Základy šifrování

Slovo šifrovačka Ti nic neříká a nevíš, do čeho jdeš? Ničeho se neboj! V tomto krátkém textu bychom Ti chtěli základně představit, o co jde. Časem jistě vznikne i podrobnější manuál s historií šifrování, šifrovaček a spoustou hezkých příkladů, zatím tu máš stručný úvod. Pokud Ti to nestačí a chceš vědět víc, můžeme vřele doporučit manuál Tmou, či web sifrovacky.cz, konkrétně sekci Principy šifer.

Co je to šifra?

Podle účelu můžeme rozlišovat dva základní typy šifer - pro bezpečné předání informace a pro zábavu.

V prvním případě je cílem předávat zprávu jen ve skupině "zasvěcených". Kdo nemá klíčovou informaci, zprávu nerozluští. V historii je mnoho zajímavých příkladů, od slavné Caesarovy šifry, přes šifrovací stroj Enigma, používaný za druhé světové války, až po moderní bankovnictví, stojící na principech asymetrické kryptografie (o té více jindy :)). Nás ale bude mnohem více zajímat ten druhý typ.

Šifry tvořené pro zábavu se od běžné kryptografie liší hlavně tím, že je může rozluštit s dostatkem důvtipu či nějakou veřejně známou informací úplně kdokoliv. Žádný přesný návod k nim ale nečekejte. Jejich řešením je nejčastěji heslo (typicky české podstatné jméno) nebo poloha stanoviště s další šifrou. V závislosti na pravidlech konkrétní šifrovací hry ale může být řešením vlastně úplně cokoliv :)

Co je to šifrovací hra?

Podobně jako u jednotlivých šifer, nemáme ani u celých šifrovacích her jasně určeno, jak mají vypadat. Nejčastěji se setkáváme lineárními šifrovacími hrami. Vyluštěním šifry zjistíme polohu dalšího stanoviště, obdržíme další šifru a tak dále, dokud nedojdeme do cíle.

To nejkrásnější na šifrovačkách je ale právě ta různorodost. Šifrovačky mohou být internetové či v terénu. Probíhají hry denní, noční, mohou dokonce trvat i více dní. Na některých hrách se jde výhradně pěšky, jinde se cestuje i vlaky. Existuje již i šifrovací hra, kde je jediný povolený způsob přepravy na člunu! Některé hry jsou pro jednotlivce, jiné pro páry či velké týmy. Proběhlo také několik akcí, na kterých Tě náhodně namíchají do týmu neznámých lidí, případně se velikost týmu v průběhu hry mění. Jsou hry lehké, těžké, brutální ...ale můžeme s klidným svědomím říct, že každou z nich stojí za to vyzkoušet.

Základní šifrovací principy

Postupným vývojem šifrovacích her se také ustálily základní běžně používané šifrovací principy. Nejčastěji je najdete v podobě šifrovacích tabulek (také jedny máme :)). Zde jsou ty nejznámější:

- Morseova abeceda
- Braillovo písmo
- Binárka (dvojková soustava)
- Semaforová abeceda
- Vlajky
- Velký a malý polský kříž

Většina principů implicitně využívá anglickou abecedu o 26 znacích, která se takto i čísluje. Běžně se tak setkáme s výstupem z šifry např. "$11, 15, 2, 12, 9, 8, 1$", který se ještě musí převést dle číslování $A = 1, \ldots, Z = 26$ na písmena. Schválně si to zkuste doluštit :)

V praxi ale málokdy jde o pouhé strojové převedení podle šifrovacího principu. Většina šifer obsahuje alespoň jeden netriviální úvahový krok. Často také nejde o přímou substituci jedné množiny znaků na jinou. Výstupem mohou být graficky namalovaná písmena nebo dokonce obrázek. V šifře je také často nezbytné využít nějaké encyklopedické znalosti. Existuje tak několik základních typů šifer.

