Bezpečnost v distribuovaných systémech, ověřování uživatelů, ověřovací servery.

Operační systémy vyžadují ochranu na třech úrovních:

- ochrana zdrojů – ochrana proti neoprávněnému použití prostředků v OS
- bezpečná komunikace – vlastní ochrana přenášené informace
- ověřování uživatelů – zabezpečení, aby zprávy přicházely od ověřeného zdroje a bez modifikace

Napadení systému:

- pasivní
  - odposlech
  - analýza přenosu – odkud, kam, kolik, ...
- aktivní
  - modifikace, zadržování nebo podstrkávání zpráv
  - modifikace toku dat – změna obsahu, opakování, změna pořadí, rušení, syntéza zpráv, změna adresy, změna dat, atd

Cíl zabezpečení:

- prevence pasivního útoku
- detekce aktivního útoku.

Ohodnocení bezpečnosti

Existuje více způsobů, uvedeme TCB (Trusted Computing Base)

Klasifikace rozdělení do 4 tříd (A – nejlepší, D – bez zabezpečení)

- skupina D – bez zajištění bezpečnosti, minimální ochrana (MS-DOS)
- skupina C – volná ochrana (ponechána na uvážení)
  - třída C1 – volná ochrana – oddělení uživatele od dat, ochrana dat před neautorizovaným přístupem
  - třída C2 – řízená ochrana přístupu – přihlašování přes LOGIN+heslo
- skupina B – nařízená nebo vynucená ochrana
  - třída B1 – značená ochrana bezpečnosti – všechny objekty mají klasifikační značky, přístup subjektů (procesů) k objektům (zdrojům) řízen, přístup pouze k objektům s nižší klasif. značkou než uživatel
  - třída B2 – strukturovaná ochrana – systém od základů psán podle formálního modelu bezpečnosti, musí být identifikován každý kanál, který může ohrozit bezpečnost systému – rozumná úroveň zabezpečení
  - třída B3 – zavádí oblasti bezpečnosti – systém musí obsahovat monitor odkazů, jsou vytvořeny oblasti bezpečnosti, tj. seznamy uživatelů a skupin s jejich přístupovými právy k objektu a dále seznam uživatelů a skupin, pro které není zaručen žádný přístup
- skupina A – verifikovaná ochrana – vyžaduje úplný formální návrh systému, který je orientován na klasifikaci informace
  - třída A1 – systém s verifikovaným návrhem – obdoba B3 a navíc úplný formální návrh

Ochrana zdrojů v OS:

- přístupovou maticí – obsahuje – model informačního toku, objekt, jeho typ a povolené operace, subjekty, které mají právo manipulovat, přístupová prává a oblasti jejich použití
- přístupovým seznamem
- seznamem schopností (capabilities)

Zajištění bezpečné komunikace:

- zaměření na linku – zabezpečení na linkové úrovni
  - musí být transparentní pro uživatele
  - zabezpečení a šifrování kontinuálního toku dat
  - není vhodné pro otevřené systémy – není zaručena bezpečnost v koncových a mezilehlých uzlech (pouze dvoubodové sítě)
- zaměření na koncové uzly – šifrování mezi koncovými uzly.
  - použitelné jak v dvoubodových, tak mnohabodových sítích.
- zabezpečení na úrovni spojení – na relační nebo aplikační úrovni
  - volba úrovně zabezpečení programátorem

Bezpečnost

- požadavky na bezpečnost se v poslední době výrazně mění
- tradičně byla zajišťována zamezením přístupu (uzamykáním a administrativně)
- se zavedením výpočetní techniky vznikla potřeba vytvářet automatizované prostředky pro ochranu souborů a dalších informací
- použití počítačových sítí a komunikačních linek vyžaduje zajistit ochranu dat během přenosu

Definice

- počítačová bezpečnost – všeobecný název pro soubor prostředků, navržených k ochraně dat a maření úsilí hackerů
- síťová bezpečnost – opatření k ochraně dat během přenosu
- bezpečnost Internetu – opatření k ochraně dat během přenosu přes soubor propojených sítí
  - spočívá v opatření k odrazení, prevenci, detekci a korekci bezpečnostních hrozeb poškozujících přenos informace

