ŠIFROVÁNÍ A LUŠTĚNÍ (1.)

Zapomeňte PIN?

CHIP CD červenec 2002

Aby vám přes léto příliš nezakrněla šedá kůra mozková (jak by určitě řekl Hercule Poirot), připravili jsme pro ni na oba prázdninové měsíce malé povyražení. Záleží jen na vás, do jaké míry se do problému ponoříte - můžete si jen počíst, nebo si také trochu zaluštit...

Také máte několik platebních karet a k tomu ještě zaheslovaný mobilní telefon? A také se bojíte, že některý PIN jednoho dne zapomenete? Nezbývá než si tato veledůležitá čísla pro jistotu někde poznamenat. Vynecháme teď ty, kteří si PIN píší na zadní stranu karty nebo na papírek ukládaný společně s kartami. Ti prozíravější si musí vyřešit problém, jak zaznamenaný PIN ukrýt.

Seznámili jsme se s výborným nápadem, který takové utajení umožňuje. Ukážeme ale, že tento na první pohled dobrý sluha může být také špatným pánem. Šifrovací tabulka ***codecard***, propagovaná sloganem „Zapomeňte PIN, pořiďte si codecard", je totiž za jistých okolností snadno luštitelná.

Začalo to docela nevinně v srpnu 2000, kdy nám jeden kolega napsal: „Podívejte se, co prodávají u pumpy! .... Uvádějí, že ke každému tajnému klíči se dá nalézt nejméně 2280 různých PIN. ... Není mi jasné, co toto tvrzení znamená, protože se mi podařilo zakódovat jeden PIN pouze 251 možnostmi. Postupoval jsem podle návodu a předpokládám, že tak učiní většina uživatelů..."

PÁR SLOV ÚVODEM

Takto nalákán jsem si codecard také koupil a vyzkoušel. Upřímně řečeno, trochu jsem autorům záviděl, že je taková věc napadla. Na první pohled mě zaujala, protože mi připomněla historické šifrovací systémy, které se všelijakými tabulkami a důmyslnými pravidly jejich používání jen hemží. Přelétl jsem návod a zkusil jsem si zašifrovat čtyři náhodná čísla. Pak jsem se ještě zeptal kolegy, jak on pochopil počet možností zašifrování, a zjistil jsem, že jsme si návod vyložili každý jinak. S předsevzetím, že se na to ještě podívám, založil jsem codecard do šuplíku. Později jsem zjistil, že návod chápe různě více lidí, což je, jak uvidíme dále, vlastně dobře.

Codecard zůstala v šuplíku hodně dlouho. Když jsem jednou zase čistil stůl, padla mi opět do rukou. K její škodě – udělal jsem si na ni tentokrát čas a po dvou hodinách se docela „položila". Ukážeme si, jak se dá luštit, a uvidíme, že k tomu není potřeba žádná zvláštní znalost. Tahle hračka má ale další zajímavé vlastnosti. Milovníci rébusů si tak možná s codecard ukrátí dlouhou chvíli, až se budou v létě opékat na sluníčku...

Rádi bychom se teď, ve spolupráci s vámi čtenáři, pokusili najít cestu, jak změnit pravidla používání codecard, aby se stala bezpečnější, a hlavně aby se nemuselo měnit její stávající příslušenství – průhledná celuloidová tabulka (dále též „fólie"); majitelé současných codecard vám za to budou jistě vděčni. Je-li pravda, co její tvůrci dříve uváděli na webu Asociace pro elektronickou komerci *(www.apek.cz)*, je jich několik set tisíc, domnívám se však, že ve skutečnosti půjde jen o tisíce uživatelů. Stojí také za zmínku, že webové stránky, které se vztahovaly ke codecard *(www.bros.cz)*, jsou nyní „ve výstavbě" a přesměrovány na *http://www.volny.cz/petr.ptasnik/codecard.html*. V době zahájení prodeje codecard byly mnohem bohatší, se soutěžemi, a dokonce speciálním e-zinem; o codecard se psalo také na internetu i v denním tisku.

Pokusme se najít změnu pravidel používání codecard, která by i při původní fólii zaručila větší bezpečnost!

