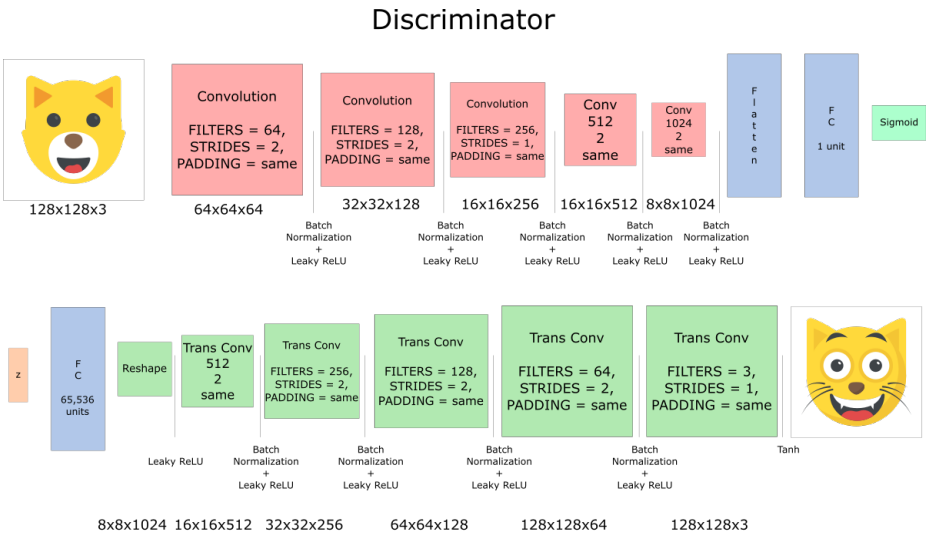
Množství dat, které má k dispozici klasifikační model obtížnosti, je pro kvalitní naučení modelu velmi nízké. Vzhledem k tomu, že zdroj těchto dat je poměrně omezený, nabízí se tato data generovat uměle. Je však otázka, zda stejným nedostatkem vstupních dat nebude trpět i generátor.

Pro generativní model byla použita implementace modelu DCGAN z open-source projektu Thomase Simoniniho [48]. Projekt je původně zaměřen na generování obrázků koček, nicméně autor předkládá kód modelu a nabízí k využití předtrénované váhy. Pokud bude tato předtrénovaná část vynechána, je model možné použít pro libovolné téma. Autorovo schéma architektury modelu zachycuje obrázek 4.6 (převzatý z Github stránky projektu[1]). Model se řídí architekturou popsanou v [26], na vstupu přijímá barevné obrázky o rozměrech 128 × 128 pixelů a obrázky stejné velikosti i generuje.

1. `https://github.com/simoninithomas/CatDCGAN/blob/master/assets/GDSchema.png`



Obrázek 4.5: Matice záměn modelu přerozdělenými daty a jazykovým modelem RobeCzech

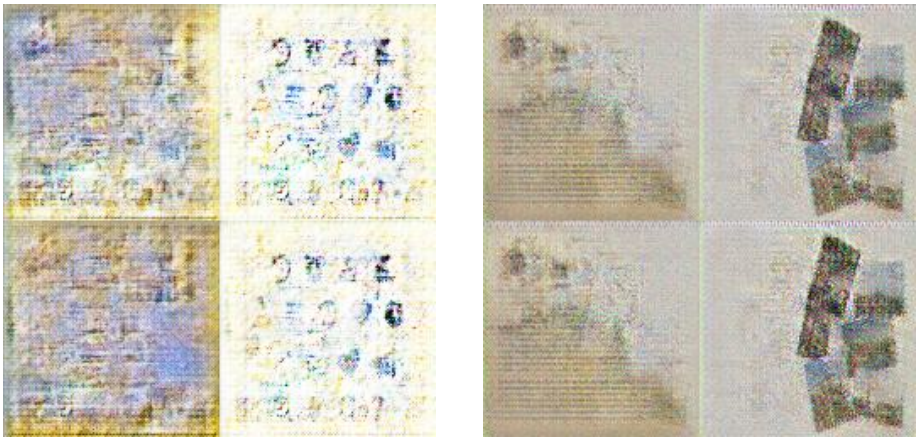


Obrázek 4.6: Schéma modelu DCGAN od Thomase Samoniniho, zdroj: Github stránka projektu [48]

Při prvním trénování modelu byly použity pouze obrázky z trénovací sady modelu obtížnosti z kapitoly 3. Tento model dokázal během učení podchytit některé znaky šifer, nicméně je velmi rychle opět ztratil. Obrázek 4.7 ukazuje příklady obrázků vygenerovaných modelem, které mají přibližné znaky šifer. Například obrázky na pravé straně obrázku 4.7b jsou velmi podobné šifře na obrázku A.9. Obrázky 4.7a připomínají tabulku drobných kreseb. Model byl celkem trénován 800 epoch s velikostí dávky 21, rychlostí učení diskriminátoru 5×10^{-5} a generátoru 2×10^{-4}. Náhled obrázků vygenerovaných během poslední epochy je zobrazen na obrázku 4.8.

Zřejmě by tedy bylo vhodné model předtrénovat a až následně ho učit generovat zadání šifer. Zadání šifer jsou však velmi různorodá (viz příloha A) dataset složený z fotografií se tedy nezdá být vhodnou volbou. Nabízí se využít ikony a drobné obrázky ve vektorové grafice, nicméně ani tyto čisté linky nejsou pro šifry zcela typické.

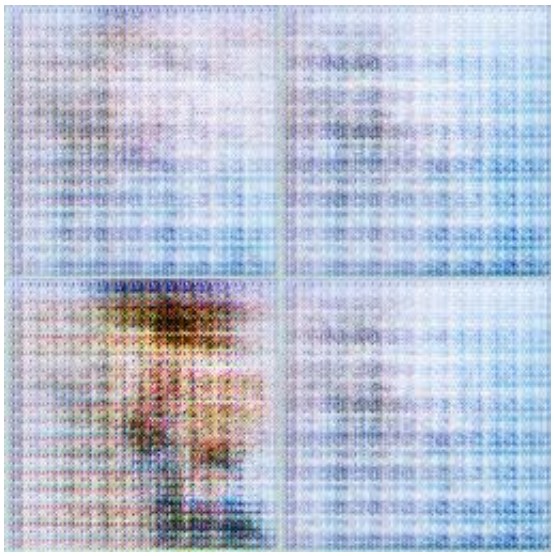
Jako zdroj obrázků k prvotnímu tréninku byl zvolen dataset Quick Draw [29]. Tento dataset reflektuje různorodost zadání šifer (jeden objekt je nakreslen mnoha různými způsoby), poskytuje širokou škálu nakreslených objektů a zároveň demonstruje, že objekt nemusí být



(a) Náhled 4 obrázků z 547. epochy trénování pouze na šifrách

(b) Náhled 4 obrázků z 740. epochy trénování pouze na šifrách

Obrázek 4.7: Náhledy výstupů první varianty generativního modelu šifer



Obrázek 4.8: Náhled 4 obrázků z 800. epochy první verze modelu

nakreslen zcela jasně (zde je to způsobeno časovým limitem, nicméně autoři šifer tento princip využívají zcela záměrně). Zároveň je tvořen čistě černobílými obrázky, to u šifer často neplatí, většinu zadání však lze bez újmy na luštitelnosti do černobílého spektra převést.

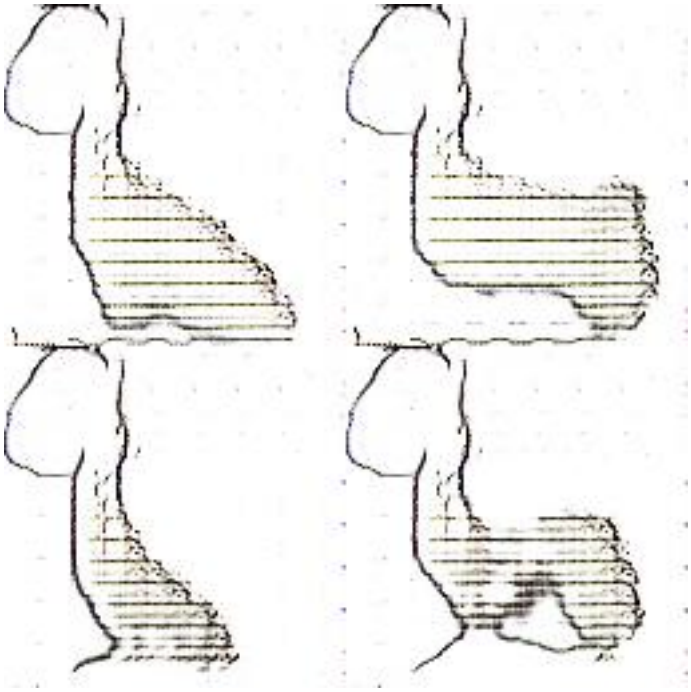
Ze zmíněného datasetu byla pro trénink modelu využita zjednodušená varianta kreseb. Jedná se tedy o kresby, které vznikly z původního datasetu pomocí těchto změn:

- zarovnání kreseb do levého horního rohu plátna, aby byla minimální hodnota rovna 0,
- uniformní naškálování kresby, maximální hodnota je 255,
- převzorkování všech tahů s odstupem 1 pixel,
- zjednodušení všech tahů pomocí Ramer-Douglas-Peucker algoritmu s hodnotou epsilon rovnou dvěma [29].

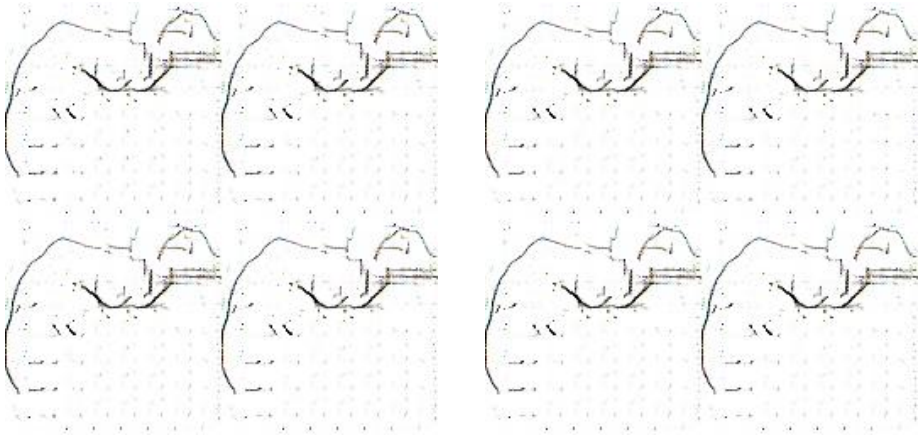
Z této sady bylo použito 150 obrázků z každé kategorie, dataset tedy celkem obsahoval 51 150 kreseb. Vzhledem k výrazně vyššímu množství dat byl model učen pouze 22 epoch, během kterých dokázal vygenerovat obrázky připomínající některé méně vydařené kresby z datasetu. Například kresby na obrázku 4.9 by mohly připomínat rychle nakresleného dinosaura, či draka bez křídel.

Takto předtrénovaný model byl následně odděleně trénován pro generování lehkých a těžkých šifer pomocí obrázků z odpovídající kategorie trénovací sady modelu predikce obtížnosti v sekci 3.1. Výsledků nejbližších k zadání šifry bylo dosaženo s rychlostí učení generátoru rovnou 3×10^{-4} a diskriminátoru 5×10^{-8} a s velikostí dávky rovnou 20. Nicméně ani tyto hodnoty model nevyvedly z předučených hodnot a oba modely následně po 40 epochách zkonvergovaly do téměř totožného výstupu (viz obrázky 4.10). Zdá se tedy, že množství vstupních obrázků (viz tabulka 2.1) je příliš malé na to, aby přineslo modelu nějakou informaci.