Služby, mechanizmy, útoky

- bezpečnostní služby – zvýšení bezpečnosti přenosu a zpracování dat
- bezpečnostní mechanizmus – navržen k detekci, prevenci a obnově po bezpečnostním útoku, používá šifrovacích technik
- bezpečnostní útok – jakákoliv akce, která naruší bezpečnost informací

Bezpečnostní architektura OSI

- doporučení ITU-T X.800, v Internetu RFC 2828
- X.800 definuje 5 hlavních kategorií
  - authentication – ověření pravosti – ujištění, že entita je to, za co se vydává
  - access control – řízení přístupu – zamezení neautorizovaného využívání zdrojů
  - data confidentiality – důvěrnost dat – ochrana dat před neautorizovaným přístupem
  - data integrity – integrita dat – ujištění, že přijatá data byla odeslána ověřenou entitou
  - non-repudiation – nepopiratelnost – ochrana proti popření jednou z komunikujících entit

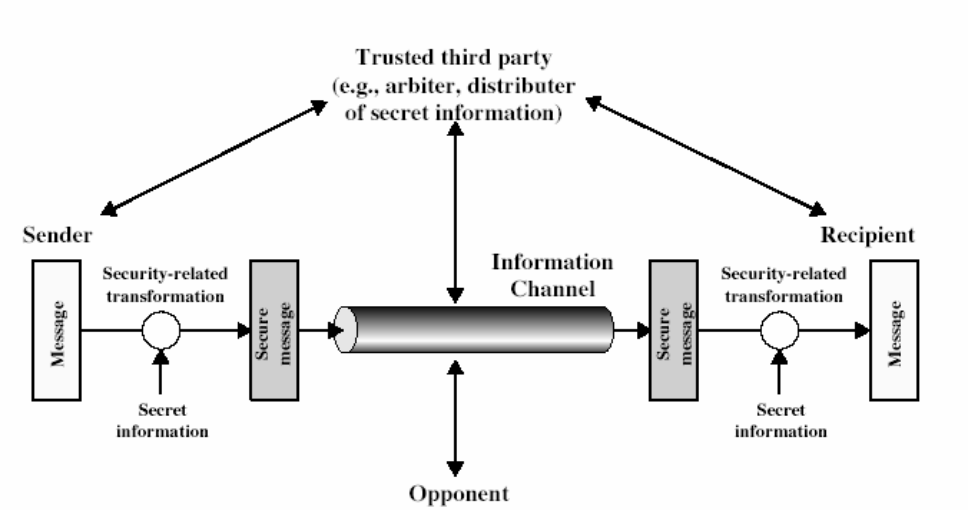
Bezpečnostní mechanizmy

- šifrování
- digitální podpisy
- řízení přístupu
- integrita dat
- ověřování výměny dat
- vyplňování přenosu
- řízené směrování
- ověřování třetí stranou

Klasifikace útoků

- pasivní útoky
  - odezírání, monitorování (získání obsahu, monitorování toků)
- aktivní útoky
  - maskování za jinou entitu
  - opakování předchozích zpráv
  - modifikace zpráv během přenosu
  - odepření služby

Model síťové bezpečnosti



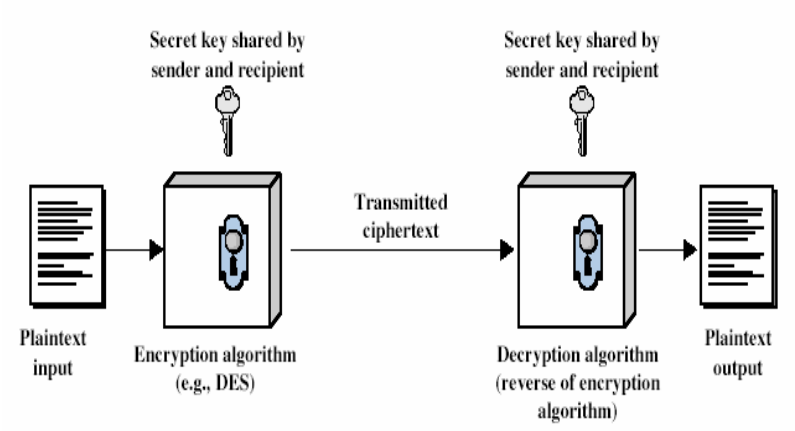
Šifrování

- symetrické (konvenční, tajný klíč, jeden klíč)
- asymetrické (tajný a veřejný klíč)

