Sifry a jejich luštitelé

Hynek Paštěka

Snaha skrýt obsah zprávy před nepovolanýma očima provází lidstvo již zhruba tři a půl tisíce let. Od provázků s uzlíky a jednoduchých tabulek jsme se dostali k vysoce sofistikovaným metodám, které využívají ty nejrychlejší počítače. I dnes jsou šifry považovány za zbraň. A existují lidé, kteří vynalézání šifer a jejich zpětnému luštění zasvětili svůj život.

Pavel Vondruška (52) sám sebe sice označuje jako kryptologa v důchodu, přesto má k problematice šifrování stále co říci. Je jedním z lidí, kteří po celá devadesátá léta vymýšleli a připravovali systém šifrování pro státní orgány, o dějinách šifrování napsal knihu, přednáší tuto problematiku na Matematicko-fyzikální fakultě UK a vydává o ní také časopis.

Začalo to Veledetektivem

„Šifry mě začaly zajímat v devíti letech, kdy jsem dostal pod stromeček mimo jiné knihu s názvem Veledetektiv Agaton Sax. Ten s pomocí Velké knihy kódů vyluštil vzkaz a já jsem to chtěl zkusit po něm. Jenže v té době tady žádná taková kniha nebyla. Tak jsem začal prohledávat jiné knihy, jestli někde nejsou zmínky o šifrování. Na něco jsem narazil třeba v knihách Julesa Verna nebo Edgara Alana Poea, ale moc jich nebylo.

V současné době můžeme pozorovat růst používání šifer a kódů v komerční sféře.
Pavel Vondruška

O šifry jsem se ale zajímal stále. Třeba na gymplu se to o mně vědělo, takže mi lidé psali zašifrované pohledy a já je udivoval tím, že jsem je vždy dokázal rozluštit. Pak u mě ale přece jen převážil zájem o matematiku, kterou jsem vystudoval, a pak jsem působil tři roky v akademii věd," rozebírá své kryptologické začátky Vondruška.

Po nějaké době však dostal nabídku, jestli by se nechtěl věnovat oboru, který úzce s matematikou souvisí. O jeho matematickém talentu se vědělo již dřív, podobně jako o zálibě v šachách. Absolvoval roční kurz kryptoanalýzy, který byl zakončen písemnou pětihodinovou zkouškou. Úspěšně ji složil a stal se profesionálním kryptologem.

Enigma na stole

Otevírá hnědý kufřík a ukazuje některé předměty, které mají se šifrováním mnoho společného. „Tak například tohle je legendární německá Enigma," říká a vytahuje přitom elektronické zařízení se spoustou diod a malou klávesnicí. „Není samozřejmě mechanická, ale jinak funguje úplně stejně. Prodávají ji v muzeu kryptologie v Nizozemsku a každý kus je číslován," dodává.

Následují dvě logaritmická pravítka, na kterých ovšem nejsou číslice, ale písmena. „Pomocí nich šifrovala naše armáda v padesátých letech. Za určitých podmínek s nimi lze vytvořit neprolomitelnou šifru.

Pak tu mám dvě bakalářské práce zabývající se rozborem šifrovacích strojů. Jedna z nich se věnuje německému stroji Lorenz, který používala německá armáda pro komunikaci mezi vrchním velitelstvím a velením jednotlivých armád. Věděli, že Enigma není až tak bezpečná, jak se předpokládalo," vysvětluje.

Kryptologická show

Ve státních službách, například v Národním bezpečnostním úřadu (NBÚ), strávil Pavel Vondruška deset let. Jeho působení tam bylo především v první polovině 90. let spojeno s různými omezeními. Například nesměl být nikde veřejně vyfotografován, nesměl publikovat a cestovat. Byl ale natolik ponořen do šifer, že mu to vlastně ani nevadilo. Navíc se mu spolu s kolegy v roce 1999 podařilo v Praze uspořádat konferenci Eurocrypt, která je něco jako kryptologická olympiáda. Sjela se na ni všechna světová esa.

