Kryptologie pro praxi

Vzhledem k rostoucímu významu zejména bezpečnostních hledisek při budování a provozování stále složitějších a nákladnějších informačních a komunikačních struktur v globalizujícím se světě vás chceme průběžně seznamovat s novým oborem, který se zabývá principy matematických metod ochrany dat. První výlet do říše kryptologie jsme učinili v březnovém čísle ST v trendovém článku Vybrané aspekty moderní kryptoanalýzy, kde jsme hovořili o jedné dílčí problematice – o tzv. postranních kanálech, kde česká kryptologie slaví úspěchy i na mezinárodním poli. Kryptologie je však mnohem bohatší a znalost základních pojmů a technik je a bude čím dál tím více prospěšnou součástí počítačové gramotnosti, či chcete-li e-gramotnosti. Také proto se budeme podrobněji zabývat problematikou šifrovacích algoritmů v cyklu volně navazujících příspěvků ve *ST*, který tímto zahajujeme.

Je pravděpodobné, že až na výjimky většina z nás používá nějaké šifrovací zařízení nebo nějaké kryptografické nástroje, aniž bychom si to uvědomovali. Příkladem budiž mobilní telefon, e-bankovnictví nebo platební karty. To jsou systémy založené na kryptografii, bez níž by vůbec nemohly existovat. Kryptoanalýza je naopak věda o luštění šifer nebo obecněji o hledání slabin v různých kryptografických technikách. Kryptologie obě tyto vědy spojuje v jeden celek. Její rozvoj umožnil zdokonalování kryptografických ochran a zvýšení bezpečnosti vůbec. Teoreticky. Prakticky se však setkáváme se spoustou slabin v informačních systémech, vyplývajících ze základních kryptologických neznalostí. Je tedy načase si tyto základní znalosti osvojit, neboť nových možností a metod přibývá téměř exponenciálně. Z tohoto důvodu velké státy na známých univerzitách kryptologii vyučují už více než deset let. Malé státy jsou v nevýhodě, ale i ony potřebují odborníky. Proto se také na MFF UK bude kryptologie vyučovat v novém oboru Matematické metody informační bezpečnosti.

Šifrování používá tajný klíč

Pojmy kódování a šifrování se často slučují. Jejich rozdíl je pro běžného občana téměř nulový, avšak v počítačové praxi se jedná o rozdíl obrovský. Pojem kód obecně označuje množinu výrazů (slov), kterými jsme schopni vyjádřit nějakou informaci. Slova příslušného kódu se skládají ze znaků, které patří do jeho abecedy. Často se stává, že jeden a ten samý reálný nosič informace označujeme jednou jako kód a jednou jako abecedu nějakého jiného kódu. Jako příklad si můžeme vzít třeba známou Morseovu abecedu. Na její základní verzi se můžeme dívat buď jako na kód se slovy (zejména) 0–9, a–z a /, jehož abecedu tvoří znaky tečka, čárka a mezera, nebo jako na abecedu znaků 0–9, a–z a /, nad kterou je pak vytvořen nějaký kód vyšší úrovně – například kód ceskeho jazyka. Slovem kódování pak označujeme přepsání informace z jedné formy kódu do druhé, například přepsání tohoto článku do Morseovy abecedy, kódování textových informací do ASCII, obrazových informací v JPEG, zvuku a videa do MPEG-x apod. Opačný převod informace se označuje jako dekódování. Poznamenejme, že ne všechny cílové kódy lze zpětně jednoznačně dekódovat, příkladem může být například převedení obrázku z formátu s úplnou informací (například GIF) do JPEG. Díky tzv. ztrátové kompresi v JPEG již nelze získat přesně původní originál (to však v řadě případů nevadí). Jistě také znáte kódy pro zabezpečení přenosu informací z hlediska spolehlivosti (kódy detekující a opravující chyby). Do oblasti kódů a kódování patří také komprimační algoritmy, konkrétně se jedná o kódování za účelem snížení redundantní informace. Tento dlouhý opisný název odpovídá teoretickému pohledu na věc. V praxi se ovšem lidé potřebují rychle dohodnout, a tak neustálé zmiňování, že se nejedná o obyčejné kódování, nýbrž o kódování za účelem snížení redundantní informace, se prostě nahrazuje výrazem komprimace. A všichni ví, o čem se mluví. S kryptografií je situace obdobná. Například některé kryptografické metody lze v kontextu nastíněné terminologie definovat také jako kódování za účelem utajení informace. To je ovšem opět příliš dlouhý a nepraktický výraz, takže používáme krátce pojem šifrování. Pokud to někomu připadá v nějakém kontextu vhodné, může používat i uvedený opisný výraz, to chyba není. Ovšem pozor! V zájmu jasného sdělení se musí tento opis uvádět celý. Pokud se zkrátí pouze na slovo kódování, tak se téměř vytrácí smysl sdělení, neboť přestává být jasné, o jaké kódování se tu vlastně jedná. Je to asi taková informace, jako kdyby vám na otázku: „Jaký typ počítače máte?“ přišla odpověď: „Elektrický přece!“. Mělo by tedy patřit k jisté vyšší etice oboru, že se vystříháme prostých a nic neříkajících slov kód a kódování, pokud budeme mít na mysli pojmy šifra a šifrování. Důležitým prvkem v šifrování (a v řadě ostatních kryptografických metod), díky kterému se diametrálně odlišuje od ostatních kódovacích předpisů, je, že používá nějakou tajnou doplňkovou informaci, kterou nazýváme šifrovací klíč. Pomocí klíče se pak u šifer zajišťuje důvěrnost (utajení zpráv, souborů dat), u jiných kryptografických technik pak i jiné vlastnosti, jako například autentizace uživatele (v počítačové síti, v síti GSM apod.), autentizace původu dat (elektronický podpis, „nepadělatelné“ zabezpečovací kódy), nepopiratelnost nějakého aktu apod.