Terminologie

- otevřený text (plaintext)
- šifrovaný text (ciphertext)
- šifra – algoritmus pro transformaci otevřeného textu na šifrovaný
- klíč – parametr šifrování
- šifrování – převod otevřeného textu na šifrovaný
- dešifrování – převod šifrovaného textu na otevřený
- kryptografie – studium šifrovacích principů a metod
- kryptoanalýza – studium principů a metod pro dešifrování bez znalosti klíče
- kryptologie – kryptografie a kryptoanalýza

Symetrický model šifrování



Požadavky

- silný šifrovací mechanizmus
- šifrovací klíč zná pouze odesílatel a příjemce
- známý šifrovací (a dešifrovací) algoritmus
- bezpečný kanál pro distribuci klíče

$Y = E_K(X)$
$X = D_K(Y)$

Šifrovací operace

- substituce
- transpozice

Šifra

- bloková
- proudová

Útok hrubou silou

- absolutní bezpečnost – bez znalosti klíče nelze odhalit otevřený text
- výpočetní bezpečnost – šifra nemůže být zlomena pro nedostatečnou výpočetní výkonnost

Key Size (bits)	Number of Alternative Keys	Time required at 1 encryption/μs	Time required at 10^6 encryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\ \mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\ \mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\ \mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\ \mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26}\ \mu s = 6.4 \times 10^{12}$ years	6.4×10^6 years

Caesarova šifra (substituční)

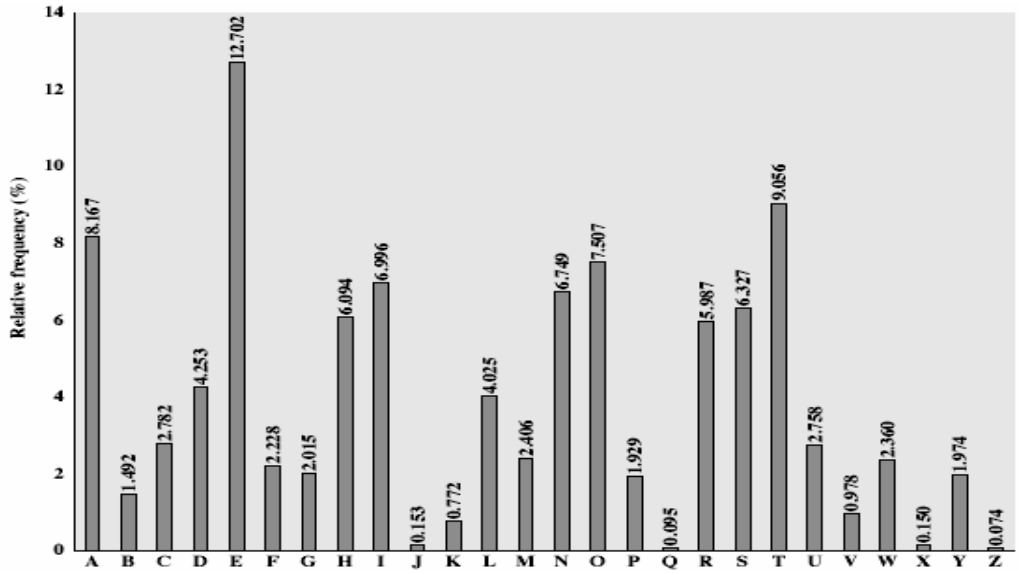
- pouze 26 možností
- útok hrubou silou

Monoalfabetické šifry

- náhodné přiřazení písmen (klíč 26 písmen dlouhý – $26! = 4x10^{26}$)

Plain: abcdefghijklmnopqrstuvwxyz
Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN
Plaintext: ifwewishtoreplaceletters
Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA

Frekvenční analýza



Šifrování tajným klíčem, symetrické metody šifrování.