Z každé kategorie byl jeden obrázek ohodnocen predikčním modelem popsaným v sekci 3.1 (obrázky mají rozměr 128×128 px, proto je jejich kvalita nízká). Přestože se obrázky zdají téměř totožné, model v nich našel značné rozdíly: obrázek 4.11a byl s pravděpodobností 0,97 klasifikován jako těžká šifra (přestože generativní model cílil na



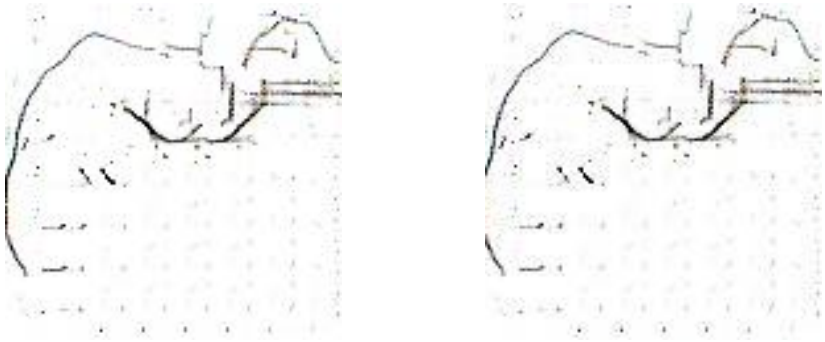
Obrázek 4.9: Náhled kresby modelu učeného na Quick Draw datasetu



(a) Náhled 4 obrázků z modelu trénovaného na lehkých šifrách

(b) Náhled 4 obrázků z modelu trénovaného na těžkých šifrách

Obrázek 4.10: Náhledy výstupů první varianty generativního modelu šifer



(a) Lehká šifra vygenerovaná modelem

(b) Těžká šifra vygenerovaná modelem

Obrázek 4.11: Náhled šifer ohodnocených modelem

lehké zadání), oproti tomu obrázek 4.11b je klasifikován jako těžký pouze s pravděpodobností 0,46.

5 Vyhodnocení a testování

Pro predikci využití nápovědy během luštění šifry je třeba předat modelu shrnutí zadání, které hráči řešili. Za tímto účelem byl vytvořen nástroj, který odhaduje obtížnost šifry. Výstup předposlední vrstvy tohoto nástroje (ve formě vektorové reprezentace zadání šifry) je společně se zbytkem dat použit pro výslednou predikci.

5.1 Vyhodnocení modelu predikce obtížnosti šifry

Vektorová reprezentace obrázku tvoří velkou část vstupu (viz tabulka D.1), její kvalita tedy výrazně ovlivňuje výsledek konečného modelu. Nejlepších výsledků dosahoval model kombinující vektorovou reprezentaci obrázků vytvořenou nástrojem *Detectron2*, vektorovou reprezentaci textů extrahovaných z obrázků vytvořenou modelem *XLM-RoBERTa* a samotné obrázky.

Z pohledu množství informací, které jsou modelu předány, lze očekávat, že extrahovaný text bude mít vliv na úspěšnost predikce. Nicméně pohled do tabulky statistik textů (5.1) tento předpoklad nepotvrzuje. Nesprávně určené šifry obsahují nejdelší text, nicméně medián délek je téměř totožný. Textů, u kterých lze určit smysl a obsahují slova z českého či anglického jazyka s malým množstvím překlepů (tedy „srozumitelných textů“) je v poměru k celkovému počtu textů více u nesprávně určených šifer. Zdá se, že jazykový model během přizpůsobování textům částečně ztratil schopnost porozumění běžnému jazyku.

Tabulka 5.1: Statistiky textů extrahovaných ze správně a nesprávně klasifikovaných šifer

	Správně určené	Nesprávně určené
Celkem šifer	58	28
Průměrná délka textu	229	411
Medián délky textu	84	83
Maximální délka textu	1671	2130
Prázdné texty	12 (~20%)	7 (25%)
Srozumitelné texty	20 (~34,5%)	16 (~57%)

Porovnáním zadání nesprávně určených šifer se nezdá, že by měly výrazné společné znaky. Šifra na obrázku A.6 byla chybně klasifikována jako těžká s pravděpodobností 0,995. Zadání obsahuje objekty uspořádané do tvaru mřížky a nejdelší text ze všech nesprávně určených šifer. Oproti tomu šifra na obrázku A.7 (opět chybně určená jako těžká s pravděpodobností 0,998) neobsahuje téměř žádný text (kromě upřesnění, kde mají hráči hledat další stanoviště, které ovšem může pomoci při řešení, proto bylo ponecháno). Objekty uspořádané do mřížky se zde vyskytují také. Zadání na obrázku A.8 však bylo určeno správně (s pravděpodobností 0,97), přestože je uspořádání velmi podobné. Naopak obrázek A.3 byl určen správně jen s pravděpodobností 0,51.

Přesnost modelu by pravděpodobně mohla být zvýšena přidáním informací o šifrách. Jako jedna z možností se nabízí přiřazení šifrovacího principu, který byl použit (viz [19]), protože například *grafické šifry* se dlouhodobě ukazují jako pro hráče obtížné [7]. Nicméně vzhledem k tomu, že šifry jsou konstruovány pro širokou veřejnost, by pravděpodobně bylo množství kategorií nízké. Například *steganografické šifry* založené na zamaskování zprávy se zde s vysokou pravděpodobností nevyskytnou, protože hráči již ví, že získaný předmět obsahuje šifru.

Další z možností je přidat texty nápověd a řešení, které v datech momentálně nejsou k dispozici. Obzvlášť popis celého postupu řešení šifry by mohl modelu pomoci rozlišit náročnost. Na druhou stranu by tento popis pravděpodobně výrazně snížil vliv obrázku na výsledek predikce. Zdá se, že bude existovat přímá úměra mezi délkou popisu řešení a obtížností šifry.

5.2 Vyhodnocení modelu predikce využití nápovědy

Všechny testované modely častěji predikují, že tým nápovědu využije (viz např. obrázky 3.4 a 4.3). To může být způsobeno nevyvážeností datové sady (68% pozitivních příkladů). Váhy tříd předané modelu pravděpodobně nedosáhly požadované rovnováhy.

Nejvyšší přesnosti vzhledem k nevyvážené sadě dosáhla architektura s přerozdělenými daty popsaný v sekci 4.1 využívající jazykový model XLM-RoBERTa. Tento model je dále analyzován.

Tabulka 5.2: Statistiky informací o týmu vzhledem k úspěšnosti predikce

Predikovaná třída	Skutečná třída	Průměr času řešení (min)	Medián času řešení (min)	Průměr poměru nápověd	Medián poměru nápověd
1	1	271	19	0,2	0,16
1	0	148	15	0	0
0	0	6,4	6,4	0	0
0	1	5	5	0,14	0

5.2.1 Analýza chyb modelu vzhledem k informacím o týmu

Porovnáním informací o týmu z validační sady přerozdělených dat popsaných v sekci 4.1 (tabulka 5.2) se zdá, že predikce modelu je silně založená na průměrné době řešení. Řádky, kterým byla predikována 1, zřejmě obsahují všechny extrémně vysoké hodnoty času (tím je způsoben vysoký průměr), nicméně i hodnota mediánu je vyšší. Výsledky srovnání hodnot pro jednu šifru (konkrétně druhou šifru hry Obrazu Josefa Temperníka) ukazují podobný trend: řádky predikované jako 1 obsahují záznamy s vyšší průměrnou dobou řešení (viz tabulka 5.3).

Detailnější pohled ukazuje v datech i lidský faktor, který model nedokáže zachytit. Tabulka 5.4 shrnuje několik vybraných týmů, pro něž byla vytvořena predikce. Všechny týmy řešily druhou šifru hry Obrazy Josefa Temperníka, informace o jejich dosavadním průchodu jsou velmi podobné (průměrný čas řešení i poměr využití nápověd), výstup modelu byl tedy pro všechny týmy téměř totožný. Přesto bylo skutečné chování týmů rozdílné, týmy 1 a 2 nápovědu využily.

5.2.2 Analýza chyb modelu vzhledem k jednotlivým šifrám

Validační sada obsahuje 14 575 záznamů týmů z řešení 88 různých šifer ze 16 her společnosti Cryptomania. Tabulka 5.5 shrnuje přehled pro šifry, u kterých byl model nejúspěšnější a nejméně úspěšný. Srovnává počty správně predikovaných týmů, nesprávně predikovaných týmů, rozdíl mezi počtem úspěchů a neúspěchů a srovnává je s počtem řádků v trénovací sadě. Šest z deseti šifer, u kterých byl model

Tabulka 5.3: Statistiky informací o týmu vzhledem k úspěšnosti predikce u 2. šifry hry Obrazy Josefa Temperníka

Predikovaná třída	Skutečná třída	Průměr času řešení (min)	Medián času řešení (min)	Průměr poměru nápověd	Medián poměru nápověd
1	1	31,3	27,8	0,625	0,75
1	0	21,91	20,91	0	0
0	0	7,8	6,8	0	0
0	1	9,3	8,6	0,11	0

Tabulka 5.4: Srovnání statistik konkrétních týmů pro druhou šifru hry Obrazy Josefa Temperníka

Číslo týmu	Predikovaná třída	Skutečná třída	Průměrný čas řešení (s)	Poměr nápověd	Predikovaná pravděpodobnost třídy 0
1	0	1	353	0	0,94
2	0	1	384	0	0,94
3	0	0	333	0	0,95
4	0	0	383	0	0,94

převážně neúspěšný, je prvních v dané hře. Model v tom okamžiku nemá žádné informace o schopnostech týmu, což může způsobovat vysokou nepřesnost. Zároveň jsou počty záznamů pro tyto šifry v trénovací i validační sadě výrazně nižší, než u těch převážně správně predikovaných (s výjimkou hry Dopis bez adresy). S vyšším počtem záznamů se množství správných predikcí zvyšuje.

Tabulka 5.5: Přehled šifer, které model predikoval převážně chybně, či převážně správně

Šifra, hra	Správně predikováno	Nesprávně predikováno	Rozdíl	V trénovací sadě
1., Dopis bez adresy	414	493	-79	1886
1., Osmý div světa	6	50	-44	116
1., Obrazy Josefa Temperníka	32	51	-19	161
6., Ztracené židovské město	29	43	-14	129
1., Avraham Harshalom	18	31	-13	84
1., Ve stínu černé vrány	8	20	-12	67
4., Ztracené židovské město	30	42	-12	133
4., Šeptající javor	3	10	-7	21
1., Ztracené židovské město	15	18	-3	51
3., Avraham Harshalom	19	20	-1	92
1., Před pikolou, za pikolou	264	32	232	570
2., Před pikolou, za pikolou	241	37	204	585
3., Před pikolou, za pikolou	238	40	198	567
7., Před pikolou, za pikolou	235	38	197	526
10., Před pikolou, za pikolou	222	33	189	498
4., Sedm klíčů	229	48	181	514
1., Sedm klíčů	224	44	180	548
9., Před pikolou, za pikolou	223	43	180	500
5., Dopis bez adresy	463	285	178	1542
3., Sedm klíčů	217	39	178	548
2., Sedm klíčů	217	43	174	551

6 Webové rozhraní

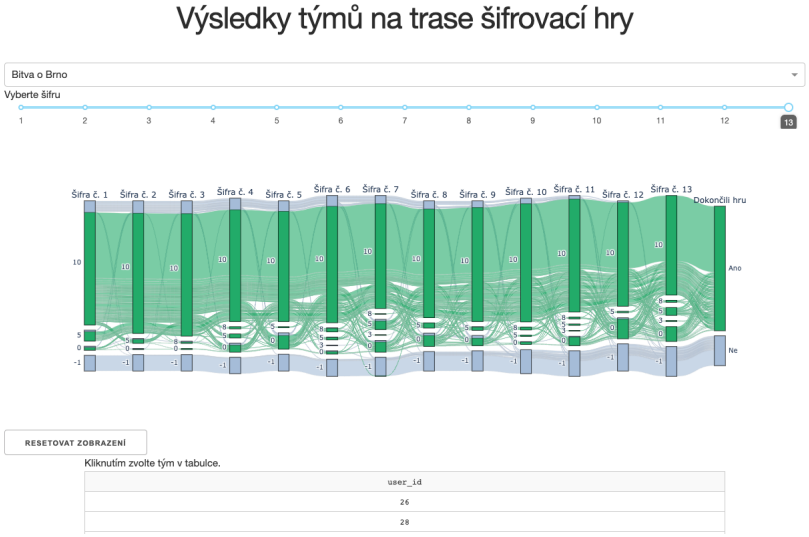
Vizualizace umožňuje pochopení obecných trendů v chování týmů. Znázorněním získaných bodů ukazuje které šifry jsou pro hráče těžké (a kde často využívají nápovědy) a zároveň demonstruje postupné ubývání týmů, které hru vzdaly. To může sloužit autorům jako podklady k úpravě hry, aby byla pro hráče příjemnější, například zjednodušením šifry, přidáním další nápovědy, či motivací k pokračování v podobě návrhu využití nápovědy. Prezentace průchodu konkrétního týmu pak dává do souvislosti predikci modelu s reálným chováním týmu a poskytuje tak představu o schopnosti modelu.