Šifry jsou zbraně

Kryptologie byla až do počátku počítačové revoluce záležitostí tajných služeb a vojáků. Poté našla komerční uplatnění a z původní vojenské kontroly se vymkla. Kvalitní šifry jsou však považovány z hlediska práva za zboží dvojího použití a patří do podobných kategorií jako tanky a řízené střely. Donedávna se k nám nesměly kvalitní šifry dovážet, nyní naopak musíme dodržovat Wassenaarskou dohodu při jejich vývozu. Uvedená opatření jsou naprosto logická, neboť schopní kryptoanalytici dokázali ve všech světových válkách ovlivnit jejich průběh tím, že luštili šifrovanou komunikaci nepřítele. Kvalitní šifry naproti tomu dokázaly nepřátelské odposlechové systémy vyřadit z boje, neboť zachycené šifrované zprávy byly protivníkovi k ničemu. Nekvalitní šifra je ovšem horší než žádná, protože poskytuje pocit bezpečí, který je falešný.

Čím se budeme dále zabývat

V následujících příspěvcích se postupně seznámíme s pojmy symetrická kryptografie a asymetrická kryptografie (kryptosystémy s veřejným klíčem pro výměnu klíčů, dohodu na klíči a pro digitální podpis, RSA, El Gamal, DSA aj.), blokovými a proudovými šiframi, hašovacími funkcemi (MD, SHA), generátory náhodných a pseudonáhodných čísel (RNG, PRNG), kryptografickými kontrolními součty (MAC, HMAC), operačními módy šifer a nejznámějšími standardy, protokoly a prostředky (SSL/TLS, S/MIME, PGP aj.).

Vlastimil Klíma, Tomáš Rosa,
vlastimil.klima@i.cz, tomas.rosa@i.cz

LITERATURA

[1] Přednášky o kryptologii na MFFUK <http://adela.karlin.mff.cuni.cz/~tuma/ciphers.html>

[2] Odposlechový systém Echelon <http://archive.aclu.org/echelonwatch/resources.html>

[3] Archiv článků o kryptologii a bezpečnosti <http://www.decros.cz/bezpecnost/_kryptografie.html>

[4] Simon Singh: Kniha kódů a šifer. Tajná komunikace od starého Egypta po kvantovou kryptografii, Dokořán, 2003, <www.dokoran.cz>