

Zapomeňte PIN?

V minulém čísle jsme si povšimli šifrovací pomůcky nazvané codecard a ukázali jsme, že se dá luštit. Nyní naznačíme, jak tomu lze jednoduše zabránit, a podíváme se také na některé její další zajímavé vlastnosti.

Jak jsme viděli minule, pravidla předepsaná výrobcem pro zaznamenání PIN na codecard zanášejí do této pomůcky bezpečnostní slabinu. Připomeňme si, že máme k dispozici čtyři možnosti, jak nastavit fólii na papírovou codecard, dva způsoby vyčítání čísel z ní (zleva nebo zprava) a pro „souřadnice“ přiložení fólie na kartičku všechny kombinace písmen A až S a čísel 1 až 15. Celkem tedy dostáváme $4 \cdot 2 \cdot 19 \cdot 15 = 2280$ možných postupů šifrování (klíčů), což při 10 000 možných hodnotách PIN nevypadá na první pohled špatně. Ukázali jsme si však také, že každé vyplněné pole na codecard nám ve skutečnosti omezuje množinu klíčů a čím více polí je zaškrtnuto, tím méně klíčů připadá v úvahu. U příkladu, který jsme uvedli minule, jsme nakonec měli jen dva možné klíče – a to je velmi špatně.

OVĚŘENÍ SÍLY CODECARD

Nabízí se otázka, zda to nebylo jen výběrem konkrétních PIN a klíče. Abychom naše závěry objektivizovali, udělali jsme následující experiment. Pro každé N od jedné do šesti, což je počet vyplněných polí na codecard, jsme zvlášť udělali stejný experiment o 1 000 000 pokusů. V každém pokusu jsme zvolili N náhodných PIN, náhodně jsme vybrali jednu z osmi metod vyčítání a náhodně jsme vybrali klíčové písmeno a číslo (A1 až S15). Potom jsme tyto PIN zašifrovali a vytvořili tak virtuální obraz kartičky s N vyplněnými poli – a tu jsme zkoušeli luštit programem *disppin*, jak bylo popsáno minule v první části tohoto článku.

Program nám tak v každém pokusu postupně vyzkoušel všech 2280 možných dešifrování a u každé obdržené dešifrované sady PIN zkontroloval, zda mohla vzniknout

podle pravidel šifrování – pokud ano, zaznamenali jsme počet nalezených řešení PR. Takto jsme získali milion čísel PR(i) pro $i = 1$ až 1 000 000, z nichž jsme vypočetli *průměr*, *minimální* a *maximální* obdrženou hodnotu, jak ukazuje připojená tabulka ve sloupci *metoda 1 až 8*. Dále jsme zjistili počet těch případů, kdy PR(i) bylo menší nebo rovno trojnásobku čísla N. V těchto případech by byl útočník úspěšný, protože by jednoduše vyzkoušel maximálně $3 \cdot N$ možných klíčů, které by mu *disppin* nabídl (viz první část článku). Tento počet, vztažený k milionu celkem provedených pokusů, je uveden v tabulce ve sloupci *úspěšnost luštění* a udává **pravděpodobnost**, že útočník bude **stoprocentně úspěšný**. Jak vidíte, tato pravděpodobnost rychle vzrůstá s počtem vyplněných polí.

V tabulce jsou pro srovnání uvedeny také výsledky při použití pouze „nejpřirozenějšího“ způsobu vyčítání (sloupec *metoda 1*) a téhož způsobu kombinovaného ještě s postupem „odzadu“ (*metoda 1 a 2*); v řádce *neřešeno* je počet případů, kdy vybraný klíč vůbec neumožňoval PIN podle pravidel zašifrovat (podrobnosti viz dále).

EXISTUJE VÝCHODISKO?

Naše experimenty tedy jen potvrdily obavy vyslovené minule, kdy jsme vás také vyzvali k hledání nějaké cesty ke zvýšení bezpečnosti codecard. Pokud jste tak učinili, můžete si teď své úvahy porovnat s našimi (a pokud

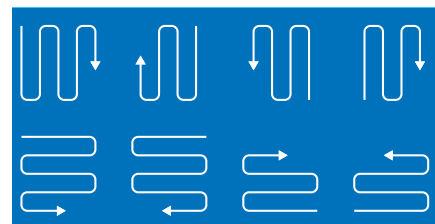
1	7	5	0	4	6	2	9
3	9	7	6	0	7	4	6
5	0	3	7	1	9	3	8
4	8	1	9	3	0	5	7
2	6	2	8	5	8	1	0
3	7	4	0	2	6	4	9

Obr. 1. Drobná modifikace pravidel umožňuje šifrovat jeden PIN více způsoby.

jste nám nějaké podnětné návrhy poslali či ještě pošlete, vrátíme s k nim příště).