Webové rozhraní bylo implementováno ve formě Dash[1] aplikace. Stránka nabízí výběr z několika her vytvořených společností Cryptomania (Fantom Brna, Bitva o Brno, Moravský Manchester a Sedm klíčů) v podobě rozbalovacího menu. Pro zvolenou hru vykreslí souhrnný graf průchodů týmů, který zachycuje buď celou hru, nebo průchod končící šifrou, kterou si zvolil uživatel na posuvníku. Konečně v tabulce shrnuje týmy, které danou šifru překonaly (ať samostatně, či s využitím nápovědy, viz obrázek 6.1), při kliknutí na konkrétní tým v tabulce vykreslí jeho průchod hrou (opět od startu po zvolenou šifru) a zobrazí predikci modelu, zda tým při řešení následující šifry využije nápovědu, viz obrázek 6.2. Při zvolení poslední šifry hry je vypsána predikce pro tuto šifru. Živý náhled rozhraní je dostupný na sifry.okusovani.cz.

6.1 Vizualizace chování týmů během hry

Chování týmů na trase hry je reprezentováno počtem bodů, které týmy získaly během hraní dané hry. Vzhledem k tomu, že body jsou týmu odečteny pouze pokud požádá o nápovědu, lze tuto metriku bezpečně použít. Zobrazená hra Bitva o Brno se odehrává venku a týmy tedy měly možnost požádat i o nápovědu k přesunu, která je připravila o dva body. Díky tomu se ve vizualizaci objevují i bodové zisky tří a osmi bodů.

1. `https://dash.plotly.com/`



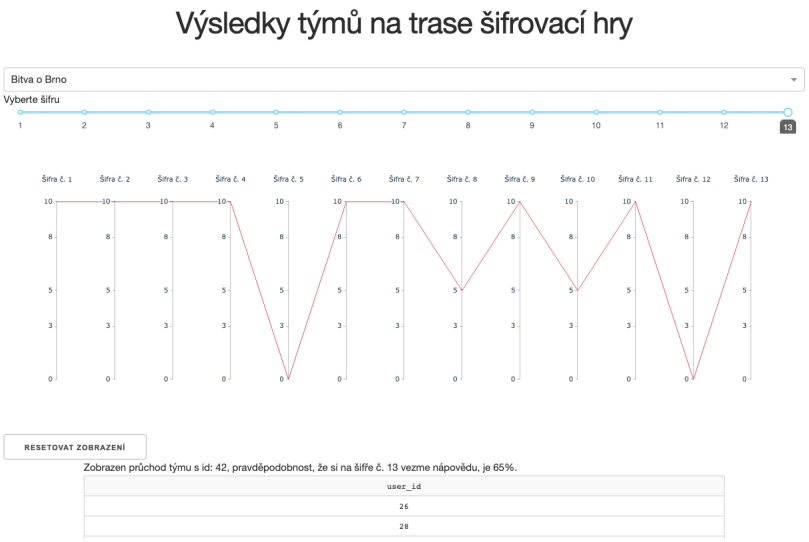
Obrázek 6.1: Náhled úvodního zobrazení webové aplikace

Graf na obrázku 6.3 je tvořen tzv. *paralelními kategoriemi*. Ukazuje skupiny týmů se stejným chováním (využily stejné nápovědy) i to, jak týmy hru postupně vzdávaly (virtuální bodový zisk -1 a šedomodrá barva). Účet týmu je vytvořen v okamžiku, kdy je zakoupena vstupenka, od toho okamžiku mají týmy minimálně rok na to hru odehrát [44]. Tím se do databáze dostávají týmy, které hru nikdy neodstartovaly, což vysvětluje týmy, které nedokončily ani první šifru.

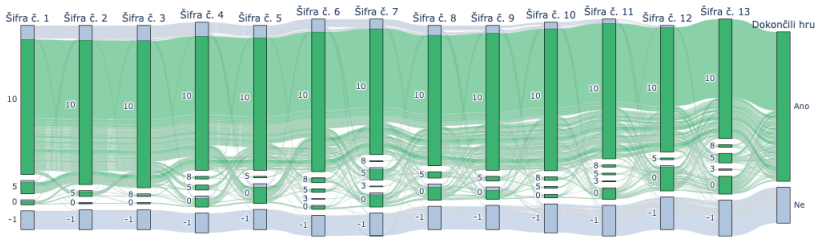
Vizualizace byla vytvořena pomocí nástroje Plotly[2], díky čemuž je vysoce interaktivní. Uživatel má možnost měnit pořadí os se šiframi či přesouvat úsek s konkrétním bodovým ziskem na ose zvolené šifry a tím hledat závislosti.

V okamžiku, kdy uživatel vybere konkrétní tým v tabulce ve spodní části stránky, je vykreslen průchod daného týmu (viz obrázek 6.2) a spočítána predikce modelu popsaného v kapitole 3. Při změně šifry, pro kterou se vykreslují data, je graf překreslen a predikce přepočítána (viz obrázek 6.4). Pokud se uživatel chce vrátit k souhrnnému pohledu na chování týmů, stiskne tlačítko s nápisem „RESETOVAT ZOBRAZENÍ“ a vizualizace se opět vrátí k zobrazení na obrázku 6.3.

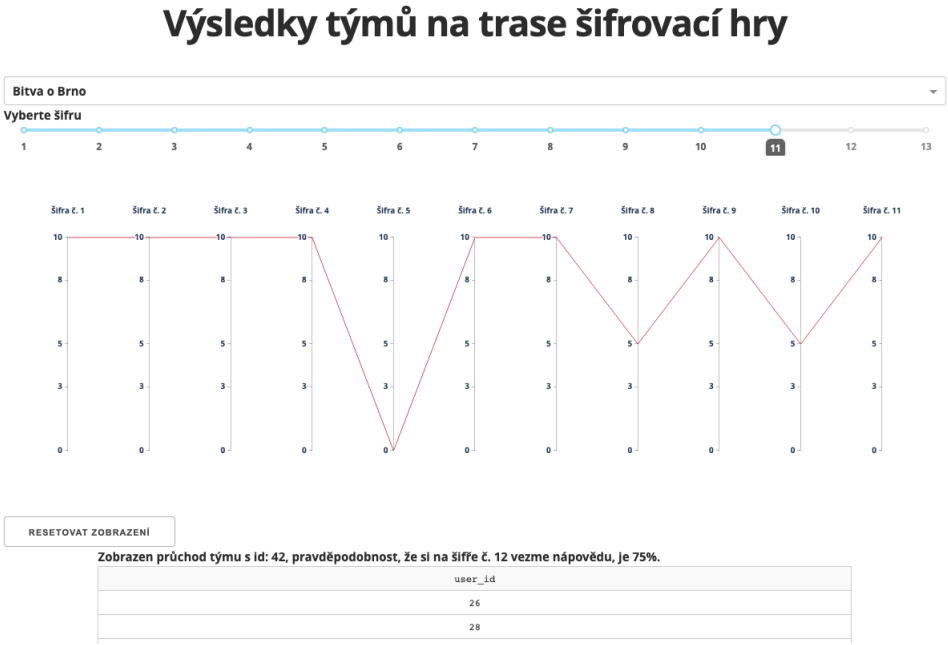
2. `https://plotly.com/`



Obrázek 6.2: Náhled zobrazení průchodu jednoho týmu



Obrázek 6.3: Průchod týmů hrou Bitva o Brno



Obrázek 6.4: Náhled zobrazení začátku průchodu jednoho týmu

7 Použité nástroje

Celá práce byla zpracována v programovacím jazyce Python[1]. Téměř všechny modely byly vytvořeny na základě knihovny TensorFlow[2], jedinou výjimku tvoří model generující vektorovou reprezentaci obrázků popsaný v sekci 3.1, který je založen na knihovně PyTorch[3]. Kromě speciálních knihoven popsaných v kapitole 1 byly pro tvorbu modelů využity standardní knihovny pro zpracování dat jako `pandas`[4] a `numpy`[5]. Vizualizace byly vytvořeny s pomocí knihoven `scikit-learn`[6] (matice záměn), `matplotlib`[7] (vývoj přesnosti) a `plotly`[8] (vizualizace

1. `https://www.python.org/`
2. `https://www.tensorflow.org/`
3. `https://pytorch.org/`
4. `https://pandas.pydata.org/`
5. `https://numpy.org/`
6. `https://scikit-learn.org/`
7. `https://matplotlib.org/`
8. `https://plotly.com/`

chování týmů). Webové rozhraní popsané v kapitole 6 bylo vytvořeno s pomocí knihovny `Dash`[9].

Zdrojové kódy jsou k dispozici na github.com/eliasbar1/diplomka.

9. `https://dash.plotly.com/`

8 Další rozvoj tématu

Jako další možnost klasifikace obtížnosti obrazového zadání šifry se nabízí využití modelu DCGAN jako extraktoru rysů. Aby však byl tento přístup možný, bylo by vhodné modelu předložit více vstupních dat a dosáhnout tak lepších výsledků. Jako zdroj těchto dat se nabízí šifry z dalších „velkých šifrovacích her“ (TMOU, Matrix, Bedna, ...). Ty by mohly sloužit jako základ pro generativní model a samotné učení obtížnosti by bylo následně realizováno se stávající datovou sadou. Tyto šifry by mohlo být možné doplnit např. výsledky některého z volně dostupných *text-to-image* modelů (např. `DALL-E`[1], `Midjourney`[2], či `DeepAI`[3]). Dále by mohlo být zajímavé využít *image-to-text* model a poskytnout modelu i textový popis šifry.

Kromě generování obrázků je možné vygenerovat i další datové body týmů a tím zvýšit velikost trénovací sady, například pomocí průměru nejbližších sousedů.

Rozdělení trénovací a testovací sady by mohlo být realizováno podle týmů. Tedy tým je na začátku určen jako trénovací a celý jeho průchod je zařazen do trénovací sady a stejně tak pro validační sadu. Aby byla data vyvážená, bylo by vhodné týmy dopředu ohodnotit (např. pomocí metrik zmiňovaných v [19]), aby bylo zaručeno rovnoměrné zastoupení týmů, které hru úspěšně dokončily, těch neúspěšných, hojně využívajících nápovědy a samostatných atp.

1. `https://labs.openai.com/`
2. `https://midjourney.com/`
3. `https://deepai.org/machine-learning-model/text2img`

9 Závěr

Práce představuje problematiku šifrovacích her. Ve stručnosti shrnuje jejich historii a českou unikátnost v celosvětovém měřítku a následně popisuje „velké šifrovací hry“ a jejich komerční variantu. V rámci shrnutí projektů na podobné téma přirovnává šifry a logické úkoly k matematickým problémům a popisuje výzkumy zabývající se úspěšností studentů při jejich řešení.

