Technologie datové bezpečnosti vnitřních sítí

Technology data safeness inner net

David Ševčík

Bakalářská práce
2007

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektrotechniky a měření
akademický rok: 2006/2007

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**David ŠEVČÍK**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Technologie datové bezpečnosti vnitřních sítí**

Zásady pro vypracování:

1. Vyhledejte vhodné zdroje řešící bezpečnost vnitřních sítí.
2. Analyzujte současná bezpečnostní rizika.
3. Navrhněte způsoby eliminace bezpečnostních rizik na úrovni současných poznatků a tyto realizujte.
4. Vyhodnoťte úspěšnost realizace a definujte silná a slabá místa zvolených řešení.

Rozsah práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

Harold Davis: Bezdrátové sítě, Grada 2006 Jaroslav horák: Bezpečnost malých počítačových sítí, Grada 2006 Scambray Kurt McClure: Hacking bez záhad, Grada 2007 Janet Valade: Linux, Grada 2006

Vedoucí bakalářské práce: **Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a statistiky

Datum zadání bakalářské práce: **13. února 2007**

Termín odevzdání bakalářské práce: **29. května 2007**

Ve Zlíně dne 13. února 2007

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Práce řeší informační a datovou bezpečnost uvnitř firemní sítě včetně stanovení její politiky. V práci budou představena možná technologická řešení ve vazbě na aktuální bezpečnostní rizika. Při práci budou využity volně dostupné internetové informační zdroje, odborná literatura, softwarová řešení a případové studie.

Klíčová slova: počítačová síť, topologie, rozbočovač, šifrování

ABSTRACT

The work smoothing informative and data safeness inside company nets inclusive assesment her engineering. In work will superior possibly technological solving on trial on actual safety risks. At work will used freely accessible Internet source of information, special literature, software solving and case study.

Keywords: computer network, topology, hub, encryption

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu mé bakalářské práce doc.Mgr.Romanovi Jaškovi, Ph.D. za jeho podnětné připomínky, návrhy, profesionální vedení, pomoc při tvorbě bakalářské práce a za odborné konzultace.

Prohlašuji, že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků, je-li to uvolněno na základě licenční smlouvy, budu uveden jako spoluautor.

Ve Zlíně …….

Podpis

OBSAH

ÚVOD

Většina moderních organizací využívá ke své pracovní činnosti služeb výpočetní techniky, osobních počítačů. Možnosti výpočetní techniky jsou obrovské a organizace toho využívají. Výměna informací v elektronické podobě je trendem dnešní doby. Organizace spojují jednotlivé počítače do malých sítí, později je můžou připojit i do celosvětové sítě Internet. Počítač může být dobrý sluha, ale zlý pán. Počítače nám výrazně zjednodušují naši práci, ale když náš počítač ovládne neoprávněná osoba, například se připojí do naší sítě a zkopíruje si obsah našeho harddisku, může nám způsobit velké hmotné i nehmotné škody. Ne každá informace je určená očím a uším každého. Proto je třeba se před takovým neoprávněným ovládnutím chránit. Jinak řečeno, data je často třeba chránit, zajistit jejich bezpečnost. Nikdy nedosáhneme ideálního stavu, absolutní bezpečnosti. Vždycky tady byly a budou různé bezpečnostní rizika, která budou bezpečnost naší sítě snižovat. Budu se naopak snažit naši síť zabezpečit tak, abych tyto bezpečnostní rizika snížil na co nejnižší úroveň a co nejvíce se přiblížil ideálnímu stavu.

Otázkou zůstává jak tohoto stavu dosáhnout.

Fyzická ochrana přenosu dat je často náročná, většinou však nemožná. Nelze si představit ochranu byť jen několik kilometrů dlouhé přenosové trasy tak, aby z ní nebylo možné signál odposlechnout. Často se navíc využívá komutované linky, která na každém uzlu k odposlechu přímo vybízí. Jistou bezpečnost snad nabízí spojení pomocí optického kabelu, ale ani v tomto případě nelze mluvit o vysokém stupni ochrany. Nabízí se tedy možnost logické ochrany dat, neboli šifrování. Znamená to zašifrovat data na straně odesilatele, odeslat je a na straně příjemce zase dešifrovat. Tato bakalářská práce je tedy zaměřená hlavně na šifrování dat, jednotlivé typy šifrování, principy a jejich následnou aplikaci v praxi.