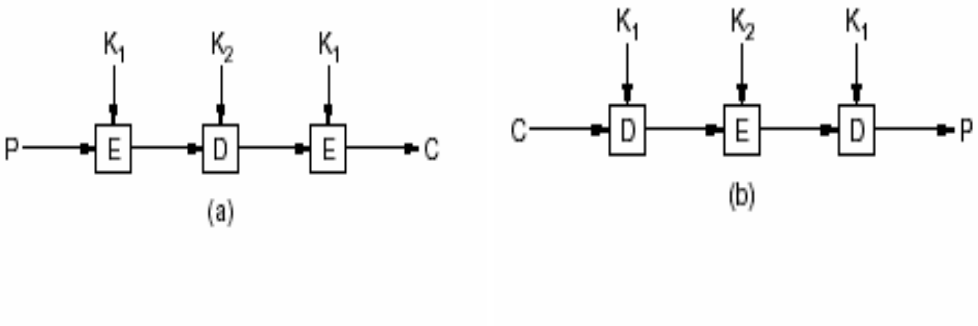
- Substituční šifry
- Každé písmeno nebo skupina písmen je nahrazena jiným písmenem nebo skupinou písmen
- Např. Caesarova šifra – použita Caesarovými vojsky
- Jednoduše prolomitelné
- Transpoziční šifry
- Přeuspořádání písmen, ale ne překódování
- Sloupcové šifrování – otevřený text je šifrován po sloupcích různými klíčovými slovy
- Ne tak jednoduché prolomení jako u substitučních šifer.

- Jednorázová hesla
- Šifrovaný text je vytvářen konverzí otevřeného textu na bitový řetězec a XOR-ován s náhodným bitovým řetězcem. Délka přenášených dat je omezena délkou řetězce (klíče)
- Neprolomitelná šifra
- Klíč je obtížné si pamatovat – odesílatel i příjemce musí přenášet i kopii klíče
- Vyžaduje striktní synchronizaci mezi odesílatelem a příjemcem. Jeden chybějící bit může pomotat cokoliv

Příklady – šifrování tajným klíčem

1. DES – Data Encryption Systém
   - Každá iterace i používá jiný klíč K_i. Složitost závisí na komolící funkci *f*.
   - Klíč K_i je odvozován od počátečního 56 bitového klíče.
   - Šifrovací algoritmus vyvinut v r. 1970 National Bureau of Standards and Technology a IBM.
   - Používá délku klíče 56 bitů a 19 různých stavů
   - Velmi silný, ale prolomitelný

2. Triple DES – řeší problém příliš krátkého klíče DES jeho rozšířením na 112 bitů
   - Pro šifrování postupně používá algoritmus šifrování klíčem K_1, dešifrování klíčem K_2 a šifrování klíčen K_1.
   - Pro dešifrování postupně používá algoritmus dešifrování klíčem K_1, šifrování klíčem K_2 a dešifrování klíčen K_1.



3. AES/Rijndael
   - DES je nyní příliš slabý
   - Nyní nahrazován vítězem konkurzu o šifrovací standard (AES – Advanced Encription Standard) – Rijndael.
   - délka klíče 128, 196 nebo 256 bitů

4. IDEA – International Data Encription Standard
   - Publikován v r. 1990
   - Používá klíč délky 128 bitů
   - Velmi silné šifrování, nebyly publikovány žádné praktické útoky, útok hrubou silou není praktický
   - Pokrytý různými mezinárodními patenty

5. Skipjack
   - Tajný algoritmus vyvinutý NSA

- Je použit v šifrovacím čipu Clipper
- Využívá klíč délky 80 bitů

Metody šifrování veřejným klíčem

RSA – vytvořeno pány Rivest, Shamir a Adlemin v r. 1978

- Velmi silná šifra
- Podporuje proměnnou délku klíčů
- Délka klíče 1024 bitů, 2048 bitů
- Delší klíče zajišťují větší bezpečnost
- Algoritmus založen na počítání s velkými prvočísly

p, q … velká prvočísla N = p.q
P.S = 1 [mod $\phi(N)$] $\phi(N)$ = nsn(p-1, q-1)
zašifr. $C = M^P \pmod N$
dešifr. $M = C^S \pmod N$
P … public key, S … secret key
– předává se P, N a utají S
– výpočet P, S, N musí být jednoduchý

Další systémy s veřejným klíčem

- Elgamal (Taher Gamal)
- Diffie-Hellman
- DSA (Digital Signature Algorithm)