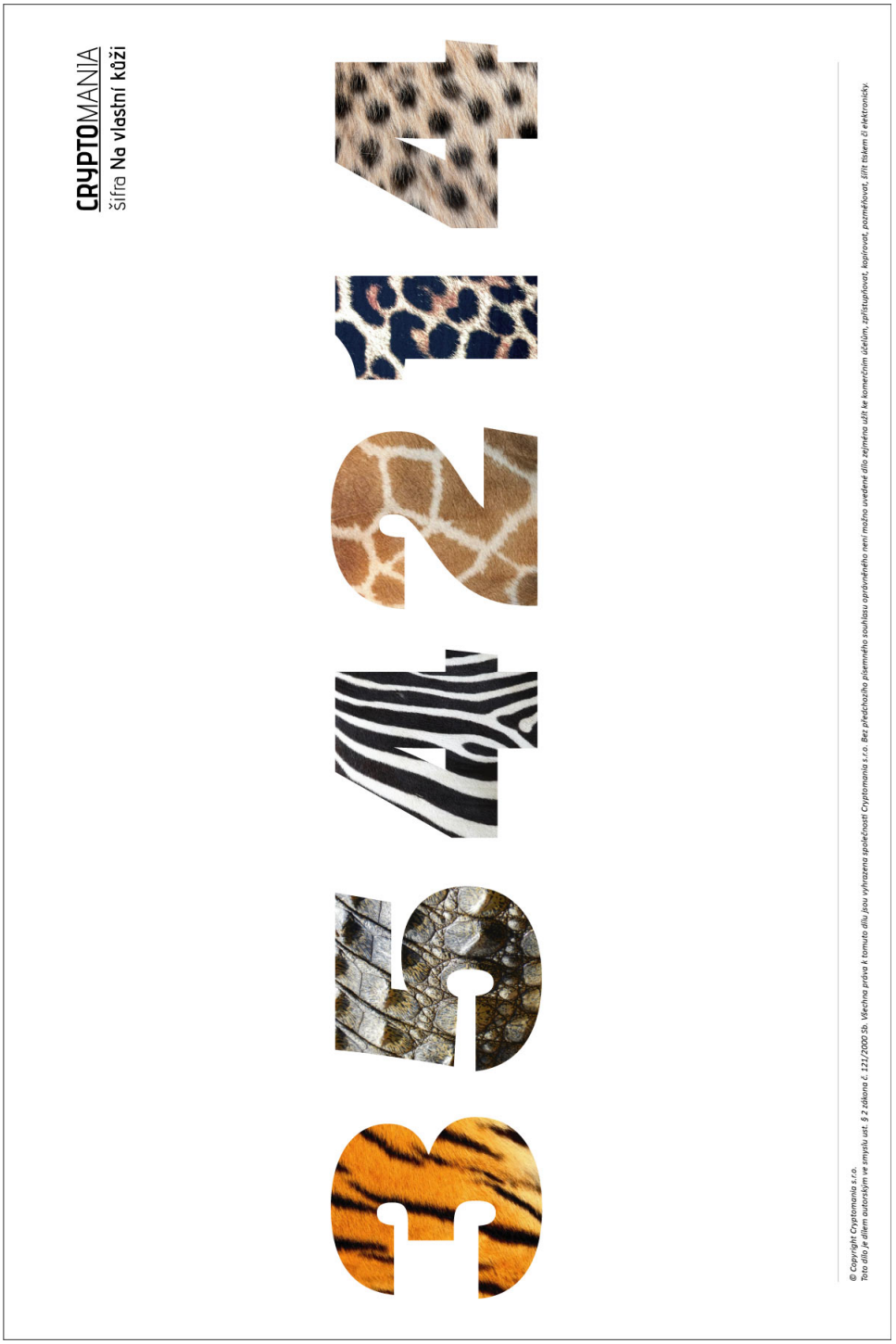
Ve druhé části jsou porovnány různé varianty modelu klasifikujícího obtížnost šifry na základě jejího obrazového zadání. Výsledný model využívá obrázky spolu s jejich vektorovou reprezentací (vytvořené nástrojem *Detectron2*) a extrahovanými texty.

Tyto vektorové reprezentace vytvořené modelem predikce obtížnosti jsou následně využity modelem predikujícím zda tým během hraní šifrovací hry požádá o nápovědu. Práce popisuje otestované varianty tohoto modelu, který kromě zmíněných vektorových reprezentací zpracovává informace o dosavadním postupu týmu hrou, informace o umístění šifry ve hře a o šifrovací hře samotné. Nejvyšší přesnosti predikce dosáhla architektura, která zpracovávala texty předtrénovaným multilingvním modelem. Nicméně i tato varianta narážela na malé množství dat a lidský faktor při jejich vzniku. Zda tým o nápovědu požádá, je z velké části psychologická otázka. Zda jsou jedinci schopni poznat, že potřebují pomoc, a zda o ni dokáží požádat je tématem řady psychologických studií [14].

Predikce tohoto modelu jsou spolu s vizualizací chování týmů na trase hry prezentovány ve formě interaktivní webové aplikace.