Podle předpovědi společnosti McAfee a jejího vývojového oddělení McAfee Avert Labs, která se týká největších bezpečnostních hrozeb pro rok 2007, dnes existuje více než 217 tisíc různých druhů bezpečnostních hrozeb a další tisíce jich dosud nebyly identifikovány. Několik nejznámějších, nejzávažnějších a nejčastěji se vyskytujících hrozeb blíže popíši a zkusím na ně nalézt adekvátní bezpečnostní opatření.

I. TEORETICKÁ ČÁST

1 CHARAKTERISTIKA VNITŘNÍ SÍTĚ

1.1 Počítačová síť

Počítačová síť je souhrnné označení pro technické prostředky, které realizují spojení a výměnu informací mezi počítači. Umožňují tedy uživatelům komunikaci podle určitých pravidel, za účelem sdílení využívání společných zdrojů nebo výměny zpráv.

Každá počítačová síť se vyznačuje svojí topologií. Skládá se ze vzájemně komunikujících uzlů (např. počítače a servery, tiskárny, datová úložiště, měřicí a zabezpečovací zařízení atd.) propojených komunikačními kanály (optické nebo metalické kabely, např. koaxiální kabel nebo kroucená dvojlinka – UTP, rádiové spoje, vzdušné optické spoje např. laser, infračervené spoje v otevřeném prostoru, ultrazvukové spoje)

1.2 Topologie

Klíčovou úlohu v počítačových a informačních sítích mají takzvané aktivní síťové prvky. Jejich úkolem je sdružovat či rozbočovat komunikační kanály, provádět přeměnu druhu rozhraní a zajišťovat různé řídicí a bezpečnostní funkce v síti.

- Sběrnice (bus, ethernet) – kabel prochází okolo všech počítačů, nerozvětvuje se
- Hvězda (ARCNet) – všechny počítače připojeny k aktivnímu prvku
- Aktivní prvek (hub) – posílá signál do všech větví
  - Switch (přepínač, chytřejší) – posílá signál jen do jedné větve (kam patří)
- Kruh – spojení je uzavřeno (vznikne propojením obou konců sběrnice)
- Strom – kombinuje sběrnici s hvězdou
- Samostatný počítač (virtuální síť)
- Neomezená (např. Internet)

1.3 Síťové prvky

- Směrovače (router)

- Přepínače (switch)
- Koncentrátory a rozbočovače (hub)
- Síťové mosty (bridge)
- Měniče rozhraní (mediakonvertory)
- Bezpečnostní zábrany (firewall)
- Opakovače (repeater)
- Modulátory/demodulátory (modem)
- Vysílače/přijímače (transceiver)

1.4 Typy sítí

Podle druhu přenášených signálů můžeme sítě rozdělit na *analogové* a *digitální*. Nejzajímavější jsou ale typy sítí z hlediska rozlehlosti a účelu.

Z hlediska rozsahu můžeme sítě rozdělit na tři základní skupiny:

1.4.1 Local Area Network – LAN

Lokální sítě propojují koncové uzly typu počítač, tiskárna, server. LAN jsou vždy v soukromé správě a působí na malém území. Připojená zařízení pracují v režimu bez navazování spojení, sdílí jeden přenosový prostředek (drát, radiové vlny), ke kterému je umožněn mnohonásobný přístup.

Přenosové rychlosti LAN začínají na desítkách Mbit/s, nejnovější technologie (r. 2004) umožňují přenos s rychlostí až jednotky Gbit.

1.4.2 Metropolitan Area Network – MAN

Metropolitní sítě umožňují rozšíření působnosti lokálních sítí jejich prodloužením, zvýšením počtu připojených stanic a zvýšením rychlosti. Rychlost MAN sítí bývá vysoká a svým charakterem se řadí k sítím LAN. Sítě mohou být jak soukromé, tak veřejné, které provozovatel pronajímá různým uživatelům.

1.4.3 Widea Area Network – WAN

Rozlehlé sítě umožňují komunikaci na velké vzdálenosti. Bývají obvykle veřejné, ale existují i soukromé WAN sítě. Typicky pracují prostřednictvím komunikace se spojením, které nepoužívají sdílený přenosový prostředek.

Přenosové rychlosti se velmi liší podle typu sítě. Začínají na desítkách Kbit, ale dosahují i rychlostí řádu Gbit. Příkladem takové sítě může být Internet.