Ukazuje se, že existuje velmi jednoduchá **úprava pravidel**, po níž se pomůcka stává nesrovnatelně bezpečnější. (Neříkáme ale, že je pak zcela bezpečná, a uvedeme i nevyhody navrženého zlepšení.) Nejjednodušším doporučením samozřejmě je při vybarvování čtverečků, tedy při zašifrování PIN, **nevybírat vždy první výskyt** dané číslice v poli, ale až nějaký „pozdější“. Pochopitelně půjde většinou o první nebo druhý výskyt, jinak by se nám nemuselo podařit daný PIN vůbec zašifrovat – vždyť v každém výřezu fólie o rozměrech 6×8 čtverečků se daná cifra vyskytuje jen cca 4krát až 5krát. Postup zašifrování čísla 5721 podle tohoto pozměněného pravidla ukazuje obrázek 1, kde je použito základní nastavení fólie a klíč K2 (první, druhou a třetí číslici jsme vybrali ne hned z první nabídky).

Takové pravidlo nám potom umožní zašifrovat jeden PIN více způsoby. Přitom si nemusíme pamatovat, kterou číslici jsme vynechali (!), protože při odšifrování se nám PIN jednoduše „vysvítí“, a nic jiného nepotřebujeme. Pokud někdo nalezne takto vyplněnou codecard, musí počítat skutečně se **všemi 2280 možnostmi**, jak PIN odšifrovat. Důkaz je jednoduchý: ať si vybere jakýkoliv z osmi způsobů přiložení fólie a vyčítání čísel a jakoukoliv z 285 souřadnic a přiloží fólii na codecard, vždy z ní vyčte nějaké čtyři číslice. Na způsob vyplňování zde neexistuje žádné omezení, a proto všechny „vysvícené“ hodnoty jsou platné (neexistují nemožné šifrové texty).



Obr. 2. Znárodnění trasy výběru PIN v dílčích polích

V KAŽDÉM EXPERIMENTU (N) PROVEDEN 1 MILION TESTŮ				
Polí (N)		metoda 1	metoda 1 a 2	metoda 1 až 8
1	PRŮMĚR	144	143	570
	ÚSPĚŠNOST LUŠTĚNÍ	0,00438	0,00354	0,00240
	MINIMÁLNÍ	1	1	1
	MAXIMÁLNÍ	285	285	1140
	NEŘEŠENO	277	260	221
2	PRŮMĚR	75	73	289
	ÚSPĚŠNOST LUŠTĚNÍ	0,04347	0,04284	0,00954
	MINIMÁLNÍ	1	1	1
	MAXIMÁLNÍ	279	282	1120
	NEŘEŠENO	527	493	433
3	PRŮMĚR	41	39	153
	ÚSPĚŠNOST LUŠTĚNÍ	0,21824	0,22203	0,06030
	MINIMÁLNÍ	1	1	1
	MAXIMÁLNÍ	276	257	1041
	NEŘEŠENO	791	729	654
4	PRŮMĚR	23	22	83
	ÚSPĚŠNOST LUŠTĚNÍ	0,49197	0,50458	0,20986
	MINIMÁLNÍ	1	1	1
	MAXIMÁLNÍ	242	254	962
	NEŘEŠENO	1068	934	837
5	PRŮMĚR	13	13	47
	ÚSPĚŠNOST LUŠTĚNÍ	0,72910	0,74348	0,42628
	MINIMÁLNÍ	1	1	1
	MAXIMÁLNÍ	218	217	943
	NEŘEŠENO	1323	1214	1036
6	PRŮMĚR	8	8	28
	ÚSPĚŠNOST LUŠTĚNÍ	0,87832	0,88823	0,63249
	MINIMÁLNÍ	1	1	1
	MAXIMÁLNÍ	200	196	781
	NEŘEŠENO	1520	1485	1293

Výsledky lušticího experimentu

- Podívejme se nyní, jak lze dále zvýšit počet možných způsobů šifrování. Dosud jsme PIN vyčítali dvěma způsoby znázorněnými v horní části obrázku 2. Můžeme však přijmout jiný způsob vyčítání, například po řádcích (a zase doprava nebo doleva, viz dolní část obrázku 2), po úhlopříčkách a podobně. Zkrátka jde o to, vybrat si nějaký „geometrický vzor“ a ten použít. Čím více, tím lépe. Další možnosti vznikají přikládáním fólie otočené o 90 nebo 270 stupňů, tak říkají „naštorc“.

pořadí zapsána v záhlaví kartičky). To je sice mnohem náročnější na paměť, nicméně zdatným dává další možnosti použití. Připomeňme, že i při šifrování tímto způsobem bychom sem tam nějakou číslici měli vynechat, tj. neoznačovat vždy první výskyt dané číslice na trase.