ElGamal

- zahrnuje tři komponenty
  - generátor klíče
  - šifrovací algoritmus
  - dešifrovací algoritmus
- generátor klíče
  - zvolí se velké náhodné číslo p takové že p-1 = kq, kde k je malé a q je prvočíslo
  - nalezne se takové g, že $g^q = 1 \bmod p$ a $g \neq 1$
- Alice zvolí náhodné $x \in \{0, ..., q-1\}$ a vypočte $h=g^x$
- Alice publikuje popis množiny, ze které generovala g a {h, g, q} (veřejný klíč)
- Bob volí náhodné $y \in \{0, ..., q-1\}$ a vypočte $c_1=g^y$ a $c_2=m.h^y$, kde m je upravená zpráva
- Bob posílá Alici šifrovaný text $\{c_1, c_2\}$
- Alice vypočte $c_2(c_1^x)^{-1} = \frac{m \cdot h^y}{g^{xy}} = \frac{m \cdot g^{xy}}{g^{xy}} = m$
- Je-li zpráva větší než G, musí být rozdělěna na několik částí

Použití šifrování s veřejným klíčem

- šifrování zpráv (časově náročné)

- šifrování relačního klíče (relační klíč se použije k šifrování (symetrické) vlastní zprávy, výměna klíčů
- ověření integrity dat (ke zprávě se pomocí hashovací funkce vygeneruje otisk, který se zašifruje tajným klíčem odesílatele – je schopen provézt pouze majitel tajného klíče – plus ověření pravosti)
- nepopiratelnost (informace zašifrovaná tajným klíčem)

Hashovaní funkce

$h = f(m)$ h … výsledek, m …zpráva

$h_1 \neq h_2 \Rightarrow m_1 \neq m_2$ a $m_1 = m_2 \Rightarrow h_1 = h_2$

– metody: SHA

MD5 – kromě zprávy m pošlu $\{h\}_{KS}$,

kde $h = f(m)$

– neexistuje inverzní funkce k f

– zpráva se znovu zakóduje a porovnají obrazy

$\{\{h\}_{KS}\}_{KP} \rightarrow h$

$m \rightarrow h_1 = f(m) \rightarrow h_1 = h$

Digitální podpisy

- Garantují autentičnost digitálně podepsané zprávy
- Digitální podpis je sám o sobě šifrován tajným klíčem, aby se dala potvrdit
  - Autenticita
  - Integrita
  - Pravost podpisu - nedal se popřít
- Podpisy tajným klíčem
  - Jako úložiště všech digitálních podpisů je použita centrální autorita
  - Centrální autoritě musí všichni věřit
- Podpisy veřejným klíčem
  - Zpráva je šifrována veřejným klíčem odesílatele a dešifrována tajným klíčem odesílatele

Autentikace

- Autentikace je technika, pomocí které se ověřuje, že komunikující partner je ten, za kterého se vydává a ne podvodník.

Existují tři způsoby autentikace

- Řekni něco co víš (heslo)
- Ukaž něco co máš (identifikační karta)
- Nech systému něco tvého změřit (otisk prstu)

Ověřovací schémata

- musí obsahovat aspoň jedno tajemství
- musí být schopna rozpoznat jeho správné použití

Ověřovací metody

- jednoduché (založeny na heslech)
- přísné (založeny na šifrovacích metodách)

Jednoduché ověřování

- identifikace jménem a heslem,
- přenos otevřeného textu, použití ověřovacího serveru

Přísné metody

- elementární metody – použití symetr. a nesymetr. kódů
- metody založené na ověřovacích serverech
- metody založené na protokolech s minimální znalostí
  - uživatel dokazuje svoji identitu odpovídáním na šifrované otázky serveru
    M1: {R, ID}
    M2: $\{C\}_K$
    M3: $\{f(C)\}_K$
    R … požadavek, K … tajný klíč, C … náhodné číslo, f(C) … domluvená funkce

Ověřovací servery

- slouží k ověření „pravosti“ uživatele
- lepší utajení klíčů
- používá se KDC (Key Distribution Center) – databáze klíčů (je tajná a indexována podle jmen uživatelů)

Certifikační autority

- Používají se k administraci a ověřování veřejného klíče.
- Musí být důvěryhodnou stranou.
- Umožňují ověřování uživatele v rozsáhlém systému – decentralizované ověřování.
- Princip – veřejný klíč je předáván ve formě, jejíž pravost lze ověřit pomocí ověřeného veřejného klíče certifikační autority.
- Certifikát je blok dat (soubor), obsahující:
  - Verze (V3)
  - Sériové číslo (02 1c 6a)
  - Algoritmus podpisu (md5RSA)
  - Vystavitel (CN = CA GE Capital Bank, OU = Direct Banking, O = GE Capital Bank, a.s., C = CZ)
  - Platnost od (28. dubna 2003 12:31:30)
  - Platnost do (27. dubna 2005 12:31:30)
  - Předmět (E = ledvina@kiv.zcu.cz, CN = uid: 120295, CN = Ing. Jiri Ledvina, ... adresa)
  - Veřejný klíč (30 81 87 02 81 81 00 bf 4a ...)
  - Distribuční místo (URL=http://www.gecb.cz/ca_ge.crl)

