MODERNÍ KRYPTOGRAFICKÉ METODY

Šifry s mnoha tvářemi

Tento volný seriál jsme v minulém čísle zahájili základními pojmy. V tomto dílu si ukážeme možné způsoby využití proudových a blokových šifer (tzv. mody jejich činnosti), úlohu inicializačního vektoru, metodu „solení“ a další techniky. Uvidíme také, co šifrování přináší pro bezpečí informačních systémů, a zamyslíme se nad úlohou šifrovacích klíčů.

PROUDOVÉ ŠIFRY

Začneme s proudovými šiframi. Víme, že zpracovávají otevřený text bit po bitu nebo bajt po bajtu s odpovídajícím proudem tzv. hesla *(running key, key stream)*, a to většinou operací XOR. Heslo je v tomto případě něco jiného než přihlašovací heslo. Je to ve skutečnosti klíčový materiál, který je sám o sobě přímo šifrovacím klíčem (Vernamova šifra) nebo je z šifrovacího klíče odvozován (obecné proudové šifry).

VERNAMOVA ŠIFRA

Mezi nejznámější proudové šifry patří *Vernamova šifra*. Jméno dostala po svém vynálezci, zaměstnanci AT&T, který s ní přišel už v roce 1917. Každý bit otevřeného textu se šifruje odpovídajícím bitem hesla pomocí operace XOR. Heslo existuje ve dvou exemplářích a dopravuje se na obě strany komunikačního kanálu. Nazývá se zde **jednorázové** *(one-time pad)* – a hned uvidíme proč. Aby totiž šifrování bylo bezpečné, musí mít heslo následující vlastnosti:

1. je stejně dlouhé jako otevřený text;
2. smí se použít k šifrování jen jednoho otevřeného textu (odtud název „jednorázové“);
3. všechny bity hesla musí být nezávislé náhodné veličiny se stejnou pravděpodobností výskytu nuly a jedničky: $p(0) = p(1) = 1/2$.

Jsou-li uvedené podmínky splněny, je tento šifrovací algoritmus z informačně-teoretického hlediska absolutně bezpečný. Z hlediska terminologie je v tomto případě šifrovacím klíčem celé jednorázové heslo.

V moderních počítačových systémech je ovšem Vernamův systém naprosto nevyužitelný, neboť nelze organizačně splnit druhou a třetí podmínku. Pro svoji bezpečnost se Vernamova šifra kdysi používala k šifrování diplomatických spojů, kurýři ale museli do zahraničí vozit kufry děrných pásek s jednorázovým heslem, což si v moderních počítačových systémech bohužel dovolit nemůžeme...

MODERNÍ PROUDOVÉ ŠIFRY

Je tu ale jiná cesta. Namísto distribuce velkého objemu hesla na obě komunikující strany můžeme využít šifrovací postupy, které generují libovolně dlouhé heslo určitým algoritmem, přičemž pro své nastavení využívají relativně krátký šifrovací klíč (např. 80 nebo 128 bitů). Tajným prvkem systému pak není celé heslo, ale jen šifrovací klíč.

INICIALIZAČNÍ VEKTOR

Pokud se klíč nezmění, algoritmus generuje, je-li restartován při šifrování nového otevřeného textu, stále totéž heslo. To je ovšem nežádoucí, protože toto tzv. dvojí použití hesla by mohlo vést k rozluštění obou otevřených textů. Aby se k šifrování nemusel používat pokaždé nový šifrovací klíč, zavádí se tzv. *inicializační vektor* (IV). Je to veřejná hodnota, která se většinou předává před šifrovanými daty v otevřené podobě. Pomocí IV, který se generuje většinou náhodně, se pak šifrovací algoritmus při šifrování nových dat nastaví i při stejném klíči vždy do nové výchozí pozice a vygeneruje potřebný objem nového hesla. Odpadá tak nutnost měnit šifrovací klíč a mění se jen IV.

Šifrovací klíče se zpravidla ukládají **do různých fyzických předmětů** – pak stačí **pamatovat si** jen příslušné **přístupové heslo** nebo **PIN**.