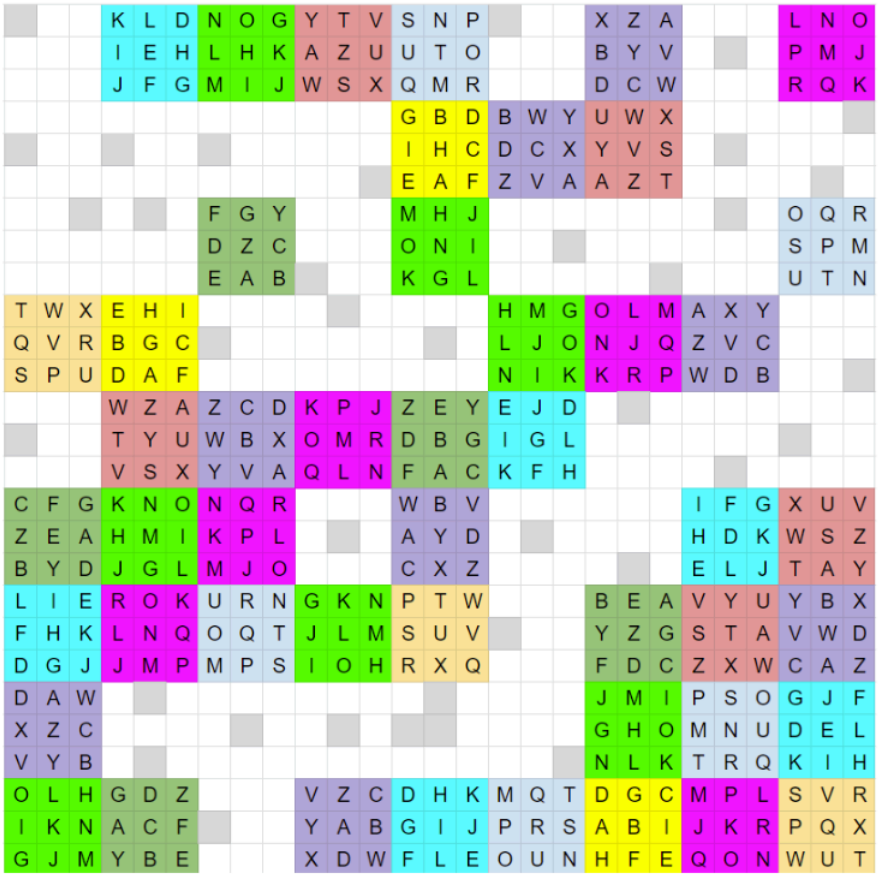
A Ukázky šifer

Obrázek A.1: Ukázka šifry ze hry pro veřejnost

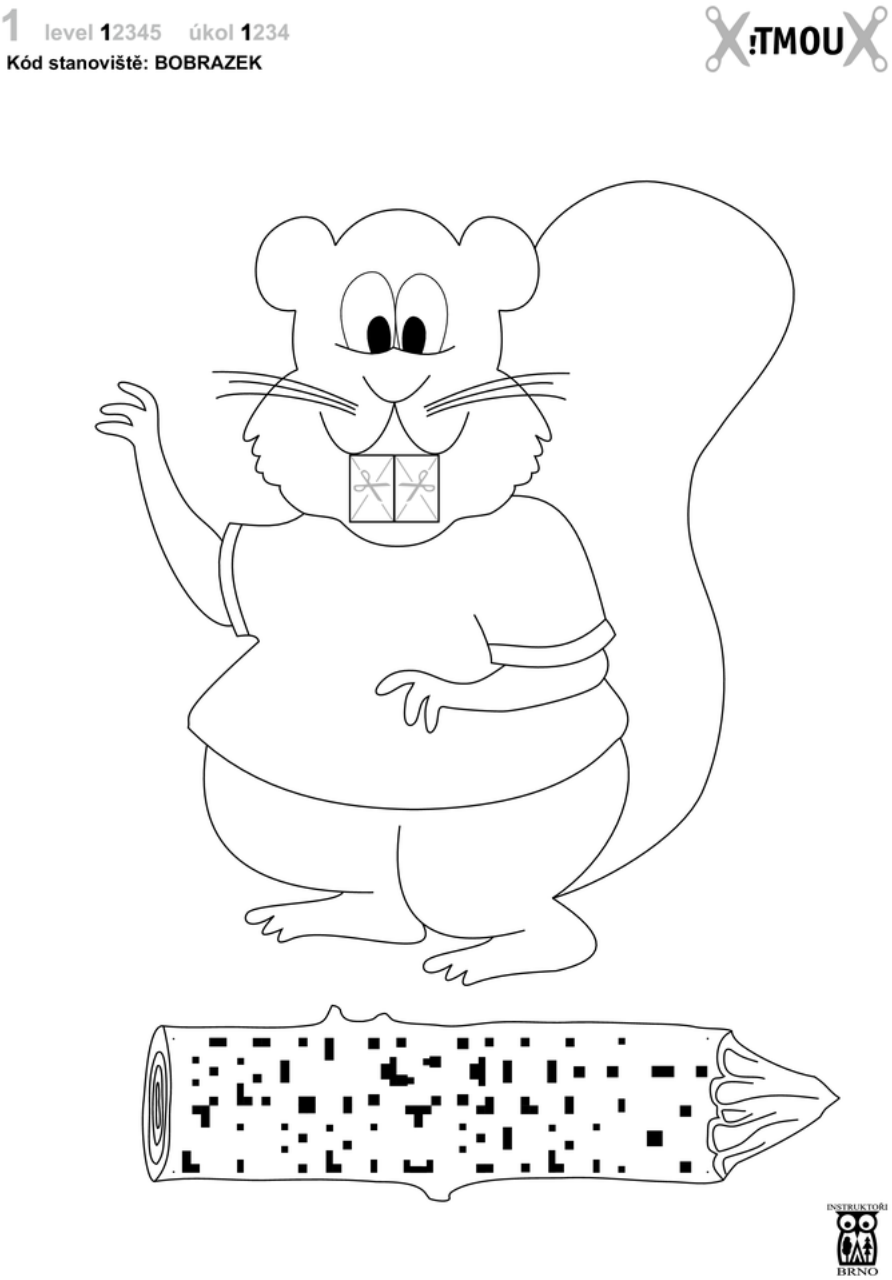


Obrázek A.2: Ukázka šifry z firemního kurzu

Obrázek A.3: Ukázka těžké šifry z šifrovací hry DNEM

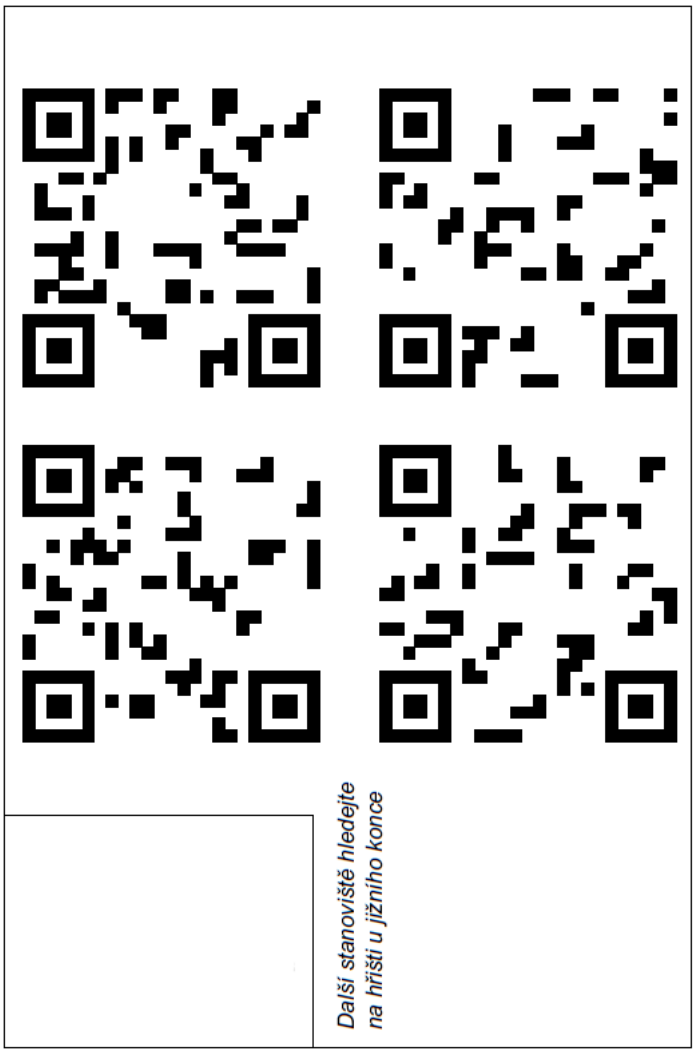


Obrázek A.4: Ukázka lehčí varianty šifry z šifrovací hry DNEM

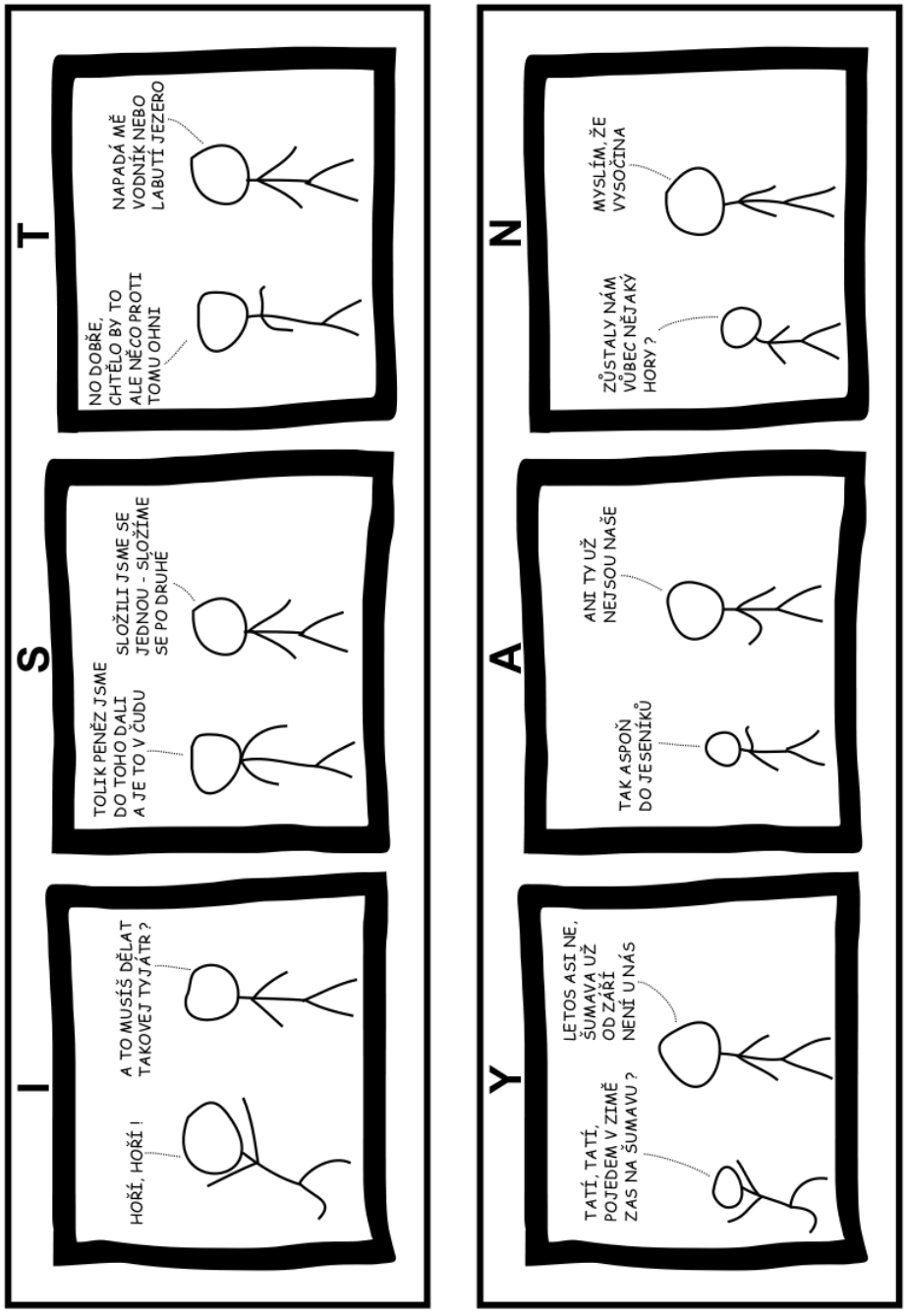


Obrázek A.5: Ukázka úvodní šifry z šifrovací hry TMOU

Obrázek A.6: Ukázka nesprávně klasifikované lehké šifry



Obrázek A.7: Ukázka další nesprávně klasifikované lehké šifry



Obrázek A.8: Ukázka správně klasifikované těžké šifry

Obrázek A.9: Ukázka šifry z Facebooku firmy

B Statistiky doprovodných textů k šifrám

Následující tabulky shrnují počty slov jednotlivých textů k šifrám. Hry, které fungují čistě online zpravidla neobsahují text na cestu, nicméně tato funkcionalita je občas používána pro zobrazení textu doplňujícího příběh (obvykle u prvního či posledního stanoviště hry), toto využití se objevuje například u hry Záhada pražských Amazonek.

Oproti to mu většina městských her má příběh rozdělen. Výjimka nastává v okamžiku, kdy mají hráči řešit šifru během přesunu (např. stanoviště 5, 7, 9 hry Bitva o Brno), nebo je šifra například bonusová (stanoviště 8 hry Moravský Manchester).

Tabulka B.1: Počet slov v doprovodných textech k šifrám fyzických her

Začátek tabulky			
Šifra č.	**Slov v textu na cestu**	**Slov v textu k šifře**	**Slov celkem**
hra Avraham Harshalom			
1	166	128	294

Pokračování tabulky B.1			
Šifra č.	**Slov v textu na cestu**	**Slov v textu k šifře**	**Slov celkem**
2	21	111	132
3	83	135	218
4	220	407	627
5	154	132	286
6	229	288	517
hra Bitva o Brno			
1	0	108	108
2	41	42	83
3	116	110	226
4	42	98	140
5	0	70	70
6	73	46	119
7	0	52	52
8	54	138	192
9	0	51	51
10	43	52	95
11	59	69	128
12	0	28	28
13	0	96	96
hra Fantom Brna			
1	0	93	93
2	0	141	141
3	0	137	137
4	0	168	168
5	0	117	117
6	0	131	131
7	0	124	124
8	0	181	181
9	0	158	158
10	0	106	106
11	0	134	134
hra Šeptající javor			
1	0	233	233
2	111	120	231
3	179	209	388

Pokračování tabulky B.1			
Šifra č.	**Slov v textu na cestu**	**Slov v textu k šifře**	**Slov celkem**
4	102	120	222
5	86	117	203
6	102	134	236
7	158	146	304
hra Královské mysterium			
1	0	87	87
2	125	38	163
3	77	77	154
4	267	32	299
5	0	61	61
6	0	82	82
hra Moravský Manchester			
1	60	123	183
2	70	173	243
3	87	116	203
4	99	119	218
5	95	64	159
6	99	87	186
7	177	142	319
8	0	159	159
hra Staré pověsti české			
1	0	5	5
2	60	75	135
3	72	80	152
4	61	113	174
5	47	65	112
6	24	66	90
7	49	97	146
8	47	102	149
9	49	75	124
10	38	121	159
11	42	74	116
12	41	53	94
hra Ztracené Židovské město			
1	120	54	174

Pokračování tabulky B.1			
Šifra č.	**Slov v textu na cestu**	**Slov v textu k šifře**	**Slov celkem**
2	69	75	144
3	134	101	235
4	81	85	166
5	44	77	121
6	252	114	366
Konec tabulky			

Tabulka B.2: Počet slov v doprovodných textech k šifrám online her

Začátek tabulky			
Šifra č.	**Slov v textu před šifrou**	**Slov v textu k šifře**	**Slov celkem**
hra Záhada pražských Amazonek			
1	196	182	378
2	0	122	122
3	0	130	130
4	0	119	119
5	0	128	128
hra Osmý div			
1	107	63	170
2	0	94	94
3	0	103	103
4	0	119	119
5	0	126	126
6	0	96	96
7	0	100	100
8	0	87	87
hra Dopis bez adresy			
1	0	234	234
2	0	97	97
3	0	115	115
4	0	132	132
5	0	92	92
hra Příběh Enigmy			
1	0	98	98
2	0	139	139

Pokračování tabulky B.2

Šifra č.	Slov v textu před šifrou	Slov v textu k šifře	Slov celkem
3	0	183	183
4	0	228	228
5	0	242	242
6	0	207	207
7	0	247	247
8	0	181	181
9	0	353	353
10	0	268	268
hra Sedm klíčů			
1	0	240	240
2	0	159	159
3	0	258	258
4	0	237	237
5	0	186	186
6	0	216	216
7	0	153	153
hra Loupež po telefonu			
1	0	98	98
2	0	139	139
3	0	183	183
4	0	228	228
5	0	242	242
6	0	207	207
7	0	247	247
8	0	181	181
9	0	353	353
10	0	268	268
hra Před pikolou, za pikolou			
1	0	65	65
2	0	193	193
3	0	265	265
4	0	271	271
5	0	117	117
6	0	159	159
7	0	297	297

Pokračování tabulky B.2			
Šifra č.	**Slov v textu před šifrou**	**Slov v textu k šifře**	**Slov celkem**
8	0	240	240
9	0	316	316
10	0	357	357
hra Ve stínu černé vrány			
1	0	175	175
2	0	184	184
3	0	122	122
4	0	222	222
5	0	170	170
6	0	152	152
7	0	115	115
8	0	201	201
hra Obrazy Josefa Temperníka			
1	0	170	170
2	0	70	70
3	0	89	89
4	0	69	69
5	0	94	94
6	0	69	69
7	0	129	129
8	0	100	100
9	0	155	155
10	0	65	65
Konec tabulky			

C Ukázky textů extrahovaných z obrazových zadání jednotlivých šifer

C.1 Text 1

```
008} © oo Ha? 4000S! 400! 7 (4-8-4-9)
! 35 © o! 35 00 RSCD of 35 00 LOVE 0! 10
001587 0039300460 © cot e?500063/|©
0! 80.60 aah e? 85 00 Ye? 500 = 00% © co Ml

o! 35 00 Be? 45 0000 o! 4000 & 9? 4500
e! 25 co Fa? 80 © co Ge? 35 © oo vt o! 100 00 Ga! 40
00 a8 5 co « © wt EH a? 55 0010, Ze? 10.00 F448 15 00 Sp
00 8% |e? 80.00 Fe? 10.00 Fs! 20 00 ("9 © co Are? 65 00%. 2 mm
o! 15.00 © © ttt? 100 00 @ 4? 15 © Ge! % (18) o? 5.0083
wep Oe! (64)
```