„Já jsem například měl možnost asistovat u přednášky legendárního izraelského kryptologa Adiho Shamira. Na jeho pokyn jsem při předvádění optoelektronického zařízení pro luštění RSA v sále zhasínal a rozsvěcel světlo," usmívá se Vondruška a dodává:

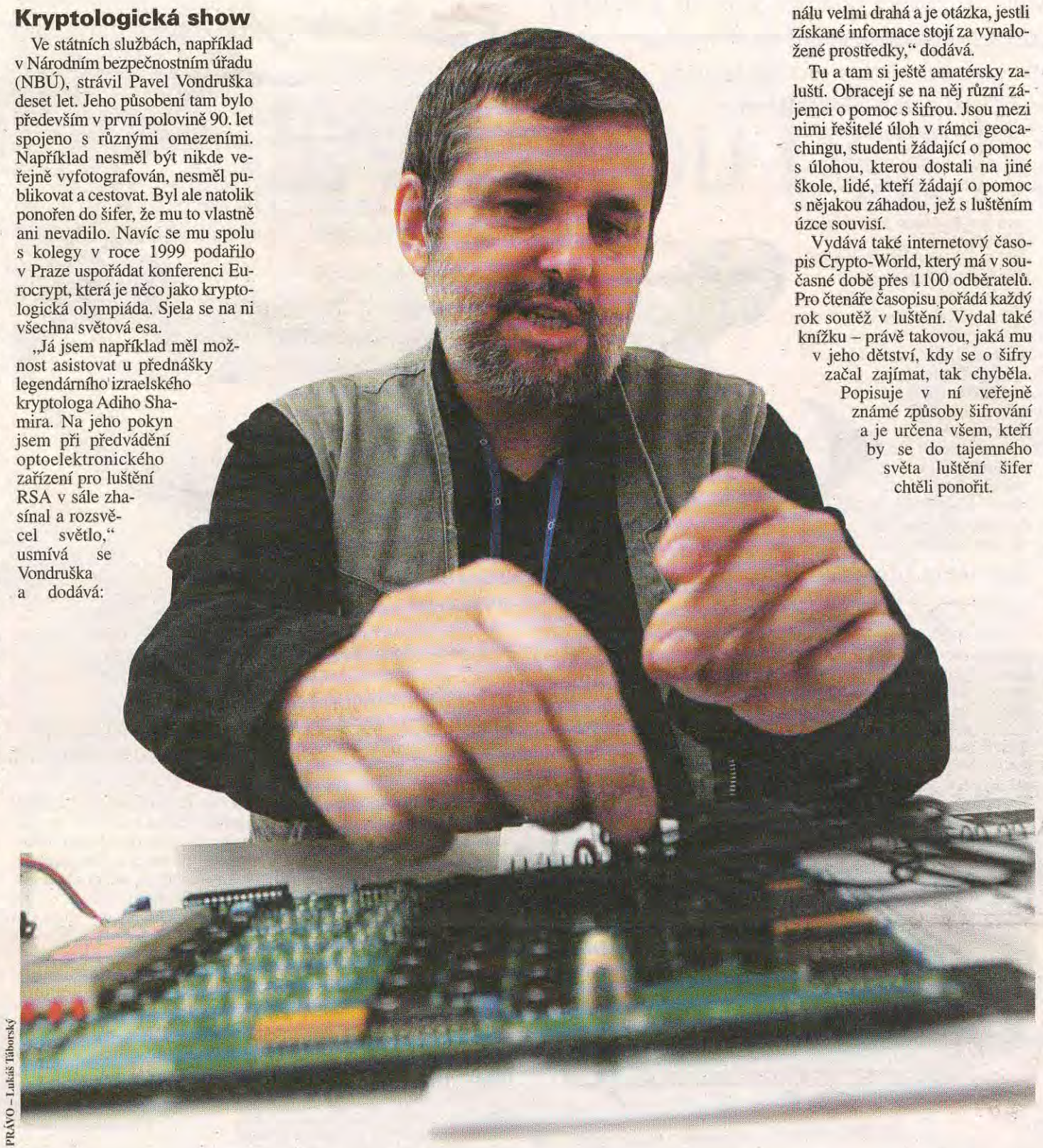

Foto PRÁVO – Lukáš Táborský

Pavel Vondruška u legendární německé Enigmy.

„Ale vážně, pro nás to byla opravdu velká událost. Bylo to znamení, že se opět dostáváme v oblasti kryptologie na dobrou úroveň."

Kryptolog ve výsluze

V roce 2000 se rozhodl ze silových resortů odejít. Ještě se nějaký čas podílel na vývoji systému pro elektronický podpis a teď pracuje pro jednoho českého operátora – testuje bezpečnost celého systému a pracuje na jeho vylepšení a především se zabývá zavedením šifrování v běžné praxi. „V současné době můžeme pozorovat růst používání šifer a kódů v komerční sféře. Dříve měly šifry používané v diplomacii a armádě před těmi civilními náskok desítek let, ten se nyní trochu zmenšuje. Kódování používané například pro mobilní telefony nebo čipové karty je proti prolomení běžnými prostředky velmi bezpečné," vysvětluje Pavel Vondruška.