SOLENÍ

Koncept inicializačního vektoru byl později obohacen o myšlenku tzv. *solení*. Spočívá v tom, že IV se sice uvede v otevřeném tvaru před vlastními šifrovanými daty, ale pro posílení bezpečnosti se jako skutečný IV použije hodnota $IV_{SALT} = f(IV, K)$,

kde K je šifrovací klíč a f je vhodná hašovací funkce (pojem hašovací funkce viz infotipy). Cílů tohoto opatření je více, hlavním z nich je však skrýt skutečně použitý IV_{SALT}. Vše vidíte na obrázku 1.

Z proudových šifer jsme už v Chipu psali o A5 nebo RC4 (viz infotipy). U A5, která se používá pro šifrování v komunikaci telefonu GSM s bázovou stanicí sítě, je inicializační hodnota tvořena (veřejným) číslem přenášeného datového rámce. Naproti tomu šifra RC4 techniku IV ani solení nepoužívá, a proto na každé spojení generuje šifrovací klíč znovu (náhodně). Komunikujícímu protějšku ho potom musí předat jiným bezpečným způsobem (většinou prostřednictvím asymetrické šifry).

Obr. 1: Vernamova šifra a proudové šifry

Blokové šifry v proudovém modu

Blokové šifry se dají použít nejen v modu ECB *(Electronic Code Book)*, se kterým jsme se seznámili minule, ale i dalšími způsoby. U modu ECB se najednou zpracoval jeden blok (např. 64 bitů) otevřeného textu. Dalšími, tentokráte proudovými mody jsou OFB *(Output Feedback)* a CFB *(Cipher Feedback)*, viz obr. 2. Při nich může blokový algoritmus šifrovat proud dat (nezarovnaný na bloky) stejně jako proudová šifra.

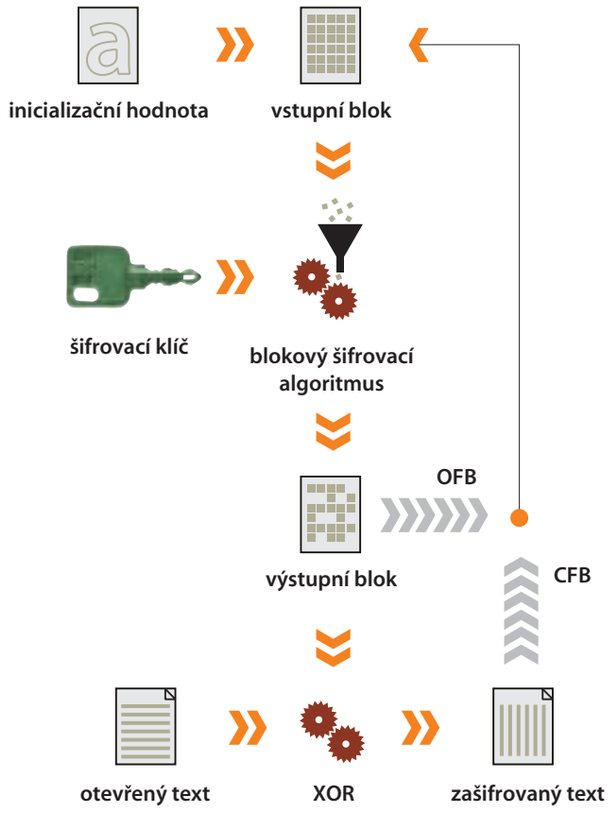
I zde se používá inicializační vektor IV, který nastaví blokovou šifru vždy do jiné počáteční pozice. Z této pozice se vygeneruje první blok hesla (právě zašifrováním IV). Vytvořené heslo se použije klasicky jako u proudové šifry – XOR na otevřený text. Klíčovou myšlenkou zde je, že právě vzniklý blok hesla nebo šifrového textu je náhodný, a dá se proto využít jako nový vstup do blokové šifry. Zašifrováním tohoto vstupu se vygeneruje další blok hesla, který se „xoruje“ na druhý blok otevřeného textu, atd. U posledního (eventuálně neúplného) bloku otevřeného textu se z připraveného plného bloku hesla použije jen tolik bitů, kolik je potřeba. Tímto jednoduchým způsobem jsme tedy blokovou šifru změnili na šifru proudovou. Podobně jako u proudových šifer i zde se může využít metoda solení IV.