C.2 Text 2

```
    Pofadi Jméno Cas

1. Honza 0:58:30,5 0:18:37
2. Karel 1:01:07,9 0:19:41
3. Adam 1:01:09,8 0:18:20
4. Petr 1:03:59,3 0:19:42
5. Tomas atti 0:19:45
6 Lukas DNF 0:18:03

ADAM

Meziéas po stielbé vieze

‘Amatérského biatlonového zavodu se ziiéastnilo 6 závodnikti:
Adam, Honza, Karel, Tomas, Petr a Lukas.
Nize vidite jejich vjsledky a z4znamy
ze stielby. P7i stfelbé mali z4vodnici 5 stfel
```

```
bez moznosti dobijeni.

0:41:15
0:41:03
0:41:45
0:45:17
0:48:55
0:40:28

HONZA
O®@@OO
Onex Nex }
eorer XT)
OOOO®e
KAREL
TOMAS
OOO8OO
Oe@O8@O
O®OO®
@Oece
PETR
LUKAS
OOOe0®8
O®@OOO
@OOOe0
@OOe@@O
Meziéas po stielbé ve stoje
```

C.3 Text 3

```
4/11
4/7
3/13
yD
```

C.4 Text 4

```
    1s

| a > am - ee . eee
a <eum SYRIA LL ANA . A REGS Aw
<Maie. SI See SVG MSV
- ACY oho ms
[A 8 AOA} ot
ZS STON I 7 eo
ASSES ESS RAZ BA BK Ue ere
= WAG GO ar AN
NEL SS
Sn KA
eaIS 4 nl 2 m
‘ a q aaa sy]
yt : Z NG) AS de ENS
4 OBS A S| Be ee
4 ares Ris
Z y
a) RY
02
X]
w
2)
PH
Pe SA
Ny) AZoees
NINA :
BEG DS
ACS J Y
av,
as
fl)
Wg
TP
}
ras
```

C.5 Text 5

```
    ministerstvo pro pruimysl a [| [| [| T]
L JE JE IE] nepoti zebra

brnénsky noéni | | T [

LE JEJE] potraw travicim traktem
lel OCG se

vychodoteské mésto IIT IE

LIL LL] vetuze sma rize
wer III

[A | ml ome] [AIL JL JL LY tins

[JL JEL] nasiestych vozidet

kruhovy I LILI

splachovaci TE LIE]

LIL LIL] se ztv0ram
bolestivy CI ILIE]

JL JL_JL_] nae totetemi
moves SII

LE JE EJ ne eatnici

L JE JE IE] evita a Metodsje
```

C.6 Text 6

```
     DNEM

UZ CTRNACT LET JEDEN KVETNOVY DEN
SANCI CHCI DOSTAT A SPLNIT SI SEN
ROZLUSTIM TY JEJICH ZALUDNE ZNAKY
ZNAM REKY SVETA | ROZPOZNAM PTAKY,

NA PISMO INKU JA JSEM SVETOZNALEC
V LATINE PRELOZIM KOTNIK Cl PALEC
JEN NEVIM PROC NENi DOVOLEN MOBIL
GOOGLE BY REBUSY JEDNA DVE PROBIL

TEZCE JSEM MAKAL A VYHRAJU TRICKO
PRIPRAVIM TI RADOST MA POSTAVICKO
LETOS JSEM ZRALY NA OKAMZIK SLAVY
TYM TVORi JEN DOBRE MYSLICi HLAVY
```

D Ukázka vstupu modelu predikce nápovědy

Vzhledem k tomu, že *Obtížnost obrazového zadání šifry* je tvořena výstupem předposlední vrstvy modelu popsaného v kapitole 3.1 a má délku 10400 prvků, není tento vstup zobrazen celý.

Tabulka D.1: Ukázka vstupu modelu predikce nápovědy

Veličina	Prvků	Hodnota
Poměr dosavadního využití nápověd a Průměrný čas strávený na šifře	2	0,125, 807,5
Poměrné pořadí šifry ve hře	10	0, 0, 0, 0, 0, 1, 0, 0, 0, 0
O jakou hru se jedná	50	0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
Obtížnost obrazového zadání šifry	10400	0,0, 0,0, 73,04374, . . . 1,3758706, -0,27289584, 0,7335073
Příběh k šifře		Stojíte u domu číslo sedm v ulici Novákových. V poštovní schránce je důvěrně známá hnědá obálka. Poslední šifra. Baví tě to. Těšíš se na seznámení s Tomášem a zjistit, jak se takové šifry dělají. Zároveň ti je trochu líto, že tahle nečekaná zábava už je skoro u konce, chtěl bys to někdy zopakovat. Možná byste mohli společně se Šárkou vyrazit brzy na nějakou další šifrovačku. To už ale čtete poslední Tomášovu zprávu. Čekám na tebe v hospodě U Červeného . . . Zbytek musíš doplnit z výsledku šifry. Makej, už je to jenom kousek!
Požádal tým o nápovědu?	1	1

E Přehled dat z her pro veřejnost

Tabulka E.1: Přehled dat z her pro veřejnost

Začátek tabulky			
Pořadí šifry ve hře	**průměrný čas (minuty)**	**label**	**sada**
hra Avraham Harshalom			
1	10,0	easy	train
2	9,2	easy	train
3	14,0	easy	train
5	10,9	easy	val
hra Osmý div světa			
1	21,6	hard	train
2	30,4	hard	train
3	64,1	hard	train
4	57,4	hard	train
5	21,0	hard	train
7	39,6	hard	train
hra Dopis bez adresy			
1	8,7	easy	train
2	12,9	easy	train
4	20,5	hard	train
5	14,1	easy	train
hra Příběh Enigmy			
1	12,4	easy	train
2	33,9	hard	train
4	61,6	hard	train
5	61,4	hard	train
6	24,9	hard	val
7	23,8	hard	train
8	53,1	hard	train
10	26,0	hard	train
hra Fantom Brna			
2	4,4	easy	val
3	6,8	easy	train
4	8,5	easy	train

Pokračování tabulky E.1

Pořadí šifry ve hře	průměrný čas (minuty)	label	sada
5	19,7	hard	train
6	13,4	easy	train
7	22,3	hard	train
9	37,2	hard	train
10	15,6	easy	train
hra Šeptající javor			
3	9,0	easy	train
4	13,9	easy	train
6	14,4	easy	train
hra Sedm klíčů			
1	11,3	easy	train
2	27,0	hard	train
3	20,0	hard	train
4	29,5	hard	train
5	45,0	hard	train
6	6,6	easy	train
hra Královské mysterium			
1	13,5	easy	train
2	15,9	easy	train
3	28,2	hard	train
6	17,1	easy	train
hra Loupež po telefonu			
1	18,2	hard	val
2	3,9	easy	train
3	6,9	easy	train
5	44,4	hard	train
8	18,8	hard	train
hra Moravský Manchester			
1	57,5	hard	train
3	10,4	easy	val
4	14,5	easy	train
6	13,9	easy	train
7	13,4	easy	val
8	14,0	easy	train

Pokračování tabulky E.1

Pořadí šifry ve hře	průměrný čas (minuty)	label	sada
hra Před pikolou, za pikolou			
1	19,7	hard	train
2	28,1	hard	train
3	48,7	hard	val
7	19,3	hard	train
8	128,6	hard	train
9	58,4	hard	train
10	54,9	hard	train
hra Staré pověsti české			
4	16,1	easy	train
5	10,7	easy	train
6	4,9	easy	train
7	2,9	easy	train
8	18,1	hard	train
9	5,1	easy	train
11	5,9	easy	val
12	22,9	hard	train
hra Obrazy Josefa Temperníka			
1	20,8	hard	train
2	7,7	easy	val
3	49,8	hard	val
4	90,1	hard	train
5	112,0	hard	train
6	173,1	hard	val
7	204,5	hard	train
8	12,2	easy	train
hra Ve stínu černé vrány			
1	6,2	easy	val
4	55,6	hard	val
5	9,2	easy	train
6	5,1	easy	train
7	34,5	hard	train
8	14,6	easy	val
hra Ztracené židovské město			

Pokračování tabulky E.1

Pořadí šifry ve hře	průměrný čas (minuty)	label	sada
1	17,5	easy	train
3	18,1	hard	train
4	10,9	easy	train
5	17,2	easy	train
6	23,9	hard	train

Konec tabulky

F Ukázková data z herního systému Cryptomania pro hru Bitva o Brno

Zde je ukázka exportu dat pro jednu z Cryptomania her pro veřejnost (konkrétně pro hru Bitva o Brno[1]). Export se skládá ze tří souborů:

`FORMAT.md`, který obsahuje dokumetaci samotného exportu, která je v anglickém jazyce,

`structure.json`, který shrnuje strukturu hry - jak jsou na sebe jednotlivé úkoly navázány

`events.json` obsahující všechny události hry s časovou známkou.

F.1 Formát exportovaných dat (`FORMAT.md`)

The export contains three files:

- `structure.json` describing how the game is composed and interconnected.
- `events.json` listing all events that happened in the game (team actions).
- `FORMAT.md` this file with documentation.

F.1.1 Structure

It is a JSON file with following structure:

- `info.name` with name of the game.
- `info.trail_id` with internal trail ID (WordPress post ID).
- `info.blog_id` with WordPress blog ID.
- `sets` with array of sets of this game, one set contains following properties:
  - `set_id`
  - `name`
  - `slug` with the URL name, used for alphabetical sorting in ascending manner.
  - `last_modified` with datetime.

1. `https://trails.cryptomania.cz/trail/bitva-o-brno/`

  - `fixed_points` with number of points for successful solutions of task in this set (without any hint used).
  - `is_bonus_set` with boolean whether this set is a bonus set.
  - `start_time` with time, only if set.
  - `end_time` with time, only if set.
  - `non_linear` with boolean whether the assignment in the set can be solved in any order.
  - `assignments` with array of IDs of assignments (see structure below).
  - `dependencies` describing when this set should be open/available:
    * `collections` with array of sets IDs after their completion this set should be opened / made available.
    * `lower_bound_points` with total team points when this set should opened / made available.
- `assignments` with array of assignments, one assignment contains following properties:
  - `assignment_id`
  - `name`
  - `slug` with URL name.
  - `last_modified` with datetime.
  - `has_access_code` with boolean whether the given assignment has an access code.
  - `hints` with array of hints for the the assignment, each contains following properties:
    * `malus` with point penalization, `0` on total hints where no points are awarded for the assignment (except penalty for access hint).
    * `is_total` with boolean whether this is a total hint or only partial.
    * `code_to_show`
    * `time_to_show`
  - `dependencies` describing when this assignment should be open/available:
    * `tasks` with array of assignments IDs after their completion this set should be opened / made available.

* `lower_bound_points` with total team points when this assignment should opened / made available.

F.1.2 Events

It is a JSON file with list of events objects, each having `event_id`, `user_id` and `type`... Other properties differs by event types, see description below.

The events are "sorted"by `user_id` in ascending manner and then by `event_id` in ascending manner. However this sorting is not perfect as aggregated events are at the place of their first saving instead of last saving (as would make sense).

Event types are:

- `GAME_START`: `time`. Planned time of start.
- `GAME_STARTED`: `time`. Actual start.
- `TASK_START`: `time` and `task_id`. Opening the task.
- `TASK_HINT`: `time` and `task_id` and `task_hint_subid` describing which hint was taken (0, 1 ...). Opening of hint for the task.
- `TASK_TRANSITION_HINT`: `task_id`. Opening of the transition hint.
- `TASK_WRONG_ANSWER`: `task_id`, `time` and `value`. Particular wrong answer.
- `TASK_CORRECT_ANSWER`: `task_id`, `time` and `value`. Particular correct answer as now there can be alternative answers.
- `TASK_FINISHED`: `time` and `task_id`. Finishing the task (successfully or with hint)
- `GAME_FINISHED`: `time`
- `LAST_PROFILE_CHANGE`: `time` when the team has changed its profile last time.
- `LAST_PROFILE_MEMBERS`: `value` number of team members (as updated by the team themselves).

Aggregated (computed by the application later in the past, also known as cached) events, which may not be fully correct, especially in corner cases, are:

- `TASK_TIME`: `task_id` and `value` with number time in seconds. Task solving time.
- `TASK_POINTS`: `task_id` and `value` with awarded number of points. Awarded number of points.
- `GAME_POINTS_SUM`: `value`. Total game points.