Základní typy šifer

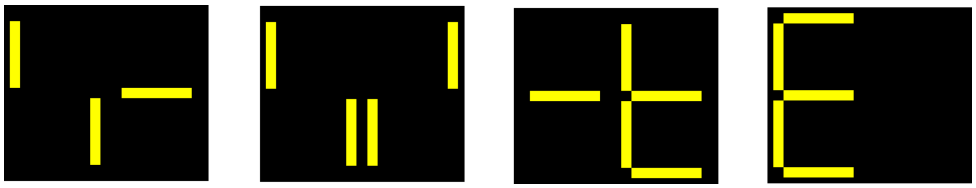
Jak již bylo zmíněno, šifry mohou mít mnoho různých podob. Zadání můžete dostat na papíře, někdy se ale jeho části nacházejí schované po okolí. Občas máte nějakou nápovědu či důležitou informaci v zadání. Někdy je dokonce skryta v jídle či artefaktu, které dostanete od organizátorů hry na cestu. Oblíbeným doplňkem online šifrovaček jsou například audiovizuální šifry (například video s písničkou od organizátorů) či interaktivní "hra".

Roztřídit všechny možné kreativní nápady do pevných kategorií je prakticky nemožné. I tak se ustálilo 6 základních typů šifer podle způsobu luštění:

Substituční šifry

Základním principem substitučních šifer je náhrada jedné skupiny symbolů za druhou. Můžeme nahrazovat písmena abecedy za jiná (např. zmíněná Caesarova šifra, nebo za úplně jiné symboly (Morseova abeceda, Braillovo písmo, ...). Přesná pravidla substituce jsou buď dopředu známa (viz), nebo je na ně třeba přijít přímo z šifry.

Příklad



Řešení

Obrázky připomínají digitální display, tedy by nás to mohlo vést na nalezení čísel a jejich následnou substituci za písmena. Svítící segmenty nám ale nic nepřipomínají, bude tedy potřeba ještě nějaký krok. Co zkusit vše naopak, rozsvítit zhasnuté a zhasnout ty, co teď svítí? Ano! Vypnuté segmenty skutečně zobrazují čísla 20, 25, 07, 18, která snadno převedeme na heslo TYGR.

Transpoziční šifry

Na rozdíl od substitučních šifer v transpozičních zadané znaky neměníme, pouze daným pravidlem upravujeme jejich pořadí či přidáváme balastní prvky (např. redundantní písmena). Běžně se čte text pozpátku, vyškrtává se každý druhý znak, případně se čtou písmenka v tabulce podle nějakého grafického pravidla (např. do spirály). Zajímavým a často využívaným principem je taky šifrovací mřížka.

Příklad

BOBR

D	P	D	O
A	J	U	A
B	K	R	E
O	A	H	A

Řešení

Tato šifra má název a jak to často bývá, je užitečný pro její vyřešení. Ačkoliv čtenáře může mást specifičnost názvu, v tomto případě je to odúvodnitelné tím, že je šifra převzata z konkrétní šifrovačky s tématem těchto roztomilých zubatých zvířátek.

První co můžeme zkusit je pojmenovat obrázky. Na internetu dohledáme známého výrobce rozvaděčů BBR, obrázek zřejmě popíše slovo OBR, BOR je jméno zámku na obrázku a známá postavička většího z králíků je BOB. Vidíme tak, že v každém slově chybí jedno z písmen slova BOBR. Máme čtyři obrázky, čtyři řádky a nabízí se tedy z tabulky vyškrtnout v každém řádku jedno písmeno na příslušné pozici. Dále využijeme vzniklou mřížku (pokud neznáte, přečtěte si popis v odkazu) a jejím postupným otáčením čteme PARA DAKO DJEH OUBA. Heslem je tedy slovo HOUBA.

