Kryptologie pro praxi

V *ST 6* [1] jsme si vysvětlili rozdíl mezi šifrováním a kódováním. Tou základní vlastností šifrovacích metod, které používáme k utajení informace, je existence nějakého tajného prvku, který nazýváme klíč. Klíč je centrem pozornosti všech kryptografických metod. Kryptografové uvažují na základě historických zkušeností velmi logicky – útočník se může dostat k šifrovacím zařízením, programům a veškerým popisům systému. Neměl by se ovšem dostat ke klíčům, jejichž ochraně je věnována mimořádná pozornost. Na předpokladu, že útočník nezná tajný klíč, je potom kryptografickými metodami vystavěna řada metod pro ochranu dat, zajištění jejich integrity, vlastnosti nepopiratelnosti apod.

Symetrická a asymetrická kryptografie

V klasických (symetrických) metodách kryptografie používají odesílatel i příjemce stejný tajný klíč, který si musí před vlastní komunikací nejprve vyměnit nějakým bezpečným kanálem. Průvodním jevem symetrických kryptosystémů je proto nárůst počtu těchto klíčů v případě vzájemné komunikace více lidí. Problémy výměny klíčů a vůbec vším, co se týká klíčů, (tj. generováním, distribucí, zálohováním, ničením klíčů apod.), se zabývá klíčové hospodářství. V roce 1976 byla uvedena ve známost kryptografie s veřejným klíčem, která přišla s myšlenkou, že šifrovací klíč pro zašifrování může být veřejný, a že je důležité jen to, aby dešifrovací klíč byl utajený (privátní klíč). V důsledku této asymetrie na straně odesilatele a příjemce se celá oblast nazývá asymetrickou kryptografií. Jestliže klíč pro zašifrování je veřejný, není nutné si ho vyměňovat před komunikací. Vzniká ovšem otázka, zda opravdu patří veřejný klíč, který používáme k zašifrování zprávy, zamýšlenému příjemci nebo byl podvržen. K řešení tohoto problému vznikly certifikační autority a celá oblast, které se říká infrastruktura veřejných klíčů (PKI). Protože asymetrické šifry jsou ve srovnání se symetrickými pomalé, k šifrování vlastních dat se používají symetrické šifry. Jejich klíč je generován většinou náhodně a k jeho přenosu příjemci ho odesílatel zašifruje asymetrickou šifrou (veřejným klíčem příjemce). Kromě toho se asymetrické mechanismy využívají k digitálním podpisům, kde se využívá asymetrie tak, že podpis může ověřit kdokoli veřejným klíčem, zatímco vytvořit ho je schopen pouze vlastník privátního klíče.

Generátory náhodných znaků

Ke generování symetrických klíčů i asymetrických párů i pro další účely se v kryptografii běžně využívá vhodný generátor náhodných znaků (RNG). V praxi není jednoduché sestrojit kvalitní generátor. Tam, kde nejsou k dispozici hardwarové generátory, se používají různé softwarové náhražky. V těchto případech jde nejprve o získání řetězce bitů (nazýváme ho seed – semínko) s co největší entropií (obvykle 80–256 bitů). Poté se kryptografickými metodami (například viz dále popsané hašovací funkce nebo blokové a proudové šifry) z tohoto semínka vygeneruje kvalitní pseudonáhodná posloupnost, kterou nelze predikovat ani ze znalosti předchozí produkce. Jako zdroj semínka by se však neměly používat tak chudé zdroje na entropii, jako je systémový čas, různá sériová čísla apod., spíše bychom měli používat fyzikálně zaměřené a těžko predikovatelné veličiny, protože bezpečnost celé posloupnosti podstatně závisí na kvalitě jejího seedu.