- `GAME_TIME_SUM`: `value`. Sum of time of task in seconds.
- `GAME_TIME_MAX`: `value`. Time of last solved task.

And all aggregated events have property `aggregated` set to `true`.

F.1.3 Notes

All timestamps are in year-month-day hour:minutes:seconds format in Europe/Prague timezone.

Rarely event can appear twice, this is due unprevented multiple user submissions.

F.2 Struktura hry (`structure.json`)

```
{
    "info": {
        "name": "Bitva o Brno",
        "trail_id": 13,
        "blog_id": 3
    },
    "sets": [
        {
            "set_id": 48,
            "name": "Bitva o Brno",
            "slug": "bitva-o-brno",
            "last_modified": "2015-04-02 23:23:25",
            "fixed_points": 10,
            "assignments": [
                20,
                21,
                23,
                29,
                27,
                31,
                33,
                35,
                37,
                40,
                42,
                44,
                46
            ],
            "dependencies": {
                "lower_bound_points": 0
            }
        }
    ],
    "assignments": [
        {
            "assignment_id": 20,
            "name": "První úkol",
            "slug": "01",
            "last_modified": "2020-10-10 10:30:00",
            "has_access_code": true,
            "hints": [
                {
                    "malus": 5,
                    "is_total": false,
                    "code_to_show": "",
                    "time_to_show": ""
                },
                {
                    "malus": 0,
                    "is_total": true,
                    "code_to_show": "",
                    "time_to_show": ""
                }
            ],
```

```
        "dependencies": {
            "lower_bound_points": 0
        }
    },
    {
        "assignment_id": 21,
        "name": "Historické Brno",
        "slug": "02",
        "last_modified": "2020-05-27 22:48:59",
        "has_access_code": true,
        "transiton_malus": 2,
        "hints": [
            {
                "malus": 5,
                "is_total": false,
                "code_to_show": "",
                "time_to_show": ""
            },
            {
                "malus": 0,
                "is_total": true,
                "code_to_show": "",
                "time_to_show": ""
            }
        ],
        "dependencies": {
            "tasks": [
                20
            ],
            "lower_bound_points": 0
        }
    },
    {
        "assignment_id": 23,
        "name": "Kniha",
        "slug": "03",
        "last_modified": "2021-07-22 10:00:46",
        "has_access_code": true,
        "transiton_malus": 2,
        "hints": [
            {
                "malus": 5,
                "is_total": false,
                "code_to_show": "",
                "time_to_show": ""
            },
            {
                "malus": 0,
                "is_total": true,
                "code_to_show": "",
                "time_to_show": ""
            }
        ],
        "dependencies": {
```

```
            "tasks": [
                21
            ],
            "lower_bound_points": 0
        }
    },
    {
        "assignment_id": 29,
        "name": "Páté kolo u vozu",
        "slug": "04",
        "last_modified": "2020-10-10 10:33:14",
        "has_access_code": true,
        "transiton_malus": 2,
        "hints": [
            {
                "malus": 5,
                "is_total": false,
                "code_to_show": "",
                "time_to_show": ""
            },
            {
                "malus": 0,
                "is_total": true,
                "code_to_show": "",
                "time_to_show": ""
            }
        ],
        "dependencies": {
            "tasks": [
                23
            ],
            "lower_bound_points": 0
        }
    },
    {
        "assignment_id": 27,
        "name": "Podzemní sýpka",
        "slug": "05",
        "last_modified": "2020-05-27 22:54:50",
        "has_access_code": true,
        "transiton_malus": 2,
        "hints": [
            {
                "malus": 5,
                "is_total": false,
                "code_to_show": "",
                "time_to_show": ""
            },
            {
                "malus": 0,
                "is_total": true,
                "code_to_show": "",
                "time_to_show": ""
            }
```

```
    ],
    "dependencies": {
        "tasks": [
            29
        ],
        "lower_bound_points": 0
    }
},
{
    "assignment_id": 31,
    "name": "Erby",
    "slug": "06",
    "last_modified": "2020-10-06 14:28:54",
    "has_access_code": true,
    "transiton_malus": 2,
    "hints": [
        {
            "malus": 5,
            "is_total": false,
            "code_to_show": "",
            "time_to_show": ""
        },
        {
            "malus": 0,
            "is_total": true,
            "code_to_show": "",
            "time_to_show": ""
        }
    ],
    "dependencies": {
        "tasks": [
            27
        ],
        "lower_bound_points": 0
    }
},
{
    "assignment_id": 33,
    "name": "Zaměřovač",
    "slug": "07",
    "last_modified": "2019-01-17 20:54:59",
    "has_access_code": true,
    "transiton_malus": 2,
    "hints": [
        {
            "malus": 5,
            "is_total": false,
            "code_to_show": "",
            "time_to_show": ""
        },
        {
            "malus": 0,
            "is_total": true,
            "code_to_show": "",
```

```
                "time_to_show": ""
            }
        ],
        "dependencies": {
            "tasks": [
                31
            ],
            "lower_bound_points": 0
        }
    },
    {
        "assignment_id": 35,
        "name": "Panorama",
        "slug": "08",
        "last_modified": "2021-07-22 10:02:21",
        "has_access_code": true,
        "transiton_malus": 2,
        "hints": [
            {
                "malus": 5,
                "is_total": false,
                "code_to_show": "",
                "time_to_show": ""
            },
            {
                "malus": 0,
                "is_total": true,
                "code_to_show": "",
                "time_to_show": ""
            }
        ],
        "dependencies": {
            "tasks": [
                33
            ],
            "lower_bound_points": 0
        }
    },
    {
        "assignment_id": 37,
        "name": "Opevnění",
        "slug": "09",
        "last_modified": "2020-05-27 23:00:27",
        "has_access_code": true,
        "hints": [
            {
                "malus": 5,
                "is_total": false,
                "code_to_show": "",
                "time_to_show": ""
            },
            {
                "malus": 0,
                "is_total": true,
```

```
            "code_to_show": "",
            "time_to_show": ""
        }
    ],
    "dependencies": {
        "tasks": [
            35
        ],
        "lower_bound_points": 0
    }
},
{
    "assignment_id": 40,
    "name": "Kruh",
    "slug": "10",
    "last_modified": "2020-10-10 10:44:17",
    "has_access_code": true,
    "transiton_malus": 2,
    "hints": [
        {
            "malus": 5,
            "is_total": false,
            "code_to_show": "",
            "time_to_show": ""
        },
        {
            "malus": 0,
            "is_total": true,
            "code_to_show": "",
            "time_to_show": ""
        }
    ],
    "dependencies": {
        "tasks": [
            37
        ],
        "lower_bound_points": 0
    }
},
{
    "assignment_id": 42,
    "name": "Zazděný poklad",
    "slug": "11",
    "last_modified": "2020-10-10 11:40:43",
    "has_access_code": true,
    "transiton_malus": 2,
    "hints": [
        {
            "malus": 5,
            "is_total": false,
            "code_to_show": "",
            "time_to_show": ""
        },
        {
```

```
            "malus": 0,
            "is_total": true,
            "code_to_show": "",
            "time_to_show": ""
        }
    ],
    "dependencies": {
        "tasks": [
            40
        ],
        "lower_bound_points": 0
    }
},
{
    "assignment_id": 44,
    "name": "Hrdina",
    "slug": "12",
    "last_modified": "2020-10-10 10:46:50",
    "has_access_code": true,
    "transiton_malus": 2,
    "hints": [
        {
            "malus": 5,
            "is_total": false,
            "code_to_show": "",
            "time_to_show": ""
        },
        {
            "malus": 0,
            "is_total": true,
            "code_to_show": "",
            "time_to_show": ""
        }
    ],
    "dependencies": {
        "tasks": [
            42
        ],
        "lower_bound_points": 0
    }
},
{
    "assignment_id": 46,
    "name": "Finále",
    "slug": "13",
    "last_modified": "2020-10-10 10:49:07",
    "has_access_code": true,
    "transiton_malus": 2,
    "hints": [
        {
            "malus": 5,
            "is_total": false,
            "code_to_show": "",
            "time_to_show": ""
```

```
                },
                {
                    "malus": 0,
                    "is_total": true,
                    "code_to_show": "",
                    "time_to_show": ""
                }
            ],
            "dependencies": {
                "tasks": [
                    44
                ],
                "lower_bound_points": 0
            }
        }
    ]
}
```

F.3 Události ve hře (`events.json`)

Níže je ukázka ze souboru s událostmi hry.

```
[
    {
        "event_id": 4380,
        "user_id": 75,
        "type": "GAME_POINTS_SUM",
        "value": 115,
        "aggregated": true
    },
    {
        "event_id": 4381,
        "user_id": 75,
        "type": "GAME_TIME_SUM",
        "value": 9409,
        "aggregated": true
    },
    {
        "event_id": 4382,
        "user_id": 75,
        "type": "GAME_TIME_MAX",
        "value": null,
        "time": "2015-05-26 14:42:12",
        "aggregated": true
    },
    {
        "event_id": 4390,
        "user_id": 75,
        "type": "TASK_STARTED",
        "value": null,
        "task_id": 22,
        "time": "2015-05-26 10:46:43"
    },
    {
        "event_id": 4391,
        "user_id": 75,
```

```
        "type": "GAME_STARTED",
        "value": null,
        "time": "2015-05-26 10:46:43"
    },
    {
        "event_id": 4393,
        "user_id": 75,
        "type": "TASK_FINISHED",
        "value": null,
        "task_id": 22,
        "time": "2015-05-26 10:52:44"
    },
    {
        "event_id": 4394,
        "user_id": 75,
        "type": "TASK_TIME",
        "value": 361,
        "task_id": 22,
        "aggregated": true
    },
    {
        "event_id": 4395,
        "user_id": 75,
        "type": "TASK_POINTS",
        "value": 10,
        "task_id": 22,
        "aggregated": true
    }
    ]
```

Bibliografie

1. INSTRUKTOŘI BRNO. *Archiv TMOU 1* [online]. Brno, 2000 [cit. 2022-11-17]. Dostupné z: `https://archiv.tmou.cz/2000/index.html`.
2. HANŽL, Tomáš; PELÁNEK, Radek; VÝBORNÝ, Ondřej. *Šifry a hry s nimi: kolektivní outdoorové hry se šiframi*. 1. vyd. Praha: Portál, 2007. ISBN 978-80-7367-196-9.
3. ŠIFROVAČKY.CZ. *Příprava na šifrovačky* [online]. Brno, 2022 [cit. 2022-11-17]. Dostupné z: `https://sifrovacky.cz/jak-hrat/priprava-pred-hrou/`.
4. PUZZLE CLUB OF MIT. *History of the MIT Mystery Hunt* [online]. Brno, 2022 [cit. 2022-11-17]. Dostupné z: `http://puzzles.mit.edu/history.html`.
5. INSTRUKTOŘI BRNO. *Výsledky TMOU 23* [online]. Brno, 2022 [cit. 2022-11-17]. Dostupné z: `https://www.tmou.cz/23/page/game-statistics`.
6. INSTRUKTOŘI BRNO. *Almanach TMOU*. 1. vyd. Brno: Tribun EU s.r.o., 2008. Dostupné také z: `https://archiv.tmou.cz/2008/obr/tmou_almanach.pdf`.
7. PODHRÁZSKÝ, Zbyšek. *Rozhovory s ředitelem Cryptomania s.r.o.* podzim 2022.
8. ŠIFROVAČKY.CZ. *TOP 50 hráčů všech dob* [online]. Brno, 2022 [cit. 2022-11-17]. Dostupné z: `https://sifrovacky.cz/statistiky/hraci/`.
9. KREVELD, Marc van; LÖFFLER, Maarten; MUTSER, Paul. Automated puzzle difficulty estimation. In: *2015 IEEE Conference on Computational Intelligence and Games (CIG)*. 2015, s. 415–422. Dostupné z DOI: `10.1109/CIG.2015.7317913`.
10. ORGANIZÁTOŘI HRY. *Hra Sendvič* [online]. Brno, 2023 [cit. 2023-03-25]. Dostupné z: `https://www.hrasendvic.cz/`.
11. ORGANIZÁTOŘI HRY. *Statek Sešlost* [online]. Brno, 2023 [cit. 2023-03-25]. Dostupné z: `https://statek.seslost.cz/tmou-2018/lusteni`.