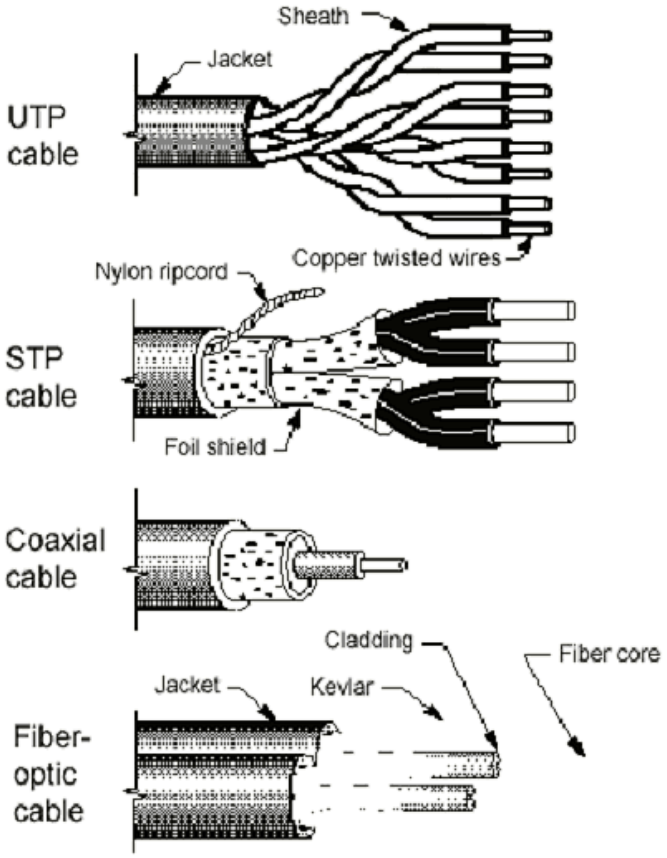
1.5 Použité přenosové médium

V současné době je v LAN nejpoužívanějším přenosovým médiem kroucený dvoupár označovaný jako UTP (Unshelded Twisted Pair).

V Evropě je ovšem používanější stíněná modifikace tohoto kabelu – stínění je prováděno na úrovni celého svazku, jedná se tedy o ochrannou fólii pod plastovým obalem kabelu. Označení je pro tuto modifikaci STP (Shielded Twisted Pair) nebo FTP (Foiled Twisted Pair).

Ještě před nedávnou dobou byl nejpoužívanějším přenosovým médiem v Ethernet LAN sítích koaxiální kabel. Výhodou byla cena a jednoduchost provedení. Nevýhodami jsou náchylnost k poruchovosti a technologická omezení (počet uzlů, rychlost). Typickou topologií tvořenou koaxiálním kabelem je sběrnice.

V LAN sítích se pro překlenutí delších vzdáleností používají optické kabely. Pro kratší vzdálenosti (cca 260 m až 2 km v závislosti na technologii) multimodové (neboli mnohovidové) pro větší vzdálenosti singlemodové (neboli jednovidové). Optické kabely se používají i pro spojování budov tam, kde je nutné realizovat spoj venkovním prostředím a to i na poměrně krátké vzdálenosti. Optické kabely totiž zajistí galvanické oddělení potenciálů a nezpůsobí zničení infrastruktury při náhodném úderu blesku. Typickou topologií tvořenou optickým kabelem je hvězda.



Obrázek 1 Typy přenosových médií

Jsou místa kde nelze použít spojení optikou. Důvodem může být např. přílišná nákladnost položení kabelu nebo dokonce nemožnost položení kabelů. V tom případě jsou používány bezdrátové technologie. Ty byly časem rozvinuté tak, že jsou používány jako alternativa lokálních sítí založených na kabelových systémech. Nevýhodou jsou prozatím cena a relativně nízká rychlost. To ale naopak nečiní překážky pro použití bezdrátových sítí pro připojování k Internetu – zde se daří dosahovat více než zajímavého poměru cena/výkon.

2 SOUČASNÁ BEZPEČNOSTNÍ RIZIKA

2.1 Možnosti úniku informací

1. nespolehlivost a selhání lidského faktoru
2. nespolehlivost a selhání technických systémů, včetně softwarových podsystémů

Lidé jsou nejčastějším problémem úniku informací a dat a jejich neznalost, nedbalost, neopatrnost a mnohdy i záměr ovlivňují spolehlivost počítačových a komunikačních systémů.

2.2 Definování požadavků

Při definování požadavků na ochranu informací je třeba si odpovědět na tyto otázky:

- Které informace, data, počítačové a komunikační systémy je třeba považovat za důvěrné či jinak utajované, které jsou hlavní elementy utajovaných informací a proč?
- Jak dlouho je třeba určité informace a data uchovávat v tajnosti a proč?
- Co je již známo a proč?
- Které podnikové útvary a z nich které osoby jsou nebo budou s danými informacemi seznámeny a proč?
- Které podnikové útvary a které osoby mají přístup do počítačového nebo komunikačního systému, v jakém rozsahu a proč?

