Kapitola 9

Kryptografie

Po prostudování kapitoly budete umět:

- vysvětlit pojmy souvisejících s kryptografií;
- popsat základní kryptografické algoritmy;
- popsat blokové a proudové šifry;
- vysvětlit pojmy DES, AES, RSA;
- vysvětlit pojem elektronický podpis;
- charakterizovat dynamický biometrický podpis.

Klíčová slova:

Kryptografie, šifra, šifrový algoritmus, DES, RSA, AES, asymetrická šifra, symetrická šifra bloková šifra, elektronický podpis DBP.

9.1 Úvod

Jedním z nejdůležitějších institutů při studiu kryptografie je matematika.

Po probrání tematického okruhu posluchači budou seznámeni s pojmy používanými při řešení současné šifrové ochrany. Zároveň se seznámí s postupem při šifrování informace symetrickou a asymetrickou šifrou. Budou mít přehled o tvorbě a možnostech použití elektronického podpisu.

9.2 Kryptografie ve věku počítačů

Kryptologie nepojednává o kryptách, což se mnoho lidí stále ještě domnívá, ale řeší otázky šifer. Šifrování je proces převedením dat do takového formátu, který nemůže neoprávněná osoba jednoduše přečíst.

Než ale metody šifrové ochrany dospěly do tohoto stádia, musela kryptologie projít velmi dlouhým a složitým vývojem. Cílem tématu je ukázat hlavní mezníky při tomto vývoji, využití mechanizačních nástrojů a následky boje mezi tvůrci a luštiteli šifer. Zároveň je cílem pojednat o základních nevýhodách historických šifrových systémů a ukázat praktické využití některého e šifrových mechanismů

Moderní kryptografie využívá dvou základních směrů – symetrické a asymetrické šifrové algoritmy. Při symetrickém šifrování obě strany používají stejný tajný klíč, a to při šifrování i dešifrování zprávy. Asymetrické šifrování je postaveno na principu, kdy každý účastník vlastní veřejný a privátní klíč pro šifrování a dešifraci zprávy. U asymetrického šifrování zná odesilatel pouze veřejný klíč příjemce a jím zašifruje svou zprávu. Příjemce pak použije svůj privátní klíč pro dešifrování této zprávy. Nikdo jiný nemůže dešifrovat tuto zprávu např. použitím veřejného klíče ani nemá možnost odhalit privátní klíč příjemce. Vzhledem k výpočetní složitosti asymetrických algoritmů se nešifrují celé zprávy, ale jejich kryptografický kontrolní součet – tzv. otisk zprávy, který je vytvořen s využití kryptografické hash funkce. (v současnosti SHA 256)

S asymetrickým šifrováním je spojena nová služba v elektronickém světě – elektronický podpis. V tom případě odesilatel použije svůj privátní klíč pro „zašifrování“ - podepsání své zprávy, resp. otisku zprávy. Příjemce pak použije veřejný klíč odesilatele „dešifrování“ otisku zaslané zprávy. Jiným než veřejným klíčem odesilatele nelze úspěšně tuto kontrolu otisku provést.

9.3 Proudové, blokové šifry

Proudové šifry V tomto algoritmu se otevřený text zpracovává bit po bitu, tj. je odebrán jeden bit otevřeného textu a na něm je provedena řada operací pro generování jednoho bitu šifrového textu. Technicky jsou proudové šifry blokové šifry o bloku velikosti jednoho bitu. Při šifrování se využívá produkce generátoru pseudonáhodné posloupnosti bitů jako klíče. Aby implementace šifry měla odpovídající úroveň bezpečnosti, musí být produkce generátoru pseudonáhodné posloupnosti kvalitní. Důležité je, aby aktivace pseudonáhodného generátoru nezačínala ve stejných počátečních podmínkách, tj. produkovaný řetězec nesmí být znovu použit.

Z používaných proudových šifer lze zmínit algoritmus RC4, který patřil nejrozšířenější zejména v softwarových aplikacích. Vzhledem k tomu, že provedené studie odhalily zranitelnosti v RC4 byl tento algoritmus ze všech aplikací stažen a v současné době se již nevyužívá.