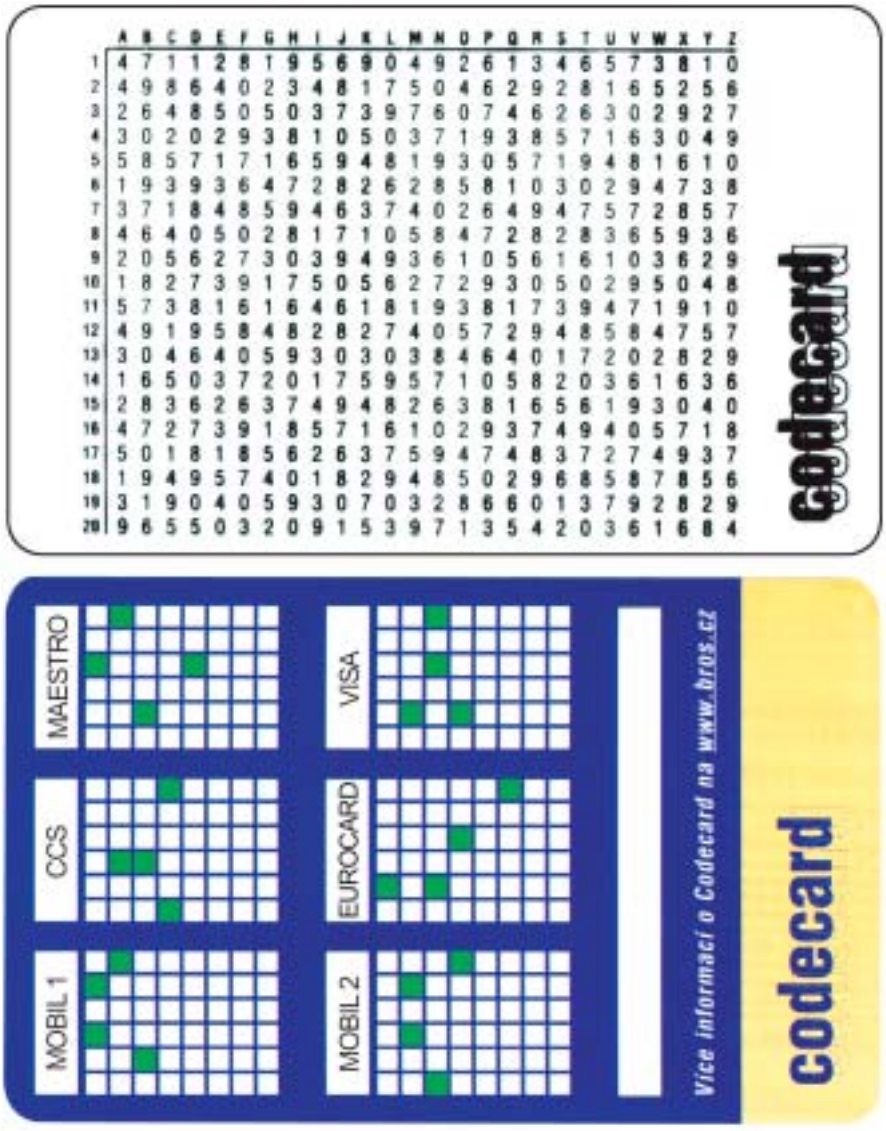
CO JE CODECARD

Prodávaný komplet se skládá z *návodu* (skládací knížečka), průhledné *fólie* s číslicemi uspořádanými do matice o 26 sloupcích (A až Z) a 20 řádcích (1 až 20) a papírové kartičky (vlastní *codecard*) se šesti poli, z nichž každé slouží k zašifrování jednoho PIN – vše ve velikosti bankovní karty. Každé pole na kartičce obsahuje 6 x 8 čtverečků, a pokud je vyplněno, jsou čtyři z nich zvýrazněny (např. zabarveny).

Fólii lze na papírovou kartu přiložit mnoha způsoby (návod tvrdí, že jich je 2280) a právě jeden z nich je naším tajným klíčem. Zvolíme-li si jako klíč „souřadnice" levého horního čtverečku kódovacího pole vzhledem k fólii, můžeme si vybrat z kombinací písmen A až S a čísel 1 až 15 (tj. A1 ... A15, B1 ... B15, ... ,S1 ... S15), což dává celkem 15 x 19 = 285 možných klíčů. Zvolme si například klíč K2. K přečtení PIN (o jeho záznamu si povíme za okamžik) stačí přiložit fólii na každé ze šesti polí tak, aby její čtvereček K2 ležel na levém horním čtverečku tohoto pole – zvýrazněné čtverečky v poli pak na fólii určují čtyři číslice – náš PIN. Abychom věděli, k čemu je který PIN, je každé pole opatřeno záhlavím, do něhož si poznamenáme potřebnou identifikaci (Maestro, VISA, CCS, mobil...). Vše je dobře patrné z obrázku 1.