12. SZABÓ, Máté; POMÁZI, Krisztián Dániel; RADOSTYÁN, Bertalan; SZEGLETES, Luca; FORSTNER, Bertalan. Estimating task difficulty in educational games. In: *2016 7th IEEE International Conference on Cognitive Infocommunications (CogInfoCom)*. 2016, s. 000397–000402. Dostupné z DOI: 10.1109/CogInfoCom.2016.7804582.

13. R. PELÁNEK, P. Jarušek. Modeling and predicting students problem solving times. In: *In: Proc. of International Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM 2012). LNCS*. Springer, 2012, s. 637–648.

14. MAO, Y. One minute is enough: Early Prediction of Student Success and Event-level Difficulty during Novice Programming Tasks. *In: Proceedings of the 12th International Conference on Educational Data Mining (EDM 2019)*. [N.d.]. Dostupné také z: https://par.nsf.gov/biblio/10136495.

15. BATAL, Iyad; FRADKIN, Dmitriy; HARRISON, James; MOERCHEN, Fabian; HAUSKRECHT, Milos. Mining Recent Temporal Patterns for Event Detection in Multivariate Time Series Data. In: 2012, sv. 2012. Dostupné z DOI: 10.1145/2339530.2339578.

16. CORTES, Corinna; VAPNIK, Vladimir. Support-vector networks. *Machine Learning*. 1995, roč. 20, č. 3, s. 273–297. ISBN 1573-0565. Dostupné z DOI: 10.1007/BF00994018.

17. PRICE, Thomas; DONG, Yihuan; LIPOVAC, Dragan. iSnap: Towards Intelligent Tutoring in Novice Programming Environments. In: 2017, s. 483–488. Dostupné z DOI: 10.1145/3017680.3017762.

18. PRICE, Thomas; ZHI, Rui; BARNES, Tiffany. Evaluation of a Data-driven Feedback Algorithm for Open-ended Programming. In: 2017.

19. ELIÁŠOVÁ, Barbora. *Systém pro detekci problémů na trase šifrovací hry*. Praha, 2019. Fakulta informatiky, České vysoké učení technické.

20. SMITH, R. An Overview of the Tesseract OCR Engine. In: *Ninth International Conference on Document Analysis and Recognition (ICDAR 2007)*. 2007, sv. 2, s. 629–633. Dostupné z DOI: 10.1109/ICDAR.2007.4376991.

21. TESSERACT. *Dokumentace* [online]. Brno, 2022 [cit. 2022-11-30]. Dostupné z: https://tesseract-ocr.github.io/tessdoc/Home.html#tesseract-with-lstm.

22. WU, Yuxin; KIRILLOV, Alexander; MASSA, Francisco; LO, Wan-Yen; GIRSHICK, Ross. *Detectron2* [https://github.com/facebookresearch/detectron2]. 2019.

23. LIN, Tsung-Yi; MAIRE, Michael; BELONGIE, Serge J.; BOURDEV, Lubomir D.; GIRSHICK, Ross B.; HAYS, James; PERONA, Pietro; RAMANAN, Deva; DOLLÁR, Piotr; ZITNICK, C. Lawrence. Microsoft COCO: Common Objects in Context. *CoRR*. 2014, roč. abs/1405.0312. Dostupné z arXiv: 1405.0312.

24. REN, Shaoqing; HE, Kaiming; GIRSHICK, Ross B.; SUN, Jian. Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks. *CoRR*. 2015, roč. abs/1506.01497. Dostupné z arXiv: 1506.01497.

25. LIN, Tsung-Yi; DOLLÁR, Piotr; GIRSHICK, Ross B.; HE, Kaiming; HARIHARAN, Bharath; BELONGIE, Serge J. Feature Pyramid Networks for Object Detection. *CoRR*. 2016, roč. abs/1612.03144. Dostupné z arXiv: 1612.03144.

26. RADFORD, Alec; METZ, Luke; CHINTALA, Soumith. *Unsupervised Representation Learning with Deep Convolutional Generative Adversarial Networks*. arXiv, 2015. Dostupné z DOI: 10.48550/ARXIV.1511.06434.

27. GOODFELLOW, Ian J.; POUGET-ABADIE, Jean; MIRZA, Mehdi; XU, Bing; WARDE-FARLEY, David; OZAIR, Sherjil; COURVILLE, Aaron; BENGIO, Yoshua. *Generative Adversarial Networks*. arXiv, 2014. Dostupné z DOI: 10.48550/ARXIV.1406.2661.

28. IOFFE, Sergey; SZEGEDY, Christian. *Batch Normalization: Accelerating Deep Network Training by Reducing Internal Covariate Shift*. arXiv, 2015. Dostupné z DOI: 10.48550/ARXIV.1502.03167.

29. GOOGLE. *Quick Draw Dataset* [online]. Brno, 2022 [cit. 2022-12-05]. Dostupné z: https://github.com/googlecreativelab/quickdraw-dataset.

30. LEHECKA, Jan; SVEC, Jan. Comparison of Czech Transformers on Text Classification Tasks. *CoRR*. 2021, roč. abs/2107.10042. Dostupné z arXiv: 2107.10042.

31. DEVLIN, Jacob; CHANG, Ming-Wei; LEE, Kenton; TOUTANOVA, Kristina. *BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding*. arXiv, 2018. Dostupné z DOI: 10.48550/ARXIV.1810.04805.

32. DEVLIN, Jacob; CHANG, Ming-Wei; LEE, Kenton; TOUTANOVA, Kristina. *BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding*. 2019. Dostupné z arXiv: 1810.04805 [cs.CL].

33. ARKHIPOV, Mikhail; TROFIMOVA, Maria; KURATOV, Yuri; SOROKIN, Alexey. Tuning Multilingual Transformers for Language-Specific Named Entity Recognition. In: *Proceedings of the 7th Workshop on Balto-Slavic Natural Language Processing*. Florence, Italy: Association for Computational Linguistics, 2019, s. 89–93. Dostupné z DOI: 10.18653/v1/W19-3712.

34. CONNEAU, Alexis; KHANDELWAL, Kartikay; GOYAL, Naman; CHAUDHARY, Vishrav; WENZEK, Guillaume; GUZMÁN, Francisco; GRAVE, Edouard; OTT, Myle; ZETTLEMOYER, Luke; STOYANOV, Veselin. Unsupervised Cross-lingual Representation Learning at Scale. In: *Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics*. Online: Association for Computational Linguistics, 2020, s. 8440–8451. Dostupné z DOI: 10.18653/v1/2020.acl-main.747.

35. COMMON CRAWL TEAM. *Common Crawl dataset* [online]. Brno, 2022 [cit. 2022-12-06]. Dostupné z: https://commoncrawl.org/.

36. SIDO, Jakub; PRAŽÁK, Ondřej; PŘIBÁŇ, Pavel; PAŠEK, Jan; SEJÁK, Michal; KONOPÍK, Miloslav. *Czert – Czech BERT-like Model for Language Representation*. arXiv, 2021. Dostupné z DOI: 10.48550/ARXIV.2103.13031.

37. KŘEN, Michal; CVRČEK, Václav; ČAPKA, Tomáš; ČERMÁKOVÁ, Anna; HNÁTKOVÁ, Milena; CHLUMSKÁ, Lucie; JELINEK, Tomáš; KOVÁŘIKOVÁ, Dominika; PETKEVIČ, Vladimır; PROCHÁZKA, Pavel; SKOUMALOVÁ, Hana; ŠKRABAL, Michal; TRUNEČEK, Petr; VONDŘIČKA, Pavel; ZASINA, Adrian. *SYN v4: large corpus of written Czech*. 2016. Dostupné také z: http://hdl.handle.net/11234/1-1846. LINDAT/CLARIAH-CZ digital library at the Institute of Formal and Applied Linguistics (ÚFAL), Faculty of Mathematics and Physics, Charles University.

38. STRAKA, Milan; NÁPLAVA, Jakub; STRAKOVÁ, Jana; SAMUEL, David. RobeCzech: Czech RoBERTa, a Monolingual Contextualized Language Representation Model. In: *Text, Speech, and Dialogue*. Springer International Publishing, 2021, s. 197–209. Dostupné z DOI: 10.1007/978-3-030-83527-9_17.

39. AUTHOR, (:unav) Unknown. *czes*. 2011. Dostupné také z: http://hdl.handle.net/11858/00-097C-0000-0001-CCCF-C. LINDAT/CLARIAH-CZ digital library at the Institute of Formal and Applied Linguistics (ÚFAL), Faculty of Mathematics and Physics, Charles University.

40. MAJLIŠ, Martin. *W2C – Web to Corpus – Corpora*. 2011. Dostupné také z: http://hdl.handle.net/11858/00-097C-0000-0022-6133-9. LINDAT/CLARIAH-CZ digital library at the Institute of Formal and Applied Linguistics (ÚFAL), Faculty of Mathematics and Physics, Charles University.

41. JAN, Švec; JAN, Lehečka; PAVEL, Ircing; LUCIE, Skorkovská; ALEŠ, Pražák; JAN, Vavruška; PETR, Stanislav; JAN, Hoidekr. General framework for mining, processing and storing large amounts of electronic texts for language modeling purposes. *Language Resources and Evaluation*. 2014, s. 227–248. ISSN 1574-020X. Dostupné z DOI: 10.1007/s10579-013-9246-z.

42. HABERNAL, Ivan; PTÁČEK, Tomáš; STEINBERGER, Josef. Sentiment Analysis in Czech Social Media Using Supervised Machine Learning. In: *Proceedings of the 4th Workshop on Computational Approaches to Subjectivity, Sentiment and Social Media Analysis*. Atlanta,

Georgia: Association for Computational Linguistics, 2013, s. 65–74. Dostupné také z: https://aclanthology.org/W13-1609.

43. KRAL, Pavel; LENC, Ladislav. Czech Text Document Corpus v 2.0. In: CHAIR), Nicoletta Calzolari (Conference; CHOUKRI, Khalid; CIERI, Christopher; DECLERCK, Thierry; GOGGI, Sara; HASIDA, Koiti; ISAHARA, Hitoshi; MAEGAARD, Bente; MARIANI, Joseph; MAZO, Hélène; MORENO, Asuncion; ODIJK, Jan; PIPERIDIS, Stelios; TOKUNAGA, Takenobu (ed.). *Proceedings of the Eleventh International Conference on Language Resources and Evaluation (LREC 2018)*. Miyazaki, Japan: European Language Resources Association (ELRA), 2018. ISBN 979-10-95546-00-9.

44. CRYPTOMANIA S.R.O. *Šifrovací hry pro veřejnost* [online]. Brno, 2022 [cit. 2022-11-09]. Dostupné z: https://trails.cryptomania.cz/.

45. STATEK. *Statistika TMOU 20* [online]. Brno, 2022 [cit. 2022-10-31]. Dostupné z: https://statek.seslost.cz/tmou-2018/statistiky-sifer.

46. CRYPTOMANIA S.R.O. *Šifrovací hra Dopis bez adresy* [online]. Brno, 2022 [cit. 2022-10-31]. Dostupné z: https://trails.cryptomania.cz/dopis/.

47. YANG, Fan; PENG, Xiaochang; GHOSH, Gargi; SHILON, Reshef; MA, Hao; MOORE, Eider; PREDOVIC, Goran. Exploring Deep Multimodal Fusion of Text and Photo for Hate Speech Classification. In: *Proceedings of the Third Workshop on Abusive Language Online*. Florence, Italy: Association for Computational Linguistics, 2019, s. 11–18. Dostupné z DOI: 10.18653/v1/W19-3502.

48. SIMONINI, Thomas. *CatDCGAN* [online]. Brno, 2022 [cit. 2022-12-06]. Dostupné z: https://github.com/simoninithomas/CatDCGAN.