    - Použití klíče (Digitální podpis, Zakódování klíče)
    - Algoritmus miniatury (sha1)
    - Miniatura (72 19 13 5c 6a 9b 4e ab 30 cf 6b 6f 49 df 15 c0 62 94 79 09)
    - Popisný název (Ing. Jiri Ledvina)
- Certifikát musí být nezpochybnitelný – zneplatnění certifikátu
- Existují různé formáty certifikátů
    - Personal Information Exchange (PEX), PKCS #12 (P12) (Public Key Cryptography Standard)
    - Cryptographic Message Syntax Standard PKCS#7 (P7B)
    - PGP certifikáty

Ověřování certifikátů

- přímé ověřování (nejjednodušší model)
    - Ověřování certifikátů mezi důvěryhodnými subjekty
    - V prohlížečích jsou certifikáty uznávaných autorit instalovány – můžeme (musíme) jim věřit. Existují ale i další certifikační autority, které nejsou uznávané – prohlížeč se na důvěryhodnost ptá.
- hierarchické ověřování – zřetězení certifikátů
    - Certifikačních autorit je hodně – získání certifikátu může být otázkou osobní návštěvy (důvěryhodné získání certifikátu).
    - Certifikační autority mohou vytvářet hierarchický strom – důvěryhodnost CA nižší úrovně je potvrzována CA vyšší úrovně. CA nejvyšší úrovně potvrzuje důvěryhodnost sebe sama.
    - Zřetězení CA je součástí certifikátu.
- kumulativní model – zahrnuje předchozí (přímé, zřetězené)

Protokoly pro bezpečnou komunikaci

Kerberos – ověřování v systému Orion na ZČU

- Používá symetrické šifrování
- Vychází z centralizované databáze uživatelů (každý uživatel musí být registrován)
- Základní část je ověřovací server (Kerberos)
- Po přihlášení (ověření) dostane uživatel lístek, obsahující práva přístupu k požadovanému serveru.
- K dalšímu ověřování uživatele se používaní pověřovací listiny (credentials), obsahující jméno uživatele a adresu jeho počítače.

SSL – Secure Socket Layer

- Vyvinuto fy. Netscape, používá se zejména pro bezpečné přenosy mezi prohlížečem a webovým serverem.
- K ověřování serveru se používají certifikáty serveru. Uživatel není ověřován.
- Po ověření se veřejný klíč použije pro vygenerování relačního klíče, sloužícího k šifrování komunikace.
- Schéma bezpečného HTTP se označuje HTTPS
- SSL se používá i u dalších protokolů (POP, IMAP)
- Je možné je využít univerzálně – vytváří mezivrstvu mezi protokolem TCP a aplikací – před použitím je třeba aplikaci (program) modifikovat.

- Obdobou SSL je TLS (Transport Level Security)

SSH – Secure Shell

- Používá se pro vytvoření šifrovaného kanálu mezi aplikacemi (aplikační úroveň).
- Pro šifrování používá opět relační klíč, vytvořený na základě výměny informací (Diffie - Hellman algoritmus pro výměnu klíčů) nebo na základě asymetrické kryptografie – RSA.

Využívá se pro

- bezpečný vzdálený přístup – náhrada Telnetu (ssh – secure shell),
- bezpečný přenos souborů – náhrada ftp (scp – secure copy),
- vytvoření bezpečného kanálu mezi libovolnými aplikacemi.

IPsec – IP security

Vytváří bezpečný kanál mezi dvěma počítač na síťové úrovni.