Blokové šifry jsou postaveny na šifrovacím algoritmu, který zašifruje blok dat otevřeného textu o velikosti n-bitů najednou. Obvyklé velikosti každého bloku jsou 64 bitů, 128 bitů a 256 bitů. Takže například 64bitová bloková šifra bude mít 64 bitů otevřeného textu a bude šifrována do 64 bitů šifrového textu. Otevřený text se tedy dělí do jednotlivých stejně velkých bloků. V případě blok otevřeného textu je kratší (vesměs poslední blok) je doplněn tzv. „zrním“, tj. náhodnou posloupností dat příslušné délky.

- V současné době se používají standardně blokové šifry. Některé z běžně používaných šifrovacích algoritmů, ze skupiny blokových šifer jsou algoritmy DES, Triple DES, AES, IDEA a Blowfish. Zajímavý je též algoritmus GOST 28147-89, který byl navržen pro státní orgány bývalého SSSR.

V dalších kapitolách jsou blíže uvedeny algoritmy DES a AES.

9.4 Symetrické algoritmy (registry kryptografických algoritmů)

Mezi hlavní představitele blokových šifer patří algoritmy:

- DES
- IDEA (International Data Encryption Algorithm) - (blok 64 B, klíč 128) - využití v systému PGP
- GOST 28147-89 - algoritmus pro státní orgány bývalého SSSR a
- AES (Advanced Encryption Standard) – algoritmus "Rijndael" (belgičtí autoři Rijmen a Daemen) - klíče 128, 192 a 256. – nová norma (nahrazuje DES)

Blíže se seznámíme s algoritmy DES a AES

Standard šifrování dat (DES)

V roce 1973 vláda USA v reakci na opakované požadavky od průmyslu a různých organizací dala svému ministerstvu úlohu stanovit jednotné federální normy pro automatické zpracování dat a v rámci tohoto oddělení byla odpovědnost předána Národnímu úřadu pro normalizaci (NBS). Jedním z konkrétních aspektů, které NBS považuje za vytvoření standardu pro šifrování dat.

Specifikace standardu šifrování dat zveřejněného NBS stanovila podmínky, které musí každý navržený algoritmus splňovat: že musí poskytovat vysokou úroveň zabezpečení, že bezpečnost nesmí být založena na tajnosti algoritmu, musí být ekonomická implementovat elektronicky, efektivně používat a k dispozici všem uživatelům a dodavatelům.

V rámci tohoto požadavku byl vytvořen návrh šifrového algoritmu IBM, který byl přijat a stal se "standardem šifrování dat" - DES.

Jedná se o blokovou šifru, kdy:

1. Algoritmus je navržen tak, aby šifroval bloky 64 bitů dat pod řízením 64bitového klíče (K).
2. Dva uživatelé, kteří chtějí komunikovat pomocí DES, se musí shodnout na (tajném) klíči, K.
3. U tajného klíče JC uživatelé vybírají sedm 8-bitových znaků (tj. Celkem 56 bitů) a DES pak sousedí s dalšími 8 bitovými bity parity, které jim dávají požadovaný 64bitový tajný klíč.

Postup zašifrování:

1. 64bitový blok dat je zadán jako počáteční permutace (IP).
2. 64 bitů dat je rozděleno na dva 32-bitové segmenty, vlevo (L) a vpravo (R).

3. Osmdesát osm bitů klíče K je kombinováno s nelineárním rozšířením 48bitové verze R ("expanze" se skládá z opakování 16 z 32 bitů R) a těchto 48 bity jsou pak "redukováno“ na 32bitový řetězec X.
4. L je nahrazeno R a R je nahrazen součtem (mod 2) X a L za účelem získání nového 32bitového R.
5. Kroky ad 6. a ad 7 se opakují 16krát pokaždé za použití různých 48bitových segmentů K v kroku 6.
6. 64 bitů finálového 16tého cyklu (rundy) je upraveno inverzní počáteční permutaci, tj. K (IP) -1.
7. Výsledkem je 64 bitů zašifrovaného bloku.

Postup dešifrování

8. Dešifrování se provádí pomocí šifrovací procedury v opačném pořadí stejným klíčem, K.

Při použití této šifry se musí uživatelé, kteří chtějí komunikovat pomocí DES, dohodnout na společném klíči a toto může být mezi nimi dohodnuto pomocí systému výměny klíčů Diffie-Hellman. Pokud třetí strana nezíská daný klíč, měla by být bezpečnost přeneseného textu zajištěna.