Jistě už tušíte, jak PIN do zvoleného pole zaznamenat (tj. zašifrovat). Fólii přiložíme na kartičku právě popsaným způsobem, v našem případě tedy na levý horní čtvereček příslušného pole přijde fólie bodem K2. Pole teď na fólii ohraničuje výřez 48 číslic v osmi sloupcích a šesti řádcích. Návod říká, že toto pole máme očima projíždět po sloupcích shora dolů a zleva doprava, a jakmile uvidíme první číslici našeho PIN, fólii na okraji přidržet, částečně odchlípnout a zvýrazňovačem vybarvit příslušný čtvereček pod ní. Pak fólii přiklopit zpět a od vybarveného čtverečku stejným postupem hledat první výskyt další cifry našeho PIN atd. Nakonec na nás přes celuloid „svítí" celý PIN. Právě tak zašifrujeme další PIN do dalšího pole – codecard nám jich nabízí celkem šest.

Je zřejmé, že přiložíme-li fólii do jakékoli jiné pozice, přečteme jiné číslo, a zdá se tedy, že když neznáme ten pravý klíč, zakódovaný PIN prakticky nemůžeme zjistit. Podstatné přitom je, že u každého pole nastavujeme vždy K2 na levý horní čtvereček pole, takže při čtení dalšího PIN musíme fólii posouvat. Vypadá to zcela jasně, moje zkušenost je však taková, že pravidla napsaná v návodu si každý interpretuje trochu jinak...



Obr. 1. Fólie a kartička codecard s příkladem zašifrování PIN 5721 (MAESTRO), 6538 (VISA), 8100 (CCS), 2276 (EUROCARD), 3472 (MOBIL 1) a 9840 (MOBIL 2) klíčem K2

Ale uvažujme dále. Zatím jsme fólii přikládali na kartičku jen tím nejpřirozenějším způsobem, kdy máme sloupce A ... Z a řádky 1 ... 20. Jak uvádí návod, fólii také můžeme otočit o 180° („nohama vzhůru“), nebo obrátit lícem dolů, nebo i obojí. Dostáváme tak další tři možnosti přiložení fólie, jimž odpovídají tyto sloupce a řádky: po otočení Z ... A, 20 ... 1, po obrácení = A ... Z, 20 ... 1, po otočení a obrácení Z ... A, 1 ... 20. U základní pozice jsme číslice zaznamenávali (a později četli) po sloupcích shora dolů a zleva doprava, můžeme to však dělat i zprava doleva (ve sloupcích stále shora dolů). Celkem tak dostáváme čtyři možná přiložení a dva možné postupy záznamu/čtení, celkem tedy osm možností, jak využít fólii. V kombinaci s 285 klíči to pak dává oněch 8 x 285 = 2280 možností šifrování uvedených v návodu. (Tolik návod. Jistě vás napadlo, že tím stále ještě nejsou vyčerpány všechny možnosti pozicování fólie, např. otočení o 90° nebo 270°, či jiný postup záznamu/čtení, ale ty teď necháme stranou a přidržíme se návodu.)

I když si luštění ukážeme s ohledem na všechny v návodu uvažované možnosti, v praxi bych opravdu chtěl vidět někoho, kdo si nepamatuje PIN, ale přitom si dokáže zapamatovat, jak vlastně přikládal celuloid a jakým směrem PIN zaznamenával, a k tomu si ještě pamatuje tajný klíč. Nehledě na to, že u „nepřirozených“ variant bude s codecard dost zápasit, protože pak vidí číslice otočené vzhůru nohama, stranově převrácené, či dokonce obojí; zejména v případě šestek a devítek to bude opravdu „lahůdka“. Luštitel může proto předpokládat, že většina uživatelů použije základní způsob přikládání fólie – v drtivé většině případů tomu tak jistě bude.

Luštíme codecard

Když jsem kontaktoval Petra Ptašnika, jednoho z autorů codecard, řekl mi, že to vymysleli s bratrem a že se to dá odhalit, ale „je to o možnostech“. Vyjádřil se, že *„... by byl asi zázrak, kdyby zloději postačilo 10 pokusů. Přitom tady je systém dvou pokusů, a pokud je třetí špatně, karta se zablokuje (bankomat ji nevydá)“*.

Víme-li, že je tady opravdu 2280 možností, jak PIN zašifrovat, asi uznáme, že zloděj je v podobné situaci, jako kdyby žádnou codecard neměl – vždyť jeden PIN má jen deset tisíc možností, což v porovnání s 2280 není tak zlé. To však porovnáváme jablka a hrušky. Zloděj, říkejme mu decentněji luštitel, totiž nestojí před otázkou zašifrování daných PIN, ale před problémem **odšifrování** (luštění), a to ne obecného, ale zcela **konkrétního** šifrového textu, jímž je nalezená (věřme, že nikoli odcizená) vyplněná papírová codecard. (Nemusí ani nalézt příslušnou fólii – ta je u všech codecard stejná, a lze si ji tedy dokoupit...) Navíc má pravděpodobně k dispozici několik bankovních karet, u nichž byla codecard uložena, čili má vzorky, proti nimž může své hypotézy testovat.