Podle toho, zda zpětnou vazbu vedeme z výstupu (hesla), nebo ze zašifrovaného textu, příslušný režim se označuje jako modus *zpětné vazby z výstupu* (OFB), nebo modus *zpětné vazby ze zašifrovaného textu* (CFB). Tyto postupy vznikly pro potřebu šifrování proudu *k*-bitových znaků (většinou šesti- nebo sedmibitových); odtud už nebylo daleko k nápadu z celého 64bitového bloku generovaného hesla využít v modu OFB k šifrování jen *k* bitů. Oněch *k* bitů hesla se pak vede zprava do vstupního registru blokové šifry a posouvá původní obsah o *k* bitů doleva.

Později se zjistilo, že pokud není *k* rovno plné délce bloku, vznikají nežádoucí krátké cykly ve struktuře produkovaného hesla (místo očekávaných průměrných cca 2^{n-1} bloků je to cca $2^{n/2}$ bloků pro n-bitové blokové šifry). Tento postup není proto pro $k < n$ tak bezpečný, pro $k = n$ je ale vše v pořádku. Poznamenejme, že například Microsoft ve svém kryptografickém jádru CSP *(Cryptographic Service Provider)* u tohoto modu používá hodnotu $k = 8$, a to dokonce bez ohledu na to, že uživatel požaduje $k = n$ a tuto hodnotu i řádně nastaví.

Nejpoužívanější je CBC

Zajímavé je, že bloková šifra se jako taková, tj. v modu ECB (viz minulý díl), používá jen velmi zřídka. Proč? Jednoduše proto, že stejné bloky



Obr. 2: Blokové šifra v proudovém modu (OFB a CFB)

Dostatečná délka klíče **je nezbytnou podmínkou bezpečnosti** i u vysoce kvalitních **šifer.**

otevřeného textu mají stejný obraz. Pokud tedy zašifrujeme nějaký soubor, ihned vidíme, kde pod zašifrovaným textem leží stejné bloky otevřeného textu – to o otevřeném textu „vyzařuje" určitou informaci, což může být nežádoucí (na druhé straně v řadě aplikací to nevadí). Aby se tomu předešlo, vznikl modus *řetězení zašifrovaného textu* – CBC (Cipher Block Chaining) a stal se také nejpoužívanějším modem blokových šifer. Jeho schéma vidíte na obrázku 3.

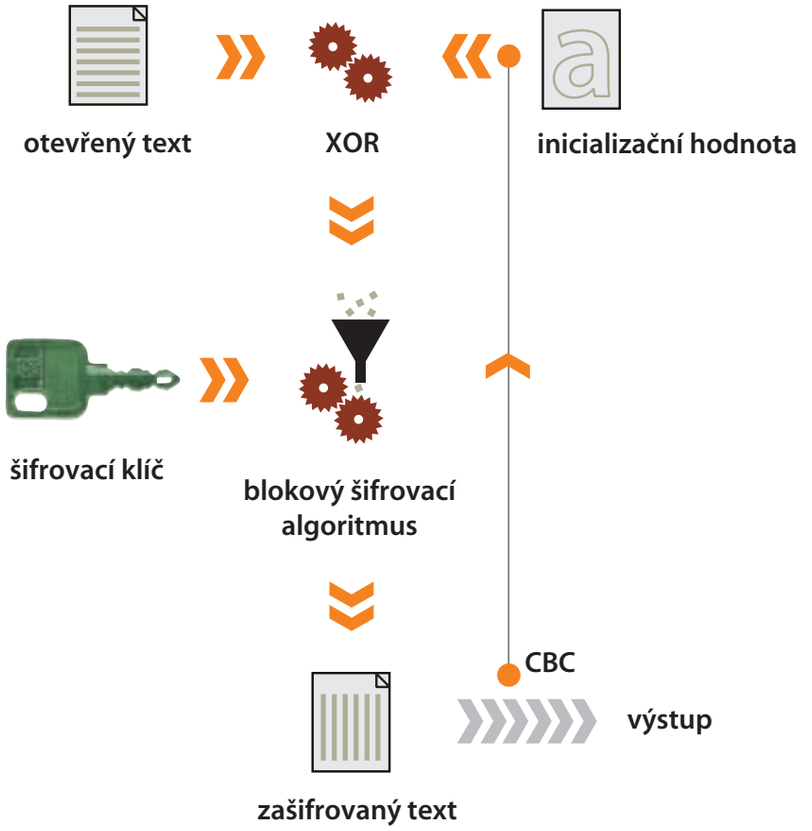
Představme si, že šifrujeme pokaždé naprosto stejný otevřený text, třeba jeden megabajt samých nul. Inicializační vektor bývá generován náhodně, a tak první blok, který jde do šifrování, je roven právě IV. Jeho obraz je vždy jiný právě z důvodu náhodnosti. Výsledný – opět náhodný a pokaždé jiný – zašifrovaný text znáhodňuje další nulový blok otevřeného textu, který také produkuje náhodný a pokaždé jiný druhý blok šifrového textu atd. Jak vidíme, i soubor samých nul bude při každém šifrování v modu CBC dávat zcela jiný (náhodný) šifrový obraz.

