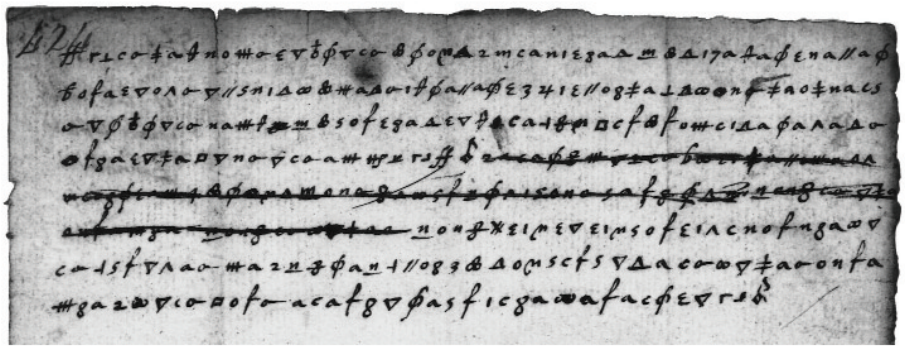
Oblíbené mýty a omyly (2)

Koncem května t. r. se v areálu Pražského Hradu bude konat již devátý ročník konference Information Security Summit 2008. Autoři seriálu kryptologie pro praxi se zde budou zabývat oblastí RFID, ale i tématem oblíbených mýtů a omylů v kryptologii.

Mýtus první: Kryptologie je šifrování

To platilo čtyři tisíce let. Před třiceti lety se ale kryptologie změnila. Nyní je to věda o matematických metodách informační bezpečnosti. Má dvě části, kryptoanalýzu a kryptografii. Předmětem kryptografie je návrh nejrozmanitějších matematických metod informační bezpečnosti (jejich příklady viz dále), kryptoanalýza se zase zabývá odhalováním slabin všech těchto nejrozmanitějších metod, nástrojů, protokolů apod. Výsledkem kryptoanalýzy může být klíč nebo otevřený text jako dříve, ale dnes je zajímavý také falšovaný elektronický podpis, změna dat přes šifrový text, ale i důkaz toho, že nějaká kryptografická technika má menší složitost nebo větší riziko prolomení, než si její tvůrci představovali.



Obr. 1 Šifrování bez autentizace dovedlo královnu na popraviště [2]

Mýtus druhý: Šifrování řeší všechno

Na tento mýtus doplatila královna Marie Stuartovna. Byla popravena proto, že její šifry neposkytovaly autentizaci dat. A tak bylo možné její šifrogram doplnit o neautentizovaná data, která ji nakonec dovedla na popraviště (luštitel dopsal dovětek, v němž jménem Marie vylákal jména osob připravujících atentát). Informační bezpečnost dnes vyžaduje a kryptografie zajišťuje tyto služby:

- utajení,
- integrita,
- autentizace,
- a nepopiratelnost.

Těchto služeb kryptografie dosahuje různými technikami, jako jsou:

- symetrické šifry – proudové, blokové,
- autentizační kódy zpráv (MAC),
- hašovací funkce,
- klíčové hašovací autentizační kódy zpráv (HMAC),
- generátory náhodných znaků a pseudonáhodné generátory,
- asymetrická schémata digitálního podpisu,
- asymetrická schémata pro šifrování,
- asymetrická schémata dohody na klíči,
- kryptografické protokoly,
- a další.

Bez nich bychom v informačních systémech mohli s daty manipulovat různým způsobem (někdy i „nad šifrou“), a přitom bychom docílili kýženého efektu.

Mýtus třetí: Kryptologie je něco zvláštního

Kryptologie je v některých případech zcela nepostradatelná (například v komunikacích). Umožňuje zajistit potřebné a důležité základní služby informační bezpečnosti, které využívají nadstavbové informačně bezpečnostní služby. Z různých hledisek se proto může zdát výjimečná, a to historické tajemno jí také zůstalo. Proto si kryptologové rádi namlouvají, že jejich dítě je něco zvláštního. Z hlediska IT však žádné velké rozdíly od ostatních metod informační bezpečnosti nenajdeme. Například proti tvrzení, že kryptologii se na světě věnuje velmi málo lidí, lze namítnout, že skutečným teoretickým matematickým metodám antivirů, antispamů apod. se věnuje možná ještě méně odborníků. Také představa, že kryptologie je založena více než jiné metody na matematických základech, je neoprávněná. Kryptologové dobře vědí, že používají velmi mohutně heuristiku, možná ještě více než antivirové metody. A způsobí virus snad menší škodu než špatně použitá nebo slabá šifra?

Rovnost kryptologie s ostatními metodami informační bezpečnosti

Z předchozího vyplývá, že kryptologie je jedna z metod informační bezpečnosti, a protože není výjimečná, není (z manažerského hlediska) nutné se jí věnovat více než ostatním metodám, jako třeba antivirům, antispamům nebo firewallům. Na druhou stranu není dobré se jí věnovat méně, neboť její zanedbání má podobné následky jako zanedbání antivirové ochrany nebo zálohování. Zkrátka a jednoduše můžete o data buď přijít, nebo (někdy ještě hůře) se dostanou do rukou konkurenta, médií, hackerů apod. Těžko říci, zda řádění viru v bance je horší než publikování dat o bankovních kontech klientů v médiích.

Svět chce kryptografii rychlou a bezpečnou, i když si to odporuje

Stejně jako ostatní metody informační bezpečnosti je kryptologie smýkána komerčním tlakem tržní ekonomiky na maximální rychlost a minimální cenu řešení. Ve skutečnosti svět nechce bezpečné funkce, ale rychlé funkce, u nichž nejsou známy slabiny (jedině vojenská a speciální řešení aplikují správně přístup opačný: chtějí bezpečnou šifru, která je použitelná).

Tyto požadavky jsou klasicky v přímém rozporu, což klade na výzkum enormní požadavky a zvyšuje riziko malé životnosti (prolomení) takových kryptografických nástrojů. Zde je navíc nutno podtrhnout slovo „zvyšuje“, protože uvedené riziko existuje i tak, vzhledem k nedokazatelnosti bezpečnosti většiny kryptografických nástrojů. Nejen tedy, že po kryptografii chceme nemožné, ale chceme, aby to bylo i rychlé. Je proto vhodné při řízení aplikované kryptologie pamatovat na to, aby používané i nové systémy byly modulární, snadno upgradovatelné, s vyměnitelnými a konfigurovatelnými algoritmy apod., jinak se z drahých zařízení mohou stát také jen bedny šrotu (viz též ST 11 a 12/2007).

Vlastimil Klíma, Tomáš Rosa,
v.klima@volny.cz, trosa@ebanka.cz

LITERATURA

[1] E-archivy http://cryptography.hyperlink.cz, http://crypto.hyperlink.cz

[2] Singh, S.: Kniha kódů a šifer – Tajná komunikace od starého Egypta po kvantovou kryptografii, přeložil Petr Koubský, Nakladatelství Dokořán a Argo, Praha 2003