Co se týče bezpečnosti algoritmu DES – bylo provedeno mnoho statistických a dalších testů na šifrovaných datech s různými klíči pomocí DES a bylo zjištěno, že při využití současných technologií a při sdílení dílčích výsledků v distribuované síti počítačů nejsou výsledky uspokojivé. Chybí zde základní předpoklad pro kvalitní blokovou šifru, tj. změna jednoho bitu na vstupu vyvolá změnu ve všech bitech na výstupu.

Z tohoto důvodu je šifra DES nahrazena šifrou AES.

Algoritmus šifrování dat AES

Současným standardem, který byl zaveden v roce2002 jako Standard federální vlády USA, využívá algoritmus AES (Advanced Encryption Standard). Je doporučen jako spolehlivý prostředek šifrové ochrany v aplikacích zajišťujících bezpečnost zpracovávaných dat, neboť v současné době provedené studie neprokázaly u tohoto algoritmu slabiny. Jedná se o blokovou šifru s velikostí bloku 128 bitů a podporuje tři možné velikosti klíče - 128, 192 a 256 bitů. Platí zde, čím delší je velikost klíče, tím silnější je šifrování. Dlouhé klíče však také vedou k delším procesům šifrování, což někdy vytváří určité potíže při implementaci AES, zejména do programových aplikací.

AES je iterativní bloková šifra, která je založena na principu "síti substituční permutace". Ta zahrnuje řadu propojených operací, z nichž některé zahrnují nahrazení vstupů specifickými výstupy (operace substituce) a další zahrnují „promíchání“ s bity „rundového“ klíče (operace permutace) v rámci jednoho cyklu (rundy).

AES provádí všechny své výpočty s Byty spíše než s bity. Proto AES zachází s blokem 128 bitů otevřeného textu jako se sadou 16 Bytů. Těchto 16 Bytů je následně zpracováno při uspořádání do matice o čtyřech sloupcích.

Na rozdíl od algoritmu DES je počet rund v AES variabilní a závisí na délce klíče. AES používá 10 rund pro 128bitové klíče, 12 rund pro 192bitové klíče a 14 rund pro 256bitové klíče.

V každé z těchto rund použit jiný 128bitový rundový klíč, který se vypočítá z původního klíče AES.

9.5 Asymetrické algoritmy

Asymetrické algoritmy jsou postaveny na principu, kdy šifrovací proces, využívá různé klíče pro šifrování a dešifrování informací. Použité klíče odlišné, ale jsou matematicky spárovány, takže tedy možné, že zašifrovaný otevřený text pomocí jednoho (veřejného) klíče z daného páru může být dešifrován s využitím druhého (privátního) z páru klíčů. Významnou výhodou zejména v počítačových sítích je velmi jednoduchá distribuce klíčů. Veřejný klíč je publikován a kdokoliv jej může využít k zašifrování textu a pouze držitel privátního klíče si jej může převést zpět do čitelné podoby.

Nejznámějším a široce používaným je algoritmus RSA nazvaný dle svých tvůrců Rivesta, Shamira a Adlemana.

RSA

Tento šifrový asymetrický systém patří mezi základní šifrové systémy, které byly navrženy. Při použití tohoto systému je nutné vyřešit dvě základní operace. Jedná se o:

- vygenerování páru klíčů,
- vytvoření šifrovacího/dešifrovacího algoritmu.

Generování páru klíčů RSA

Každá osoba nebo strana, která se chce účastnit komunikace pomocí šifrování, potřebuje vygenerovat pár klíčů, jmenovitě veřejný klíč a soukromý klíč. Postup při generování klíčů vygenerování využívá principu faktorizace velkých prvočísel. Kdy výpočetně v reálném čase nemožné z vypočtené hodnoty n, která je součástí veřejného klíče, při faktorizaci velkého prvočísla nalézt dva hodnoty (p & q), které se používají k získání n.

9.6 Elektronický podpis

Návrh asymetrických kryptografických algoritmů umožnil navrhnout řešení elektronického podpisu.

