Epilog
Klec v místnosti 31

Kapitán Carda přivezl za zvýšených bezpečnostních opatření nejcennější exponát výstavy – dosud neznámou variantu **chameleóna**, kterého nazval Cryptomelon Pragensis. Chameleón byl uzavřen do speciálně zabezpečené klece v poslední výstavní místnosti 31.

Klec byla opatřena kódovým zámkem. Kapitán Carda zadal kód, kterým zámek uzavřel. Chameleón tak zůstává v naprostém bezpečí, kód lze totiž získat jedině tak, že jej někdo bezchybně zadá.

Kapitán Carda se svěřil přítomným novinářům, že podle něj to není prakticky možné. Na otázku, co se stane, když on sám kód zapomene, odpověděl, že by to nevadilo, protože je schopen kdykoliv kód odvodit. Dokonce řekl novinářům, že je ochoten jim postup sdělit, ale je přesvědčen, že i tak jim to nebude nic platné. Po menším naléhání postup prozradil, ale zdůraznil, že je tam několik neznámých, které jim neprozradí a tím zaručí bezpečnost své chlouby Cryptomelona Pragensis.

Kapitán Carda začal vysvětlovat, jak kód připravil:

„Nejdříve jsem sepsal tajná jména všech třiceti chameleónů, které jsem zde na výstavu přivezl a které jsou po jednom uloženy v místnostech 1 až 30. Potom jsem jména sepsal do dvou sloupců o 15-ti řádcích. Nejdříve jsem zaplnil sloupec první a pak druhý. V prvém řádku je tedy tajné jméno prvého a šestnáctého chameleóna atd.
Potom jsem v textu zvolil jedno slovo, které jsem přesvědčen, že nezapomenu. Slovo je vytvořeno jednoznačně v tom smyslu, že jsem vzal prvé písmeno slova a v textu vyznačil jeho prvý výskyt. Pak jsem vzal druhé písmeno slova a od místa, kde jsem skončil, jsem nalezl opět prvý výskyt tohoto druhého písmene a takt jsem pokračoval dále. Mimochodem poslední písmeno zvoleného slova leží v posledním řádku. Pro jistotu jsem si však vyrobil mřížku, kterou, když na text přiložím, tak slovo uvidím. Takové šifrovací mřížce se říká Cardanova“ (nezapomněl poučit novináře kapitán Carda o svém nejoblíbenějším systému).
„Mřížku jsem schoval do trezoru a nikdo se k ní nedostane“ , pokračoval ve svém výkladu. *Původně jsem chtěl toto slovo použít jako kód zámku na klec s chameleónem. Pak jsem si však vzpomněl na přednášky z informační bezpečnosti a bylo mi najednou jasné, že to není dokonalé heslo, protože by jej mohl někdo uhodnout a nebo se mohl pokusit otevřít klec „slovníkovým útokem“. Rozhodl jsem se tedy heslo zesílit velmi důmyslným a dosud nikde nepopsaným způsobem. Jsem přesvědčen, že ani můj známý Pavel Vondruška takovýto postup nezná! No* (upřesnil kapitán Carda), *alespoň si myslím, že nezná, protože tento postup ve své knize Kryptologie, šifrování a tajná písma nepopsal.*
Zesílení spočívá v tom, že za heslo neberu přímo písmena kódu, která lze v otvorech Cardanovy mřížky přečíst, ale písmena následující přímo v textu vpravo za nimi. Kód tedy vypadá zcela náhodně a nelze jej získat slovníkovým útokem.
Jsem přesvědčen, že chameleóna mi nikdo do konce výstavy (začátek listopadu) neukradne, neboť na rozdíl ode mne nezná tajná jména mých třiceti chameleónů a nemá moji mřížku!

Novináři výkladu kapitána Cardy příliš nerozuměli, a tak jim vše vysvětlil ještě jednou na malém příkladu. Vzal 6 slov a sepsal je do dvou sloupců po třech.

DNES	BOTA
BOK	NOS
VLAK	BRÁNA

Potom zvolil vhodné slovo - BASA. Toto slovo je v dané tabulce vepsáno výše popsaným jednoznačným způsobem. Příslušná Cardanova mřížka by vypadala tak, že by měla vystřižené mezery v místech, které vyznačil žlutě. Kód k zámku klece je v tomto případě OBVK (písmena ležící za vybraným slovem BASA).

Foto: Hackerský útok na vzácného chameleóna ….
(z archívu autora)