Steganografické šifry

Steganografie je metoda skrývání tajné informace do běžného objektu či v případě šifer do libovolného zadání. Cílem této metody není šifru překódovat či popřeházet znaky, ale nějakým způsobem ji skrýt. Tímto způsobem vznikají často ty nejzajímavější šifry, jako jsou třeba vzkazy psané neviditelným inkoustem, upravené fotografie či videa a kódy skryté uvnitř nějakého předmětu (třeba i hlavolamu).

Dalo by se polemizovat, jestli tu není překryv s některými transpozičními principy (šifry s přidaným balastem), ale jak už jsme naznačali, toto není exaktní věda :)

Příklad

Řešení

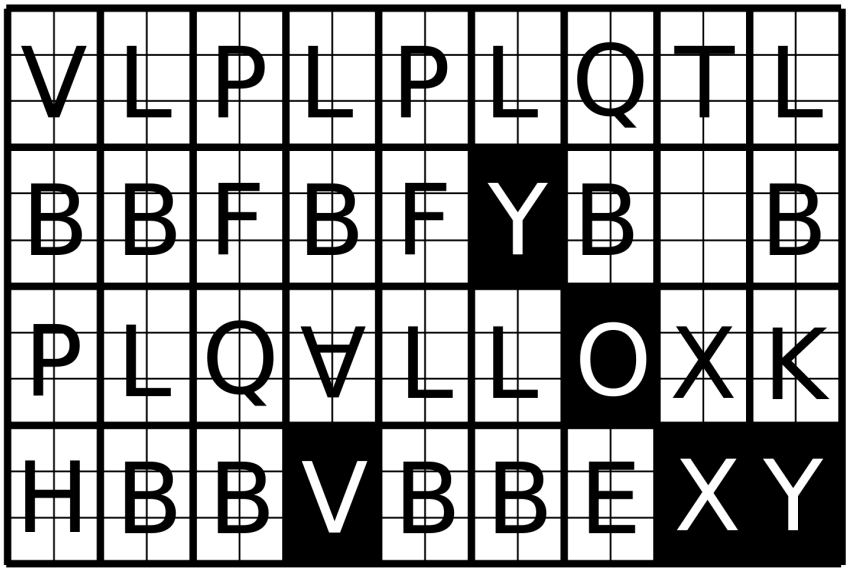
Šifra obsahuje spoustu protáhlých černých obdélníčků, mohla by tedy navádět na substituci jako je binárka či Morseova abeceda. Toto je ale příklad steganografické šifry. Pokud

si obrázek otočíš o 90 stupňů (proti směru hodinových ručiček) a podíváš se na něj pod hodně velkým úhlem (oči skoro na úrovni hrany papíru), obrázek se opticky zúží a můžeš číst heslo HAVRASPAR. Schválně si to vyzkA celkově textuoušej :)

Grafické šifry

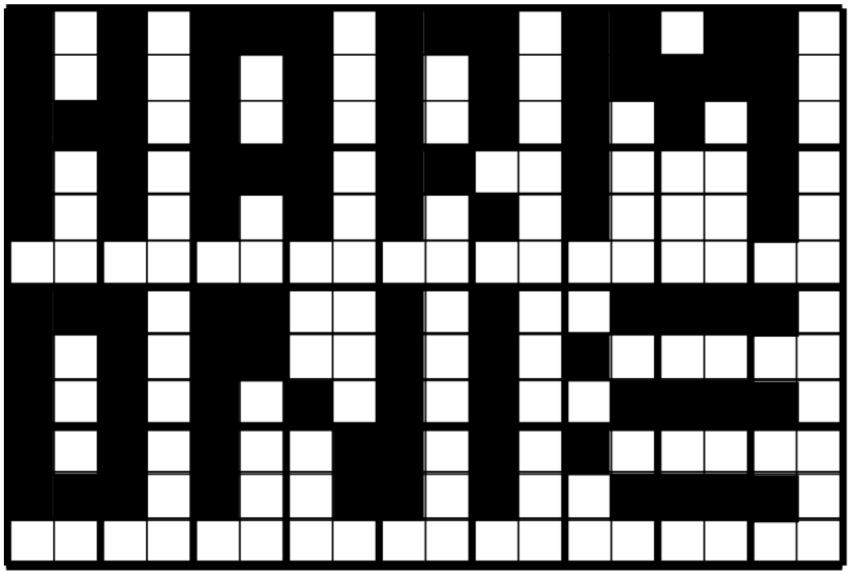
Základním principem grafických šifer je, že něco kreslíme. Typicky nám správný postup vykreslí písmena, ze kterých přečteme heslo.