Další výhodou je vlastnost „samosynchronizace". Při ztrátě nějakého bloku zašifrovaného textu dešifrovací proces „nezabloudí", ale vzpamatuje se a už druhý následující blok zašifrovaného textu začne odšifrovávat správně (promyslete si způsob odšifrování). Pokud si vzpomenete na náš seriál Utajené komunikace (viz infotipy), za základ myšlenky řetězení zašifrovaného textu můžeme považovat Vigenerovu šifru z roku 1585; jeho vynález se sice nazývá autoklíč a funguje na blocích malé délky, ale smysl je velmi podobný modu CBC.

Poznamenejme ještě, že všechny čtyři uvedené mody činnosti blokových šifer jsou standardizovány a naleznete je v mezinárodních normách ISO 8372 a ISO/IEC 10116.

Dostatečně dlouhý klíč!

Jak známo, i kvalitní šifra může být znehodnocena, pokud se u ní volí krátký klíč (většina šifer umožňuje variabilní délku klíče). K délce klíče existují různé studie, které berou v úvahu různé technologie i různé odhady technologického vývoje (například Mooreův zákon). Víme také, že např. 56bitovou DES je možné luštit „hrubou silou" *(brute-force attack)*, tedy vyzkoušet všechny možné kombinace klíčů. Tuto práci umí udělat *DES-cracker*, o němž jsme už v Chipu také psali (viz infotipy).



Obr. 3: Bloková šifra v modu CBC

Připojený diagram (obr. 4) – který si nedělá nárok na jakoukoliv prognózu! – dobře ilustruje vztah délky klíče a praktických možností vyluštění šifry. Ukazuje totiž, kolik by teoreticky stál DES-cracker, pokud by klíč k DES měl jinou délku (osa x). Je dobré si přitom uvědomit, že základní jednotka DES-crackeru umí vyzkoušet jeden klíč za jeden hodinový cyklus, z čehož vyplývá, že technologicky na něm lze zlepšovat jen taktovací kmitočet.