S využitím algoritmu RSA lze jednoduše „podepsat“ příslušnou zprávu tím, že odesilatel použije svůj privátní klíč pro „zašifrování“ - podepsání své zprávy. Příjemce pak použije veřejný klíč odesilatele „dešifrování“ otisku zaslané zprávy, čímž získá důvěryhodnou informaci o tom, kdy danou zprávu podepsal (zašifroval privátním klíčem, který vlastní pouze dotčený odesilatel). Jiným než veřejným klíčem odesilatele (který je spárován s jeho privátním klíčem) nelze danou zprávu ověřit.

9.7 Biometrický dynamický podpis

Alternativou k Elektronickému podpisu na bázi kryptografických metod je dynamický biometrický podpis.

Systémy dynamických biometrických podpisů zaznamenávají vlastnoruční podpis s využitím speciálního „pera“ a digitalizačního tabletu, zaznamenávajícího data, která umožní analyzovat jak statické, tak zejména dynamické vlastnosti podpisu spojeného s typickým chováním podepisující se osoby. Počet a rozsah analyzovaných parametrů závisí na zvoleném tabletu a SW analyzujícím sejmutá biometrická data. Navrhované systémy tak mohou analyzovat nejen data souřadnicového systému podpisu, ale i další dynamické identifikátory.

Dynamický podpis obsahuje biometrické informace o tom, jak podpis byl vytvořen, odráží tedy charakteristické znaky podepisující se osoby, její návyky a projevy chování. Tyto vlastnosti představují biometrickou stopu, která je unikátní pro každého jednotlivce a nemůže být padělatelem reprodukována (na rozdíl od samotného obrázku podpisu, který zde tvoří pouze jeden z parametrů biometrické stopy).

Důležitým atributem dynamického biometrického podpisu je, že již sám v sobě obsahuje nejen prvek „živosti" objektu (pisatele), ale i skutečnost, že podpis vytvořil pisatel vědomě, takže není potřeba vyvíjet další mechanismy testující, zda objekt je živý či nikoliv rozdíl od statických biometrických metod (kontrola otisku prstů, dlaně, oka apod.). Můžeme také vycházet z vyvratitelného předpokladu, že osoba věděla, co podepisovala.

Verifikace osoby na základě jejího podpisu je jedna z nejpřirozenějších biometrických metod, protože jsme dennodenně zvyklí cokoliv stvrzovat naším podpisem.

V kapitole jsou uvedeny základy kryptografie. Je vysvětlen pojem kryptografický algoritmus a uvedeny jeho základní typy. Jsou zde popsány blokové a proudové šifry. Jsou popsány i hlavní představitelé symetrických a asymetrických algoritmů – DES, AES a RSA. Je zde uveden princip elektronického podpisu a jeho alternativy dynamického biometrického podpisu.

1. Co znamenají pojmy kryptografie, šifrování, šifrovací algoritmus?
2. Popište blokové kryptografické algoritmy a uveďte jejich odlišnost od proudových kryptografických algoritmů.
3. Popište princip symetrického kryptografického algoritmu.
4. Popište princip asymetrického kryptografického algoritmu.
5. Popište schéma DES, AES.
6. Popište princip RSA.
7. Co znamená pojem elektronický podpis?
8. Co znamená pojem dynamický biometrický podpis?

Literatura k tématu:

[1] http://www.tutorialspoint.com

[2] SMEJKAL, V., KODL, J., Uřičař, M. *Elektronický podpis podle nařízení eIDAS. Revue pro právo a technologie*, VI., 2015, č. 11, s. 189–235. ISSN 1804-5383 (Print), ISSN 1805-2797 (Online)

[3] CLARK, David Leon. *Enterprise Security: A Manager's Defense Guide*. 1st. ed. Boston: Addison-Wesley Longman Publishing Co., Inc., 2002. 288 s. ISBN 978-02-017-1972-7.

[4] MENEZES, Alfred, Paul C. Van OORSCHOT a Scott A. VANSTONE. *Handbook of Applied Cryptography. Rev. repr. with updates.* Boca Raton: CRC Press, 1997. 780 s. ISBN 0-8493-8523-7.

[1] SCHNEIER, Bruce. *Applied Cryptography,* Second Edition: Protocols, Algorithms, and Source Code in C. 2nd ed. New York: John Wiley & Sons, 1996. 758. ISBN 0471117099