Proudové šifry

Proudové šifry zpracovávají vstupní otevřený text po znacích (bit po bitu, bajt po bajtu) a k tomu používají tzv. heslo (zde to není přihlašovací heslo, ale historicky vžitý pojem v oblasti proudových šifer), které může být vytvořeno zcela náhodně, nezávisle a s rovnoměrným rozdělením znaků (Vernamova šifra), nebo může být vygenerováno deterministicky (moderní proudové šifry) na základě šifrovacího klíče. Známá je například Vigenerova šifra, kde se heslo tvoří periodickým opakováním klíče (EVAEVAEVA... atd.). Přestože je luštitelná, často je v počítačové praxi používána. Šifrový text ($\check{S}T$) vzniká slučováním jednotlivých znaků otevřeného textu (OT) a hesla (H), a to nejčastěji operací *xor* ($\oplus$), tj. $\check{S}T=OT\oplus H$. Odšifrovává se podobně: $OT=\check{S}T\oplus H$. Je možné dokázat, že Vernamova šifra je nerozluštitelná, pokud se její heslo použije k šifrování pouze jednou. Pokud se ale tentýž proud hesla použije k šifrování dvou různých otevřených textů, stačí jejich příslušné šifrové texty přetransformovat funkcí *xor*, heslo vypadne a oba dva otevřené texty se náhle octnou v přímém ohrožení. Místo transportu hesla na obě dvě strany komunikačního kanálu (v praxi se například pro diplomatické spojení rozvážely děrné pásky a později jiná paměťová média s heslem) se v počítačové praxi pro generování hesla používají proudové šifry a distribuují se pouze klíče pro jejich nastavení. Aby bylo pokaždé generováno jiné heslo a klíč nemusel být měněn, zavedl se princip inicializační hodnoty (IV). Na každou zprávu se generuje náhodně a přenáší se šifrovaným textem. Nastavuje příslušný algoritmus vždy do jiného počátečního stavu, přičemž utajenost generovaného hesla garantuje klíč. Tato technika se s malou obměnou využívá i u blokových šifer.

Blokové šifry

Blokové šifry na rozdíl od proudových zašifrují najednou vždy celý blok B bitů, například B=64 u algoritmu *DES* nebo B=128 u standardu *AES*. Šifrový text se vypočítá jako $\check{S}T=E_K(OT)$, kde K je klíč, E operace zašifrování (encryption) a OT je blok otevřeného textu. Zpětně pak $OT=D_K(\check{S}T)$, kde D označuje operaci odšifrování (decryption). Blokové šifry jsou konstruovány tak, že při neznalosti klíče K se jeví jako náhodné zobrazení z množiny $\{0,1\}^B$ na množinu $\{0,1\}^B$. Útočníkovi proto ani nestačí znalost mnoha odšifrovaných zpráv k tomu, aby mohl cokoli říci o chování šifry na novém otevřeném nebo šifrovém bloku.

Hašovací funkce

Hašovací funkce (h) se používají velmi hojně v celé kryptografii, ale klíčovou roli sehrávají pro digitální podpisy. Zpracovávají libovolně dlouhý vstup m na hašový kód (haš) $h(m)$ pevné délky, například 160 bitů u nejpoužívanější hašovací funkce h=*SHA*–1 nebo 256 bitů u nové funkce *SHA*–256. Hašovací funkce musí být jednocestná a bezkolizní. Jednocestnost znamená, že z m lze $h(m)$ vypočítat jednoduše, ale naopak to není výpočetně zvládnutelné. Bezkolizní požaduje, aby výpočetně nezvládnutelné bylo i nalezení jakýchkoliv dvou různých zpráv se stejným hašovým kódem (to nazýváme kolizí). Bezkolizní umožňuje místo (objemné) zprávy m podepisovat pouze její haš $h(m)$, tj. řádově stovky bitů. Haš vlastně identifikuje zprávu m, nebo se lze přesvědčit, že vede na hašový kód $h(m)$ a současně není možné najít jinou zprávu se stejnou identifikací (haší). Využíváme faktu, že i když teoreticky víme že existují, nelze se k nim standardním způsobem dopracovat. Na jednocestnosti hašovacích funkcí je založena řada kryptografických technik, o nichž si povíme v příštích číslech *ST*.

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

LITERATURA

[1] Kryptologie pro praxi, Sdělovací technika č. 6, 2003, s. 19

[2] Simon Singh: Kniha kódů a šifer. Tajná komunikace od starého Egypta po kvantovou kryptografii, Dokořán, 2003,

[3] Vybrané aspekty moderní kryptoanalýzy, Sdělovací technika č. 3, 2003, s. 3–7

[4] http://adela.karlin.mff.cuni.cz/

[5] http://www.decros.cz/bezpecnost/kryptologie.html