Příklad



Řešení

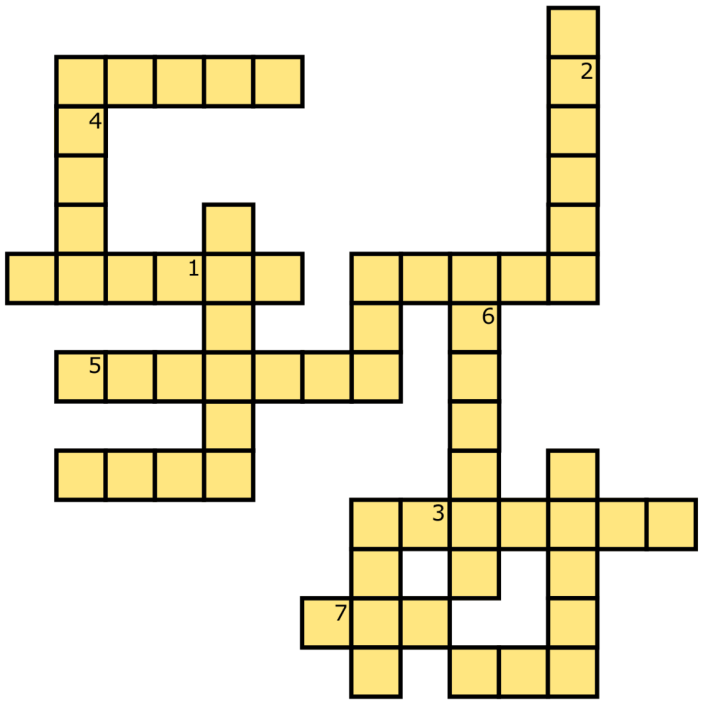
Mřížky 2×3 nás mohou okamžitě navést na Braillovo písmo. Dává smysl si vyznačit do buněk příslušná písmena. Už je jen potřeba přijít na to, co dělat s otočenými písmeny či těmi s bílými na černém pozadí. I ty můžeme celkem snadno vyjádřit Braillovým písmem. U otočených prostě otočíme i puntíky a u bílých písmen vyměníme tečky za prázdné pozice (písmeno v Braillovi invertujeme). Z výsledku můžeme graficky číst heslo HARMONIE.



Znalostní šifry

Znalostní šifry můžeme velice snadno popsat jako šifry, které vyžadují nějakou znalost nad rámec běžných šifrovacích principů.