Zabezpečení elektronické pošty

PEM (Privacy Enhancement for Internet Electronic Mail)

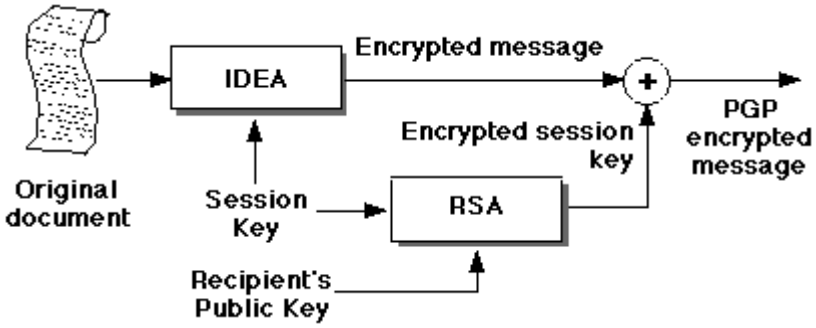
- Dnes historický protokol pro vytváření a zpracování bezpečných zpráv.
- Vznikl v druhé polovině 80. let.
- Původní specifikace RFC989, poslední specifikace RFC1421 až RFC1424 (1993).
- V praxi nedošlo k jeho masovému využití nejširší veřejností - nebyl totiž běžně dostupný software, který by jej podporoval.
- Na přelomu 80. a 90. let nebyla ještě masová poptávka po software tohoto druhu.
- Stal základem pro novější protokoly (S/MIME)

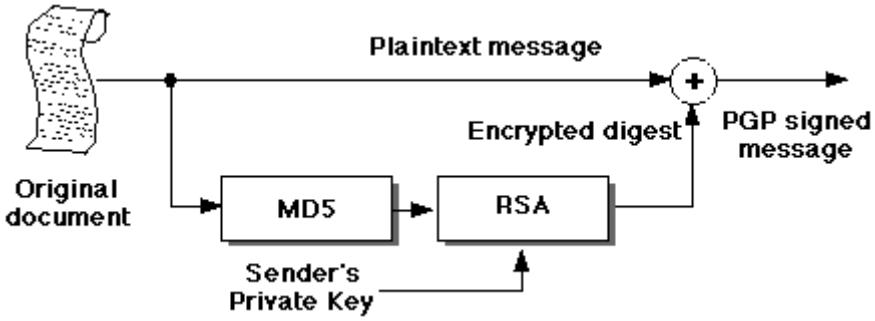
S/MIME

- Podobné PEM
- Kontrolní součet (otisk) SHA-1 a MD5
- Asymetrické šifrování (šifrování symetrických šifrovacích klíčů a elektronický podpis): RSA s délkou klíče minimálně 512 bitů.
- Symetrické šifrování - šifrování textu zprávy (DES-CBC, triple DES).
- Norma PKCS-7 pro tvorbu bezpečných zpráv - elektronický podpis, šifrování, obojí.
- Definuje MIME hlavičku Content Type: Application/pkcs7-mime

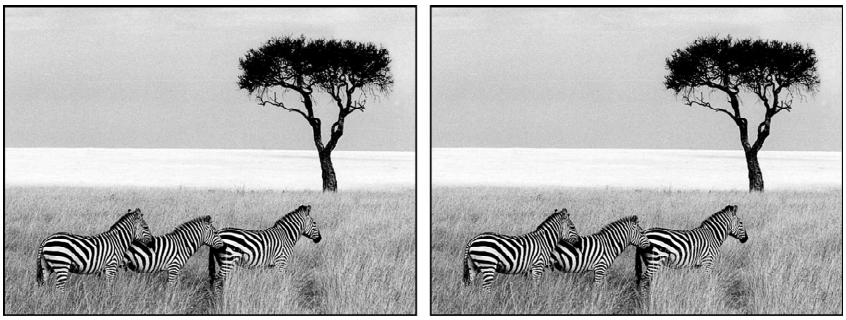
PGP (Pretty Good Privacy)

- Uživatelsky jednoduchý program dostupný nejširší veřejnosti.
- PGP je nejrozšířenější prostředek pro zpracování bezpečných zpráv (RFC1991).
- Vytvořil Američan P.R.Zimmerman (1991).
- Bezpečný přenos zpráv pomocí SMTP, POP, IMAP (nepotřebuje nový protokol, nadstavba nad stávajícími).
- Asymetrické šifrování - RSA (šifrování symetrického relačního klíče pro šifrování vlastní zprávy).
- Symetrické šifrování algoritmus - IDEA.
- Komprese dat před šifrováním - PKZIP.
- Výpočet kontrolního součtu (otisku) - MD5.
- Převod binárních dat na ASCII - Radix-64.





Steganography



(a) Three zebras and a tree. (b) Three zebras, a tree, and the complete text of five plays by William Shakespeare.