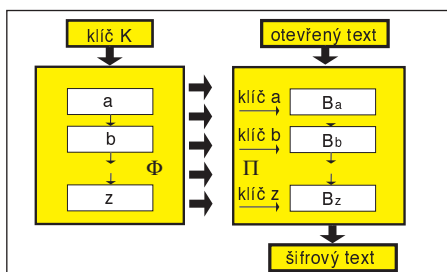
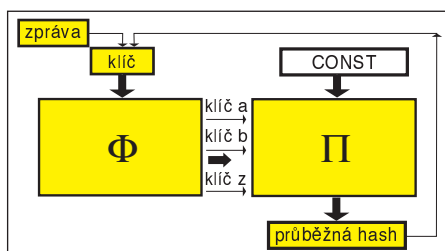


# Speciální blokové šifry a hašovací funkce

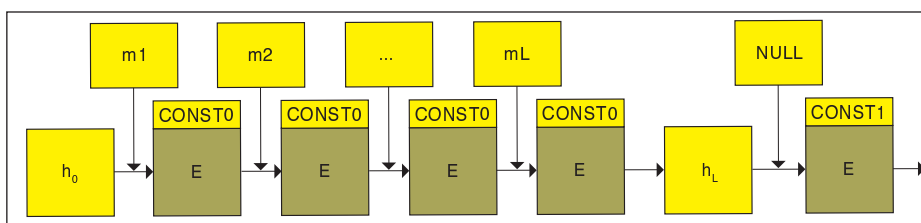
V tomto článku se seznámíme s tzv. speciální blokovou šifrou a hašovací funkcí. Uživatelé chtějí mít všechny možné informace a služby všude a hned, což stimuluje rozvoj informačních a komunikačních technologií, ale i zvyšuje objem a rychlost přenosu dat. Tím se musí rychle inovovat informační a komunikační technologie. Nutí to také kryptology navrhovat stále rychlejší kryptografické nástroje, aby nezpomalovaly toky dat. Přitom se snadno zapomíná na to, že většina těchto nástrojů má nedokazatelnou bezpečnost (a nikdo to nemůže změnit). Proto je zcela normální (a nikoli senzaci), že čas od času je některá tato technika prolomena nebo je odhalena nějaká její slabina



Obr. 1 Speciální bloková šifra



Obr. 3 Použití speciální blokové šifry ve speciální hašovací funkci



Obr. 2 Speciální hašovací funkce

nebo je prostě ukázáno, že nemá takovou odolnost, pro jakou byla vytvořena. V některých sektorech (stát) je však nutné, aby bezpečnost byla zajištěna vždy.

## Kryptografická bezpečnost není samozřejmostí

V letech 2004–2006 došlo k prolomení hašovací funkce MD5 a oslabení SHA-1 a byly ukázány (teoretické, generické) nedostatky konstrukce SHA-2. Na základě toho vzniklo celosvětové úsilí zaměřené k nalezení nových teoretických východisek. I u nás NBÚ vypsal projekty k řešení této situace. Na základě toho vznikly tzv. speciální blokové šifry DN a speciální hašovací funkce HDN. Hlavním cílem bylo navrhnout funkci, která bude mít vysokou bezpečnost, založenou na prokazatelných tvrzeních, ale současně reálně použitelnou. Z časového hlediska vznikly nejprve teoretické koncepty speciálních vnořených autentizačních kódů (SNMAC) a spe-

ciálních blokových šifer (SBŠ). V druhé fázi byla navržena konkrétní speciální bloková šifra DN a na její bázi hašovací funkce HDN. V době zadání projektu takové funkce nebyly známy a do současnosti není známo mnoho jiných alternativ. NBÚ z tohoto důvodu dokonce umožnil jejich publikování. A na základě toho také vznikl dodatečný výzkum (konstrukce sítí DN).

## Bloková šifra i hašovací funkce je v ČR k dispozici

Současný stav je tedy takový, že vývojáři (nejen, ale zejména) v ČR mají k dispozici dokonce určitou stavebnici, ze které mohou vytvořit (zodolněnou, speciální) blokovou

## Speciální hašovací funkce

Speciální hašovací funkce vychází z konstrukce SNMAC zvláštním využitím (speciální) blokové šifry. Toto využití je vidět z obrázku. Klasické konstrukce využívající blokovou šifru k hašování vedou zprávu a průběžnou haš (různým způsobem) do dvou vstupů – na vstup otevřeného textu a do klíče. Speciální hašovací funkce oba vstupy řetězí a vede je do klíče, zatímco otevřený text zůstává konstantní. Tato jednoduchá myšlenka zabraňuje všem hrozivým současným diferenciálním útokům na hašovací funkce jednoduše proto, že s otevřeným textem nelze manipulovat neboť je konstantní. Odtud také název „speciální bloková šifra“, neboť v hašovací funkci je použita jen se dvěma otevřenými texty (Const0 a Const1).

## Speciální šifrování

Možnost využít speciální blokovou šifru i pro šifrování je přirozená. V takovém případě přivádíme do blokové šifry  $\Pi$  proměnný otevřený text. Tato bloková šifra má však neobvykle kvalitní zpracování klíče (blokovou šifrou  $\Phi$ ), neboť soudobé blokové šifry používají namísto ní jednoduchou transformaci.

## Stavebnice

Všechny uvedené funkce jsou ve skutečnosti stavebnicového typu, neboť neomezuji konkrétní náplň jednotlivých bloků. Pouze vyžadují určité jejich vlastnosti a dávají možnost vybrat z nekonečně mnoha variant. Pochopitelně, že za takto zvýšenou bezpečnost uvedených nástrojů se platí snížením rychlosti. Proto také tyto nástroje nebudou vhodné pro ultrarychlé přenosy, ale spíše tam, kde jde o vysokou záruku bezpečnosti. Vhodnou volbou variantních náplní jednotlivých prvků lze však rychlost dosti optimalizovat. Strukturovaný design umožňuje realizovat tyto funkce jednoduše i v HW, kde lze dosahovat i gigabitových rychlostí.

## Závěr

V tomto článku jsme chtěli vývojáře upozornit na existenci volně dostupných nástrojů pro potřeby kvalitního šifrování i hašování. Vzhledem k tomu, že všechny tři uvedené koncepty byly široce publikovány, každý z nich má svoji samostatnou internetovou stránku s literaturou a dalšími zdroji na [1].

Vlastimil Klíma,

nezávislý kryptolog, v.klima@volny.cz

LITERATURA

[1] <http://cryptography.hyperlink.cz>