Příklad



Řešení

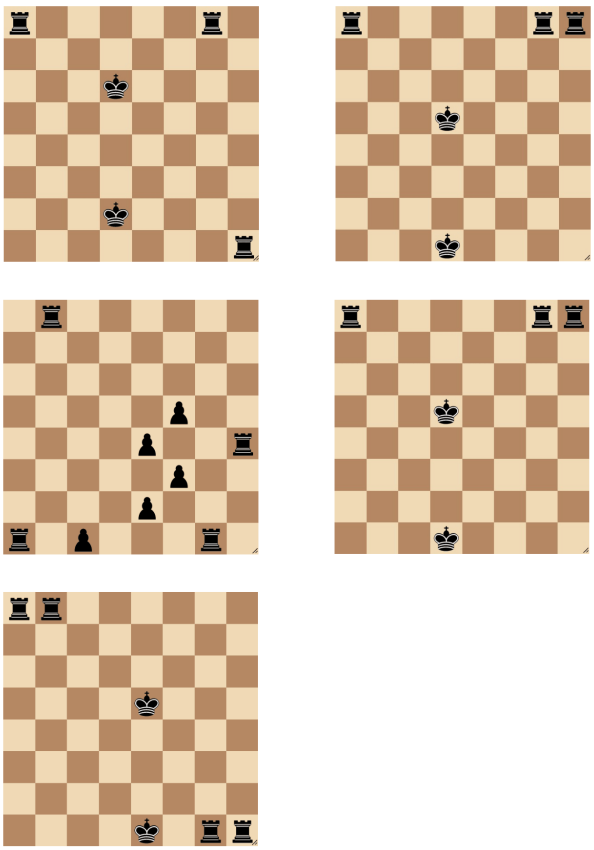
Na první pohled nemáme k dispozici nic jiného, než tajenku a název. U názvu hned upoutá gramatická chyba. Je dost nepravděpodobné, že by se jednalo o překlep, tudíž musí být součástí šifry. Která zvířata v sobě mají y? Přece ta z vyjmenovaných slov! Když si je vypíšeme, zjistíme, že je můžeme jednoznačně doplnit do křížovky a z čísly označených políček dostaneme heslo POLYNOM.

Logické hádanky

Poslední kategorie by se dala částečně zařadit jako speciální případ znalostních šifer, každopádně se spíše jedná o jakousi znalost "mechanismu"luštění než o čistou informaci. Hlavním principem je začlenění pravidel běžné logické, deskové či jiné hry (popřípadě hlavolamu) do klasické šifry.

Příklad

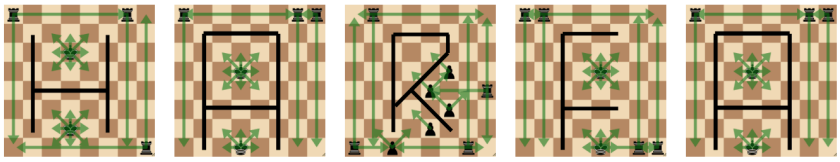
Bezpečná oblast



Řešení

V tomto případě lze okamžitě usoudit, že se hodí znát pravidla šachů. Jak už napovídá název, zajímá nás bezpečná oblast, v šachu tedy oblast, na kterou neútočí žádná figurka.

Postupné vyškrtání ohrožených polí vykreslí ze zbytku písmena a můžeme číst heslo HARFA.



Kombinace

Jak vás už jistě napadlo, v praxi se častěji setkáváme s kombinacemi těchto 6 základních typů šifer. Náš příklad transpoziční šifry by se jistě dal považovat i za šifru znalostní, protože bez jména zámku Bor či králíka Boba šifru těžko vyluštíte. Grafická šifra zase využívá přímo principu Braillova písma a je tedy na pomezí se substituční. No a logická hádanka má grafický výstup řešení.

Možnost kombinování základních principů je obrovská výhoda. Celkem existuje teoreticky $2^6 - 1 = 63$ unikátních kombinací principů. A to mluvíme jen o základních principech! Když si uvědomíš, že na každou jednu z těchto kombinací jde vymyslet spousta unikátních šifer (například znalostních je prakticky neomezeně), poskládat je neotřelým způsobem do šifrovačky se zajímavým tématem a jedinečným herním mechanismem ...možnosti jsou neomezené.

Závěrem

Tento text je jen základním vhledem do světa šifer. Snad Ti dal mnoho námětů na přemýšlení a pár dobrých rad pro řešení šifer. Jak jsme již doufám naznačili, existuje nepřeberné množství způsobů přístupu k šifrám, a to jak z pohledu autora, tak řešitele. Nové šifry i celé hry vznikají i po desítkách let šifrovacích her. Možná i Ty jednoho dne přijdeš s novým skvělým nápadem, jak hru udělat ještě o něco zajímavější :)

Organizátoři Štábu
20. června 2026