Podle něj by sice šlo použít i lepší, ale bylo by to na úkor uživatelského pohodlí a také ceny. „Víte, že když pojedete autem a narazíte do stromu, tak se můžete zabít. Ale nebudete kvůli tomu jezdit tankem. Navíc jsou zařízení umožňující dekódování mobilního signálu velmi drahá a je otázka, jestli získané informace stojí za vynaložené prostředky," dodává.

Tu a tam si ještě amatérsky zaluští. Obracejí se na něj různí zájemci o pomoc s šifrou. Jsou mezi nimi řešitelé úloh v rámci geocachingu, studenti žádající o pomoc s úlohou, kterou dostali na jiné škole, lidé, kteří žádají o pomoc s nějakou záhadou, jež s luštěním úzce souvisí.

Vydává také internetový časopis Crypto-World, který má v současné době přes 1100 odběratelů. Pro čtenáře časopisu pořádá každý rok soutěž v luštění. Vydal také knížku – právě takovou, jaká mu v jeho dětství, kdy se o šifry začal zajímat, tak chyběla. Popisuje v ní veřejně známé způsoby šifrování a je určena všem, kteří by se do tajemného světa luštění šifer chtěli ponořit.

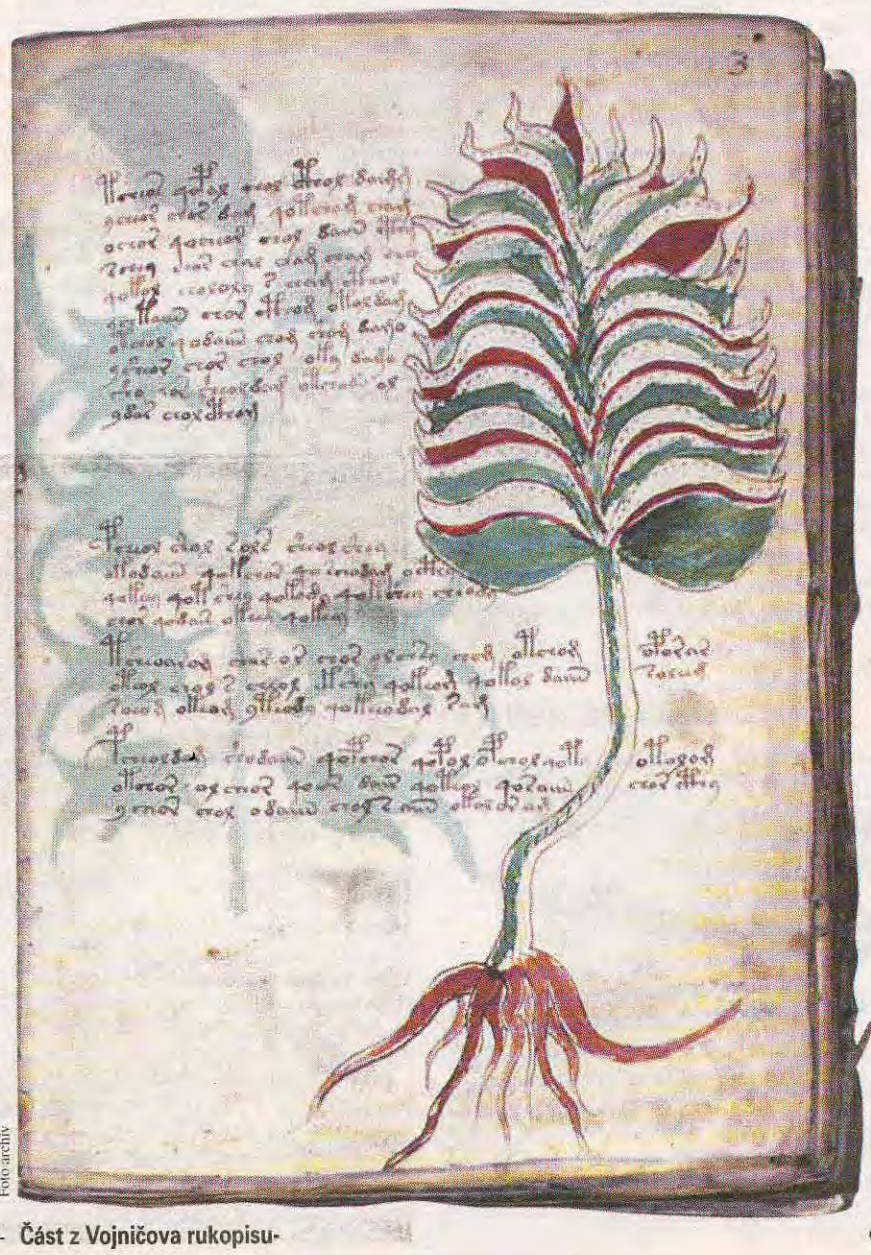

Foto archiv

Část z Vojničova rukopisu

Nejzáhadnější rukopis světa

Existuje vůbec neprolomitelná šifra? Pavel Vondruška tvrdí, že takové šifry sestavit lze, říká se jim absolutně bezpečné. Podle něj je poměrně rozšířený názor, že každá šifra je po nějakém čase rozluštitelná, nesmysl. Jako stoprocentní odborník zcela jistě ví, o čem mluví. Kromě toho v dějinách kryptologie existují i případy, kdy se šifru, i když nepatří do třídy absolutně bezpečných, nepodařilo rozluštit ani po celá staletí. Jednou z nich je takzvaný Vojničův rukopis.

Ten dostal jméno podle antikváře, který jej v roce 1912 objevil a zakoupil v Itálii. Jedním z jeho majitelů byl například císař Rudolf II. Má 250 stran s texty a kresbami a postupně dostal přízvisko „nejzáhadnější rukopis světa". Kresby totiž obsahují fantastické rostliny a výjevy a dosud není znám jazyk, písmo ani případná šifra, kterou je rukopis napsán. Badatelé tedy řeší jednu rovnici o třech neznámých.

Čechokanaďan Jan Hurych (72) se pokusům o jeho rozluštění věnuje již deset let a zařadil se tak mezi dlouhou řadu těch, kteří se pokoušejí nebo pokoušeli o totéž.

„S rukopisem jsem se seznámil před deseti lety v knize Davida Kahna Codebreakers. Pochopitelně mě zaujalo to, že rukopis je vlastně i částí naší české historie, i když jeho autorem nemusí být zrovna Čech (ale vyloučit to nelze)," říká Jan Hurych. První články o rukopisu mu vyšly v roce 1999 v internetovém časopisu Hurontaria anglicky a hned nato i česky. Později se připojil do mezinárodní korespondenční konference a dnes píše asi do tří anglických žurnálů o rukopisu.