Ukažme si nejprve princip luštění. Představme si, že jsme nalezli vyplněnou codecard se šesti poli jako na obrázku 1, a uvažujme nejprve základní způsob přiložení fólie a první možný klíč A1. První pole (MAESTRO) by znamenalo PIN 2755, druhé pole (VISA) by dalo 8147, třetí 0219, čtvrté 5588, páté 4375 a šesté 9031. Zatím jsme daleko nepokročili, ale zkusíme klíč A2. U prvního pole dostáváme PIN 3932 – ale pozor, u druhého pole nám něco nesouhlasí, získaný PIN 9829 nemohl vzniknout podle pravidel! Ten, kdo by zašifrovával PIN 9829, by správně měl vybarvit první čtvereček s devítkou už v druhém sloupci nahoře – podle návodu se totiž zaškrtává *vždy první výskyt dané číslice PIN*. Druhé pole tedy vylučuje klíč A2! Určitě si dovedete představit další postup. Zkusíme klíč A3 – zjistíme, že ho vylučuje třetí pole, klíč A4 je vyloučen šestým polem atd. (viz obrázek 2).

Zbývá otázka, kolik klíčů je u nalezené codecard vlastně možných. Zjišťovat odpověď popsaným manuálním postupem by bylo zdlouhavé a (člověk je tvor chybující) nespolehlivé. Ale od čeho jsou počítače? Stačilo napsat poměrně jednoduchý program (*disppin*) a nechat jím všechny možné klíče vyzkoušet. Výsledek (přípustné klíče a odpovídající PIN) ukazuje výpis na obrázku 3. V úvahu tedy připadají pouze dva klíče (K2 a M2)!

Program respektuje všech osm možných použití fólie (tj. i nepřirozená přiložení) – přitom ale kupodivu žádná další řešení nenašel. Mimochodem, program také vyloučil klíč A1

Klíč A1, první pole, PIN 2755

4	7	1	1	2	8	1	9
4	9	8	6	4	0	2	3
2	6	4	8	5	0	5	0
3	0	2	0	2	9	3	8
5	8	5	7	1	7	1	6
1	9	3	9	3	6	4	7

Klíč A2, druhé pole, PIN 9829

4	9	8	6	4	0	2	3
2	6	4	8	5	0	5	0
3	0	2	0	2	9	3	8
5	8	5	7	1	7	1	6
1	9	3	9	3	6	4	7
3	7	1	8	4	8	5	9

Klíč A3, třetí pole, PIN 9380

2	6	4	8	5	0	5	0
3	0	2	0	2	9	3	8
5	8	5	7	1	7	1	6
1	9	3	9	3	6	4	7
3	7	1	8	4	8	5	9
4	6	4	0	5	0	2	8

Obr. 2. Výřezy fólie v určitých nastaveních

a odhalil tak moji chybu. Přehlédl jsem totiž, že v pátém poli, které dává 4375, by měl být vybarven už první čtvereček v prvním sloupci, nikoli druhý.

Uvedený příklad je pouze ilustrativní. V praxi dostáváme mnohem různorodější výsledky a zpravidla více řešení než dvě, a to i v nepřirozených nastaveních. Abychom mohli udělat obecné závěry, provedli jsme velmi rozsáhlý experiment, jehož účelem bylo zjistit, kolik pokusů v průměru a v extrémních případech musí luštitel vyzkoušet, aby správné PIN získal. O tom ale až v dalším čísle.

Několik poznámek

Jak jsme právě viděli, luštění nám umožnily tzv. *nemožné šifrové texty*. Pro daný klíč prostě není možné obdržet určité šifrové texty (vyplnění polí). To ale také znamená, že pokud naopak před sebou už máme nějaký konkrétní šifrový text, omezuje určitým způsobem množinu možných klíčů, které k němu mohou vést. První šifrový text (1. vyplněné pole) tak vytváří první omezující množinu klíčů, druhý šifrový text druhou atd. Hledané řešení (klíč) musí ležet v průniku všech těchto množin, neboť použitý klíč je společný všem polím. V příkladu šesti polí na obrázku 1 je průnik velmi malý – obsahuje jen dva prvky (K2 a M2).