Ačkoliv tento konkrétní exotický způsob vyčítání nemusí být obecně bezpečný, pokud zůstane utajen, stává se ve skutečnosti novým klíčem. Jak je mohutný a jak je pak prostředek bezpečný při vyrazení této

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

Obr. 3. Exotické trasy a využití fólie

V úvahu připadá i trochu „exotické“ použití fólie, při němž bychom ji přiložili do základního postavení (levý horní roh fólie na levý horní roh kartičky) a nepohybovali bychom s ní! Zvolili bychom si jen tajný klíč (třeba K2) jako počátek trasy a nějakou trasu (geometrický vzor) vyčítání čísel přes celou fólii 20 × 26. Na trase bychom pak vyčítali vysvícené číslice po čtyřech a dostávali tak postupně jeden PIN za druhým (příslušná označení by např. byla v odpovídajícím

metody, záleží na metodě samé a dalších okolnostech. Podobně exotických metod lze pochopitelně vymyslet ještě mnoho a mnoho, třeba jako na obrázku 3. Protože si však codecard zřejmě pořídí lidé s nepříliš dobrou pamětí, nelze předpokládat, že by většina z nich nějaký exotický způsob použila. Útočník proto může počítat se standardními pravidly (případně námi vylepšenými) a základním způsobem vyčítání.

KONSTRUKCE CODECARD

Víme už, že jednoduchou modifikací pravidel šifrování lze zásadním způsobem zvýšit bezpečnost codecard – postačí označovat nikoli první, ale „nějaký“ výskyt dané číslice PIN. Může se však stát, že ani nyní nepůjde každý PIN zašifrovat všemi 2280 klíči. Codecard má totiž jednu drobnou vadu – podíváme-li se na fólii podrobněji (pro příklad postačí základní nastavení), uvidíme, že některé klíče dávají nevhodná klíčová pole. Například klíčové pole C3 při vyčítání zleva i zprava neumožňuje zašifrovat celkem 174 číselných kombinací! Je to vidět na obrázku 4: v příslušném výřezu 6 × 8 čtverečků jsou jen tři šestky, přičemž první z nich je až uprostřed pole. Navíc není vhodné ani rozložení sedmiček. Pokud tedy budeme šifro-

vat PIN začínající na dvě šestky, zbývá nám v klíčovém poli sekvence 7, 9, 8, 3, 1, 5, 2, 4, 1, 7, 0, 9, 8, 6, 7. To nám neumožní zašifrovat zbývající dvojice číslic rovné například 00, 01, 02, 03, 04, 05, 23, 25 nebo 71 až 75 a podobně.

Takových nevhodných výřezů je kromě C3 ještě více (například B3, D3, problémy s osmičkou mají zase O6, P6, Q6, R6, S6 apod.). Za všech osm metod je to celkem 3768 nemožných šifrování PIN. Je to však nepatrný zlomek z 2280 × 10 000 možností, takže při modifikovaných pravidlech nám tato vlastnost fólie tolik nevadí. Zbývá otázka, zda by bylo možné (doutáme, že ano) navrhnout jiné rozložení číslic na fólii tak, aby umožňovala zašifrovat všechny kombinace PIN pro všechny možné klíče. Ale to už vám necháváme jako bonbonek na zbytek prázdnin...

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

Obr. 4. Klíčové pole C3 neumožňuje zašifrovat například PIN 6661 nebo 6605.

Předpokládáme, že nám autoři neprozradí, jak „náplň“ fólie navrhovali (nebo ano?), a tak se to můžete pokusit odhadnout sami. Pár poznámek přece jen na úvod máme. Stávající fólie je konstruována tak, že až na výjimky jsou v lichých sloupcích číslice 1...5 a v sudých 6...9 a 0. Liché sloupce ukazují obrázek 5 – jsou zde patrné některé pravidelnosti, které se ale ukazují být příliš nesystematické. Základním požadavkem na fólii – aby se s ní vůbec dalo šifrovat – je, aby v každém výřezu 6 × 8 byla každá cifra obsažena minimálně čtyřikrát (abychom mohli zašifrovat PIN složený ze stejných číslic). Není to však postačující pravidlo, protože pokud budou tyto cifry (X) ve výřezu těsněji za sebou, nemusíme být schopni zašifrovat PIN typu YXXX nebo XXXY. Obecné pravidlo, které by zajišťovalo zašifrování jakéhokoliv PIN, by tedy znělo, že při dané metodě vyčítání by měly jít za sebou vždy sady číslic 0123456789 v různých permutacích. To však dodrženo není, a dokonce není dodrženo ani požadavek povinné přítomnosti čtyř výskytů každé cifry v každém výřezu 6 × 8.

