# Kryptologie pro praxi – nejpoužívanější šifry

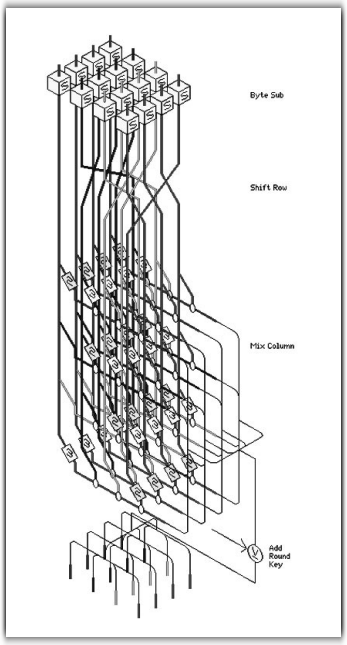
V ST 9 [1] jsme poznali několik možností, jak lze používat blokové šifry k šifrování dat. V tomto článku se budeme zabývat ve světě nejpoužívanějšími symetrickými blokovými šiframi. Jedná se o DES, TripleDES a AES.

## Současné blokové šifry

Víme, že narozdíl od proudových šifer, blokové šifry zašifrují nebo dešifrují najednou celý blok vstupního textu. Staré standardy v čele s DES a TripleDES používaly blok o délce 64 bitů, nové standardy v čele s AES používají a budou používat blok 128 bitový. Zašifrování bloku zapisujeme symbolicky jako $\check{S}T=E_K(OT)$, kde $K$ je šifrovací klíč, $OT$ otevřený text a $\check{S}T$ šifrový text, a odšifrování jako $OT=D_K(\check{S}T)$. Délka klíče bývala dříve u šifer povolena malá, což umožňovalo jejich luštění hrubou silou, zejména u variant těchto šifer pro vývoz. Také k nám se ještě před několika lety dovážely americké šifry pouze se 40bitovým klíčem. Plnohodnotný standard DES měl přitom pouze 56bitový klíč. V současné době patří k dobrému bontonu používat klíč minimálně 80bitový s tím, že by se spíše měla nabízet délka 128 bitů a výše. AES podporuje tři délky klíče: 128, 192 a 256 bitů. Tyto délky zaručují, že nebude možné využít útoku hrubou silou, neboť zásadní praktické problémy s konstrukcí a cenou lušticího stroje začínají už u 80 bitů. Klíče o 128 bitech a výše pak zaručují utajení minimálně na několik desítek let dopředu. Dodejme zde ovšem, že délka klíče je nutná, leč nikoliv postačující podmínka bezpečnosti. Velmi záleží také na konkrétním šifrovacím algoritmu, který musí zaručit, že metoda zkoušení všech možných klíčů hrubou silou je skutečně jediný možný způsob útoku. Z praxe je známa řada případů, kde díky slabému algoritmu nebyly ani klíče délky 128 bitů nic platné.

## Bloková šifra jako black box

Při využití blokových šifer návrháře informačních systémů většinou nezajímá, jak vypadají uvnitř, a používají je jako černou krabičku, transformující vstup na výstup, přičemž tuto transformaci na počátku pouze nastaví příslušným šifrovacím nebo dešifrovacím klíčem. Občas se ovšem na šifrách najdou nějaké chyby, a je dobré o nich vědět, aby využití objevených slabin nebylo možné. Bloková šifra se musí chovat na jednu stranu deterministicky, na druhou stranu jako náhodné zobrazení, pokud pozorovatel nezná její klíč. Vymyká se trochu našim představám požadavek, že i když luštitel bude mít k dispozici prakticky neomezené množství dvojic ($OT$, $\check{S}T$) pro otevřené texty jaké požaduje, nesmí mu tato znalost dát žádnou použitelnou informaci o otevřeném textu příslušejícímu jakémukoliv novému textu šifrovému. Dále se jak klíč, tak otevřený text, musí do šifrového textu promítat složitě, ale přesto „rovnoměrně“ tak, aby závislost $\check{S}T$ na klíči a $OT$ nešlo vyjádřit jednoduše nebo v ní nalézt nějakou anomálii, jako byly např. nalezeny u transformace DES (komplementárnost, slabé a poloslabé klíče). Rostoucí shopnosti kryptoanalýzy vyžadují pozornost i při tvorbě klíčů.