Hurychův výzkum se týkal historie rukopisu, jeho autora, písma a snažil se rozluštit i jazyk či šifru, ve které je zakódován. „Došel jsem k názoru, že rukopis patrně přivezl do Čech nějaký cestovatel – mohl to být nejprve Vojničem citovaný Angličan John Dee, ale mohl to být třeba i Kryštof Harant z Polžic a Bezdružic, asi ke konci 16. století, blíže už to asi neurčíme," vysvětluje Hurych, jinak profesí elektroinženýr.

Hrozí ztráta tajemnosti

Na projektu pracovala řada známých vojenských kryptografů z první i druhé světové války, ale marně. Někteří badatelé se dokonce domnívají, že jde o zašifrovaný nesmyslný text nedávající smysl.

To si ale Jan Hurych nemyslí. V době, kdy byl text psán, byla cena za pergamen enormní a výzkumy ukazují, že se v textu například opakují určité koncovky slov. Pravděpodobnější je, že se jedná o zašifrovaný vědecký nebo náboženský text, který bylo nutné ukrýt před nepovolanými zraky, jako byla například inkvizice nebo konkurence.

Navrhl jsem proto použít metody umělé inteligence, například neuronové sítě, kde se počítač umí sám učit z výsledků dokonce rychleji a lépe než člověk.
Pavel Vondruška

„Navrhl jsem proto použít metody umělé inteligence, například neuronové sítě, kde se počítač umí sám učit z výsledků dokonce rychleji a lépe než člověk. Zatím však máme ještě potíže se sestavením takového programu. Jedno je ale jisté: až – všimněte si, že neříkám ‚jestli'– tedy až někdo záhadu Vojničova rukopisu vyřeší, bude to i jisté minus. Přestane totiž být tím nejzáhadnějším rukopisem světa," říká Hurych.

S bednou do tmy

Zájem o šifry kromě jiného znamená, že se rád zúčastňuje šifrových soutěží *vedoucích* ulicemi českých měst. Nejznámější se koná v Brně pod názvem Tmou a v Praze se jmenuje Bedna. Jde o závod pro tří- až pětičlenná družstva, která musejí po celé trase luštit šifry. Ty jim pomohou dostat se na další stanoviště.

Postupně se na tyto soutěže hlásí stále víc družstev a s tím se zvyšuje i náročnost zadaných úkolů. „Poslední Bedny se zúčastnilo přes 200 týmů, do cíle v limitu ale došel jen jeden. My jsme skončili na jedenáctém stanovišti, dál už to nešlo. Ale ta radost, když se nám podařilo vyluštit některou šifer, to je prostě paráda. Příští rok jdeme zas, třeba se bude dařit lépe," dodává Pavel.