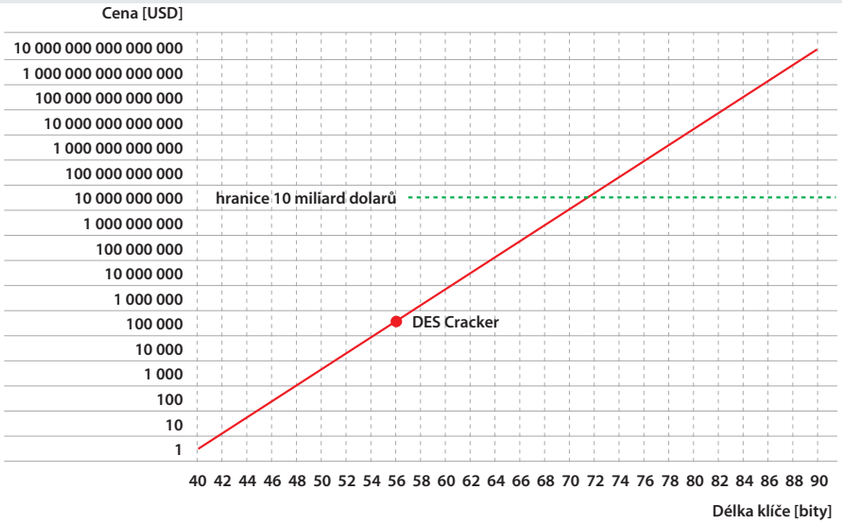
Cena použitého hardwaru v roce 1998, k němuž se graf vztahuje, byla 130 tisíc dolarů a stroj garantoval svým výkonem vyzkoušení všech 2^{56} klíčů za devět dní (pamatujme ale na Moorův zákon!). Pokud zvýšíme délku klíče o jediný bit, musíme už koupit dva DES-crackery, jinými slovy cena se zdvojnásobí. Za uvěřitelného předpokladu, že nikdo nebude chtít do luštění investovat více než 10 miliard dolarů, docházíme k důvěryhodné délce klíče cca 80 bitů (a to i tehdy, dopřejeme-li lušticímu stroji na hledání klíče nepřetržitě pět let). Poznamenejme dále, že NSA u svého algoritmu Skipjack také zvolila délku klíče 80 bitů – přičemž v komerčním světě jsou za bezpečné považovány délky klíčů 128 bitů a výše. Nově připravovaný standard AES jde ještě dále a mandatorně podporuje délky klíčů 128, 192 a 256 bitů.

Proč šifrovat

Podívejme se nyní na šifrování z aplikačního hlediska. Co nám může přinést za výhody? Jak

infotipy

Všechny použité pojmy jsou podrobně vysvětleny v následujících článcích.
Naleznete je na adrese:
▸ *www.decros.cz/Security_Division/Crypto_Research/archiv.htm*
nebo také
▸ *ftp://ftp.decros.cz/pub/Archiv/Publications/*.
Jsou zde uvedeny pod mnemotechnickým označením *časopis-rok-měsíc-strana(od)-strana(do).ext:*
A5 – Chip 2/00, str. 38 – 41
RC4 – Chip 9/99, str. 42 – 44
Hašovací funkce – Chip 3/99, str. 40 – 43
Vigenerova šifra – Chip 7/94, str. 138 – 141
DES-cracker – Chip 11/98, str. 74 – 75



Obr. 4: Cena lušticího stroje v závislosti na délce klíče

známo, mezi základní požadavky na bezpečnost každého informačního systému – a na internetu či v podnikových intranetech tím spíše – patří důvěrnost, integrita a dostupnost. Kryptografické metody mohou pomoci při zajištění všech těchto požadavků.

Důvěrnost: Uložená data mohou být neoprávněně prohlížena, čtena nebo ukradena, přenášená data mohou být odposlouchána. Zašifrovaná data však mohou smysluplně využít jen ti, kdož mají šifrovací klíč. Šifrování tak zajišťuje funkci důvěrnosti dat.

Integrita: Prostřednictvím kryptografických technik, jako jsou kryptografické zabezpečovací kódy, hašovací funkce, digitální podpisy apod., lze umožnit detekci neoprávněné modifikace dat.

Dostupnost: Dostupnost je třetím hlavním požadavkem na bezpečný informační systém. Nelze ji sice zcela zajistit kryptografickými prostředky, ale hodně lze pro to udělat řízeným přístupem. Dobře navržený *řízený přístup* (uživatelů k informacím) může zamezit přístupu k datům všem útočníkům i nepovolaným osobám. V řízeném přístupu hraje kryptografie zásadní roli, protože umí zajistit kvalitní autentizaci, a proto si o něm povíme více.