Jako uživatelé codecard bychom chtěli, aby luštitelův postup vedl k co nejvíce klíčům, což za stávajících pravidel, jak jsme viděli, není obecně možné. V situaci, kdy útočník má vedle codecard k dispozici i příslušné platební karty (většinou se ztrácí celá peněženka...), totiž poměrně snadno eliminuje nesprávné klíče – stačí nejprve vyzkoušet dva z možných klíčů nalezených programem disppin (prostřednictvím zjištěných PIN) u první bankovní karty (bankomat mu ji nezabaví), potom další dva klíče u druhé karty atd. až po poslední N-tou kartu. Pokud neuspěje, znovu na první kartě vyzkouší třetí klíč, totéž u druhé a nakonec u N-té.

Při N vyplněných polích (1 až 6) má tedy útočník (se zaručeným úspěchem) k dispozici 3N pokusů. Proto bychom chtěli, aby těch řešení bylo pro každý šifrový text řádově spíš 100*N, nebo ještě lépe 9999, aby nám codecard PIN skutečně chránila. K tomu ale (nechceme-li měnit přímo ji) vede jediná cesta – změnit pravidla jejího používání.

Spuštění programu:

```
disppin.exe 13213553 25313345 24344146 15354361 12142135 22243641
```

Výstup:

```
Folie: A...Z 1...20. Vycitani: zleva doprava:
reseni K 2  -  PINy:  5721  6538  8100  2276  3472  9840
reseni M 2  -  PINy:  3053  8418  9366  2599  7105  6926
pocet reseni: 2
```

Obr. 3. Luštící program

Program disppin luští nalezenou codecard. Vstupem je tolik parametrů, kolik je na codecard vyplněno polí. Výstupem je přípustný klíč a jemu odpovídající rozšifrované PIN. Podrobnou nápovědu obdržíte spuštěním programu bez parametrů.

Každý parametr udává zakódování jednoho pole tak, že každému vybarvenému čtverečku odpovídá dvojice číslic určujících jeho sloupec a řádek uvnitř pole. Například „13" znamená čtvereček v 1. sloupci a 3. řádku, „21" čtvereček v 2. sloupci a 1. řádku atd. První parametr „13213553" tedy zadává první pole z obrázku 1.

Výstup programu říká, že pro zadané kombinace PIN jsou jen dvě možná řešení – K2 a M2, a to jen v základním nastavení fólie při základním postupu záznamu/čtení; v ostatních sedmi možných kombinacích nastavení a postupu program žádná další řešení nenalezl.

Je libo rébus?

Majitelé codecard teď nejspíš trochu znejistěli. Dosud se domnívali, že mohou codecard klidně ukládat k bankovním kartám, nyní si to asi myslet nebudou. Programem *disppin* si mohou zjistit, kolik jejich codecard umožňuje řešení, a bude-li to málo, mohou papírovou kartu zničit, aby v případě ztráty PIN neprozradila. Položme si teď otázku, zda by se pak zbylá fólie nedala úpravou pravidel přece jen nějak zužitkovat – papírovou kartu si lze snadno znovu vyrobit.

První úkol pro čtenáře tedy zní: Je možné navrhnout nová pravidla využití stávající fólie tak, aby se rapidně zvýšil počet řešení? Další otázka je vyloženě pro hravé a obávám se, že nemá konkrétní odpověď: Existuje nějaký algoritmus nebo nějaká pravidelnost, jak jsou uspořádány číslice na stávající fólii? Má tento algoritmus nějakou viditelnou nevýhodu nebo výhodu?

Poznamenejme k tomu jen, že zcela zřejmou vlastností je, že v lichých sloupcích jsou až na výjimky číslice od 1 do 5 a v sudých číslice 6 až 9 a 0. Dále platí, že v každém výřezu fólie o rozměrech 6 x 8 se každá cifra vyskytuje většinou čtyřikrát, některé až pětkrát; najdeme ovšem i výřezy, v nichž se na některou číslici dostalo jen třikrát (!).

Příště vás seznámíme s výsledky experimentů a eventuálně i s vašimi náměty, nápady a postřehy (posílejte je na níže uvedenou e-mailovou adresu nebo poštou na adresu redakce). Další informace k tématu i zmíněný program najdete na Chip CD 7/02. ■ ■ ■

Vlastimil Klíma, *autor@chip.cz*

Infotipy

Soubory na přiloženém Chip CD 7/02:
návod k použití codecard
soubor číslic fólie ve formátu xls
program disppin

Webová stránka codecard, nyní přesměrovaná na:

http://www.volny.cz/petr.ptasnik/codecard.html