**Obr. 1 Ilustrace jednoho cyklu šifrování v AES**

## Transformace Data Encryption Standard

Nejpoužívanější šifrou na světě byla až donedávna DES (Data Encryption Standard). Vznikla na základě veřejné soutěže v USA a poté od roku 1977 platila jako šifrovací standard, určený pro ochranu citlivých neutajovaných dat ve státní správě. Díky tomu se stala de facto celosvětovým standardem a byla (a často ještě je) součástí mnoha průmyslových, internetových a bankovních standardů (např. ANSI standard X9.32.). Avšak už v roce 1977 bylo upozorňováno na příliš krátký klíč 56 bitů, který byl do původního návrhu IBM zanesen vlivem americké tajné služby NSA. Občas se setkáme i s tím, že se klíč pro DES uvádí jako 64bitový. V takovém případě se vždy nejnižší bit v bajtu považuje za lichou paritu od horních sedmi bitů. Do algoritmu jako takového ale vstupuje pouze 56 bitů. DES se také stala předmětem intenzivního výzkumu a útoků a byly objeveny některé její negativní vlastnosti. Jedná se například o tzv. slabé a poloslabé klíče, vlastnost komplementárnosti a později i teoreticky úspěšnou lineární a diferenciální kryptoanalýzu. Existují 4 slabé klíče, pro něž DES nešifruje, tj. pro každé takové $K$ a každé $OT$ platí $OT=E_K(OT)$. Dále existuje šest dvojic poloslabých klíčů ($K_1$, $K_2$), pro něž platí $OT=E_{K2}(E_{K1}(OT))$, pro všechna $OT$. Vlastnost komplementárnosti pak umožňuje přes DES protlačit lineární změny takto: pro každé $K$ a $OT$ platí $E_K(OT)=\mathrm{non}(E_{\mathrm{non}K}(\mathrm{non}OT))$. Jedinou zásadní praktickou nevýhodou byl však pouze krátký klíč. Aby se ilustrovala možnost sestrojení lušticího stroje, byl skutečně v roce 1998 postaven DES-Cracker [2]. Principiálně jednoduchý stroj v ceně asi čtvrt milionu dolarů je schopen vyzkoušet všechny možné klíče DES na daném šifrovém textu. Obsahuje 29 desek, každá z nich má 64 čipů, které zkouší klíče z různých částí klíčového prostoru. Celkem se dosahuje rychlosti 90 miliard zkoušek klíčů za sekundu, což umožňuje prohledat celý klíčový prostor v garantované době 9 dní. Naposledy byl DES-Cracker nasazen v rámci soutěže DES-Challenge III, kdy nalezl klíč DES za 22 hodin. Další zajímavosti o něm a kompletní technický popis můžete nalézt na [2]. Nejen kvůli sestrojení DES-Crackeru byla platnost DES jako standardu ukončena až na výjimky (může být používán jen v dobíhajících systémech a kvůli kompatibilitě) a místo něj byl přijat TripleDES, definovaný normou FIPS 46-3. Od 26. května 2002 je pak už v platnosti standard nové generace, AES.