Řízený přístup a šifrovací klíče

V běžném životě máme klíče od těch objektů, kam máme mít právo přístupu. Jak to ale udělat u dat? V případě, že jsou šifrovaná, můžeme běžné klíče nahradit těmi šifrovacími. Každý uživatel pak může dostat ty šifrovací klíče, které chrání data, s nimiž má právo pracovat. Podle typu šifrování mohou šifrovací klíče sloužit pro přístup k zašifrovaným souborům, diskům, uživatelským nebo bankovním kontům apod. Když klíče nemáme, data jsou nám nedostupná. Šifrování tak může prostřednictvím šifrovacích klíčů elegantně zajistit funkci řízeného přístupu.

Šifrování mj. umožňuje **nahradit ochranu obrovských** objemů dat **pouze ochranou** kratičkých šifrovacích **klíčů.**

U zašifrovaných dat můžeme dále využít tyto užitečné vlastnosti:

- **Ochranu velkých objemů dat lze transformovat na ochranu šifrovacích klíčů (tedy malých objemů dat).** Například desítky gigabajtů dat na serveru mohou být šifrovány prostřednictvím 128bitového šifrovacího klíče.
- **Šifrovací klíče lze uložit do fyzických předmětů.** Fyzickými předměty mohou být čipové karty, různé tzv. tokeny, přídavný bezpečnostní HW apod.
- **Prostřednictvím různých typů šifrovacích klíčů může být řízení přístupu k datům transformováno na řízení přístupu k těmto klíčům.** Například mohou vzniknout klíče, jejichž názvy vyjadřují jejich účel: klíč organizace (všeobecný klíč pro komunikaci uvnitř organizace), klíče skupin, oddělení, klíče na projekty apod. (V řadě existujících systémů to už tak také funguje. Osobně například v denní praxi používám klíč oddělení, klíč pro komunikaci s centrálou a klíče aktuálních projektů.)
- **Šifrovací klíče mohou být bezpečně uloženy ve fyzických předmětech a řízení přístupu může být realizováno distribucí těchto předmětů.** Klíče si člověk nemusí pamatovat – pro většinu zaměstnanců ve velkých podnikových systémech je výhodné pro úschovu klíčů používat fyzický předmět a zaměstnanci si pak pamatují jen přístupové heslo nebo PIN k němu. Příkladem může být distribuce čipových karet či tokenů s asymetrickými nebo symetrickými klíči. Takové systémy jsou běžně realizovány pro šifrování elektronické pošty a digitální podpis v rozsáhlých organizacích. (Známé jsou i tokeny generující časově závislou autentizační informaci na malém displeji, které se používají pro přístup uživatelů do rozsáhlých sítí.)
- **Při distribuci šifrovacích předmětů nemusí uživatelé znát hodnoty šifrovacích klíčů, které jsou v nich uloženy (někdy je to dokonce nežádoucí). Postačí, pokud mají právo předměty s klíči používat. Je to jedinečná bezpečnostní vlastnost, výhodná pro zaměstnance i pro zaměstnavatele, pro uživatele i vydavatele těchto tokenů (vlastníků dat).** Tento přístup používá například Expandia banka pro přístup klientů k jejich účtům přes internet. Jedná se o token *(Active Card)*, který obsahuje šifrovací klíč pro autentizaci klienta a jeho příkazů, přičemž klient si volí pouze přístupový PIN k tomuto tokenu, nikoli obsažený šifrovací klíč. Na podobném principu pracují i tokeny jiných firem pro přístup zaměstnanců k podnikovým informačním systémům nebo pro přístup klientů k internetovým službám. A v podstatě tak pracují i bankovní karty (s magnetickým proužkem nebo čipem), neboť jejich vlastník nemá ani ponětí o tom, jaký klíč je spojen s jeho identitou, systém však takový klíč využívá pro ochranu nebo autentizaci jím zadaných operací.

Závěr

Kryptografie patří mezi nejúčinnější metody ochrany dat. Pro případy, kdy dojde k odcizení nosiče dat nebo odposlechu přenášených dat, není ani jiná ochrana možná. Dnes jsme se seznámili s principy používanými u proudových a blokových šifer a s některými implementačními aspekty šifrování; zaručeně však bude o čem povídat i příště...

Vlastimil Klíma
(v.klima@decros.cz)