ZPŮSOB ZAŠIFROVÁNÍ „JE VIDĚT“

V tabulce experimentů jsou údaje ve sloupcích *metoda 1* a *metoda 1 a 2* téměř stejné. Ptáte se, jak je to možné, když více metod by mělo obecně dát více řešení? Odpověď je jednoduchá. Metody 1 a 2 od sebe rozeznáte prakticky vždy přímo ze šifrového textu. U metody 1 (postup zleva) budou zvýrazněná pole blíže levému kraji, u metody 2 (postup zprava) blíže k pravému kraji. Jen v některých případech to nebude příliš zřetelné, a ty také vytvářejí o něco více řešení, pokud uvažujeme obě metody.

Z praktického hlediska to znamená, že luštitel (při šifrování podle původních pravidel) může to, zda byla použita metoda 1 nebo 2, určit pouhým pohledem na vyplněnou codecard. Protože jsou to zřejmě dvě v praxi nepoužívané metody, je to pro něj stejně náročné, jako kdyby uvažoval jen metodu 1.

JAK SI ZADĚLAT NA MALĚR

Používáme-li codecard, to nejhorší, co můžeme udělat, je zašifrovat na ni své osobní karty společně třeba s kartou CCS, kterou jsme dostali od zaměstnavatele. Pak má zaměstnavatel v roli luštitel (netvrdíme, že to zaměstnavatelé dělají) šanci zjistit PIN vašich soukromých karet. K tomu stačí spustit program *disppin* (či jakýkoliv jiný se stejnou funkcí) a vybrat ta nalezená řešení, v nichž se u CCS vyskytuje odpovídající PIN. V drtivé většině případů bude stoprocentně úspěšný!

Stejná (ne-li horší) situace nastane, pokud na codecard uložíme také PIN nějaké další osoby (manželky, manžela ap.). Jak potvrzují statistiky, velmi mnoho

Pozor, některé bankomaty umožňují zadávat větší počet nesprávných PIN za sebou!

manželských párů se rozvádí – zhrzený partner pak může mít mnoho důvodů (jistě více než zaměstnavatel) ke snaze zjistit PIN k vašim kartám, ale také například k osobnímu organizéru (kde si lze přičíst třeba některé zajímavé kontakty na jiné partnery či partnerky...).

A raději už ani nemysleme na případ, že by vás někdo se zlým úmyslem požádal, abyste mu nějaký PIN připsali na svou codecard...

MALÝ DOVĚTEK

Ukázali jsme, že pravidla používání codecard by se měla změnit, a navrhli jsme jak – v podstatě nepatrná změna přitom přiná-

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

Obr. 5. Liché sloupce fólie a některé pravidelnosti

ší značný bezpečnostní efekt. Myslíme si však, že k ochraně dat se nemá využívat „lidová tvořivost“ tohoto druhu – autoři codecard by proto možná mohli naše poznatky respektovat v eventuální další verzi této pomůcky.

A ještě drobnou pikantnost na závěr. Codecard mj. spoléhá na to, že bankomat neumožní více než tři chybná zadání PIN; jak mě upozornil kolega Rosa, nemusí tomu tak být vždy. Stačilo zajít k bankomatu a zarisovat „sežráné“ karty. Připadal jsem si sice jako nějaký kriminální živel, ale věda žádá oběti. Pokusů jsem zanechal po šesti špatných zadáních PIN! Pak jsem ale pokračoval na jiném bankomatu s dalšími šesti, takže jsem celkem vyzkoušel (bez jakýchkoli

námitek přístroje) 12 chybných PIN za sebou! Můj bankovní dům takové pokusy prostě nezakazuje, což sice zapomenlivý člověk občas uvítá, ale za šťastné řešení to rozhodně nepovažuji...

Naše prázdninová ukázka „užití kryptoanalýzy a kryptografie“ tím končí. Snad jsme vás po dávce spíše teoreticky zaměřených článků přesvědčili, že tento obor má docela blízko i k běžnému životu v moderní společnosti a že může být v leccems užitečný. Možná jste si i trochu zapřemýšleli a pohráli s numírkou, ale také si snad odnesli ponaučení, že ostražitost není v dnešním světě plněm číslem nikdy dost. ■ ■ ■

Vlastimil Klíma, autor@chip.cz