## TripleDES

TripleDES používá DES jako stavební prvek celkem třikrát s dvěma nebo třemi různými klíči. Nejčastěji se používá varianta této šifry (EDE), která je definována ve standardu FIPS PUB 46-3 a v bankovní normě X9.52, kdy vstupní $OT$ je zašifrován podle vztahu $\check{S}T=E_{K3}(D_{K2}(E_{K1}(\mathrm{OT})))$, kde $K_1$, $K_2$ a $K_3$ jsou buď tři nezávislé klíče nebo $K_3=K_1$. Klíč je tedy dlouhý buď 112 bitů nebo 168 bitů. Varianta EDE umožňuje kompatibilitu s DES, pokud zvolíme všechny tři klíče shodné. TripleDES (označovaná často 3DES) se považuje za spolehlivou, pokud se předchází uvedeným teoretickým slabinám (komplementárnost, slabé klíče). Je možné ji používat, stejně jako jakoukoliv jinou blokovou šifru, v různých operačních modech, například CBC (označení takové šifry je pak 3DES-EDE-CBC), jak jsme o nich psali v [1]. Známou modifikací DES je DESX od firmy RSA Security. Má klíč o délce 128 bitů, přičemž jeho první polovina je naxorována na otevřený text před průchodem DES a druhá je použita jako vlastní klíč DES. Na výstup z DES je na závěr ještě naxorována další hodnota, odvozená z původních 128 bitů klíče.

### Ostatní blokové šifry

Dalšími často používanými šiframi jsou 64bitové blokové šifry CAST, IDEA, RC2 a Blowfish. Existuje jich ještě celá řada a všechny měly společný cíl nabídnout bezpečnou alternativu k DES v době, kdy ještě nebyl k dispozici AES a šifrování pomocí TripleDES bylo pomalé. Lze očekávat, že tyto šifry budou ještě dlouho používány, ale postupně je AES vytlačí, zejména v nových systémech. Tento přechod není snadný ze systémového hlediska, neboť se musí přepracovat datové struktury, které byly ve všech systémech po dobu 25 let (často pevně) svázány s délkou bloku 64 bitů a s jedním klíčem (AES podporuje tři délky klíčů). Vývoj se samozřejmě nezastaví a požadavky na zabezpečenost se budou spojitě zvyšovat.

### Šifrování AES (Rijndael)

Výběrové řízení na Advanced Encryption Standard (AES) bylo americkým úřadem pro standardizaci NIST vypsáno 2. 1. 1997 a přihlásilo se 15 kandidátů. Nakonec byl z pěti finalistů vybrán algoritmus Rijndael a jako AES byl přijat s účinností od 26. května 2002, – viz oficiální publikace FIPS PUB 197 [3]. AES *(obr. 1)* má blok délky 128 bitů a podporuje tři délky klíče: 128, 192 a 256 bitů. V závislosti na tom se částečně mění algoritmus – tzv. počet rund (cyklů, v nichž je zpracováván otevřený text), který je po řadě 10, 12 a 14. Větší délka bloku a delší klíče zabraňují mnoha útokům, které byly aplikovatelné na DES a jiné blokové šifry. Zdrojové kódy naleznete např. na [5], další informace jsou na domovské stránce AES na [3], včetně vědeckých pracích, matematického popisu a dalších vlastností. Očekává se, že AES bude platným šifrovacím standardem minimálně 10–15 let, ale spíše několik desetiletí a že se časem stane převládající šifrou ve světě.

Vlastimil Klíma, Tomáš Rosa,
v.klima@volny.cz, t_rosa@volny.cz

*LITERATURA*

*[1] Kryptologie pro praxi (4), Sdělovací technika č. 9, 2003*

*[2] Stránka DES-Crackeru: http://www.eff.org/des-cracker/.*

*[3] Normy FIPS-PUB (DES, TripleDES, AES) naleznete na webu NIST: http://csrc.nist.gov/encryption/*

*[4] Archivy autorů, kde naleznete české články na téma kryptografie a bezpečnost http://cryptography.hyperlink.cz a http://crypto.hyperlink.cz*

*[5] Zdrojové kódy šifer: ftp://ftp.funet.fi/pub/crypt/cryptography/*