2.3 Bezpečnost softwarových prostředků spočívá:

- v ochraně proti virům
- v obraně proti zneužití programového vybavení
- v ochraně proti zničení či poškození softwarových vybavení
- v ochraně proti podnikové špionáži

2.4 Druhy ohrožení

Z hlediska způsobu ohrožení informačního systému rozlišujeme dva druhy:

a) úmyslné – sem patří vyzvídání, odposlouchávání, tzv. počítačové pirátství (pronikání do informačního systému s cílem data získat, změnit nebo zničit), ohrožení systémů počítačovými viry aj.

b) nedbalostní – způsobené lidským faktorem, např. chybami operátorů´, chybnými vstupními daty, chybami programového vybavení, selháním hardwaru, prostředím (výpadek proudu, přírodní katastrofa…)

2.5 Druhy škod

a) přímě ztráty – vyzrazení obchodních záměrů, výsledku výzkumu, důsledky nelegálních finančních transakcí, zvýšené náklady na obnovení ztracených informací nebo obnovení výroby v důsledku nuceného přerušení výroby či expedice zboží aj.

b) nepřímé ztráty – ztráta dobrého jména podniku, protože nebyly dodrženy dohodnuté podmínky, čímž dochází i k finančním ztrátám…

2.6 Následky různých hrozeb

- ztráta dobrého jména
- ohrožení bezpečnosti osob
- porušení právních norem
- porušení důvěrnosti osobních údajů
- vyzrazení obchodního tajemství
- přerušení aktivit organizace tím, že služby informačního systému nebudou dostupné

2.7 Informační hrozby

V oblasti nových technologií se objevují nové typy hrozeb, u kterých se předpokládá, že se časem rozšíří a způsobí velké ztráty. Jsou to hrozby webu 2. generace, databázové červy, hrozby RFID, reverzní inženýrství zdrojových kódů firemního SW, zneužití ovladačů koncových zařízení, ROOTKITY, zneužití malých kancelářských nebo domácích aplikací, hrozby sdílených kódů/SOA technologie, hrozby nespravovaných koncových zařízení, hrozby VoIP a hrozby virtualizační.

V nadcházejících dvou letech budou kulminovat hrozby krádeže identity, sociální inženýrství a cílené hrozby s finanční motivací. Proto bude důležitá pravidelná systematická výchova všech uživatelů.

2.7.1 Stručný popis jednotlivých bezpečnostních hrozeb

Krádež identity – rozumíme tím krádež osobních nebo finančních dat za účelem páchání trestné činnosti vedoucím zpravidla k nejrůznějším podvodům.

Sociální inženýrství – jedná se o přesvědčování uživatelů, aby udělali něco, co by při dodržování všech bezpečnostních pravidel nikdy neudělali, tím jsou prolomena technologická a organizační bezpečnostní opatření umožňující kybernetický útok.

Spyware – je to nežádoucí software, který poškozuje systémy, monitoruje uživatele a informace předává pachateli bez vědomí uživatele.

Cílené hrozby – jde o kybernetické útoky s cílem obohatit se. Jsou vedeny proti firmě nebo celému průmyslu. Není možné je detekovat nebo jim preventivně zabránit použitím standardních typových opatření. Útočníci používají netypické formy útoků.

Viry – jsou škodlivé programy, které vykonávají určitou z bezpečnostního pohledu negativní činnost.

DoS útoky – cílem je poškodit nebo vyřadit určité služby, např. zahlcením systému velkým množstvím požadavků na zpracování dat.

Hybridní červi – jsou programy způsobující škody za využití technologie běžných virů. Na rozdíl od virů jsou hybridní červi samospustitelní, jejich cílem je analyzovat slabá místa SW nebo technologické prostředí, což způsobuje jejich rychlé rozšíření.

Databázoví červi – cílem je útok na systém řízení relační databáze. Sami se šíří a jsou schopni zničit obrovský objem dat ve velice krátkém čase.

Finanční trojští koně – jedná se o škodlivý software, speciálně určený pro finanční podvody. Vkládá podvodné transakce během bankovních nebo jiných komerčních transakcí s autentizací uživatele.

Nezabezpečený aplikační vývoj – umožňuje útočníkům detekovat a zneužívat slabá místa aplikačního SW. Útočníci využívají nástrojů na penetrační testování analyzátory zdrojových kódů a nástroje reverzního inženýrství, dešifrovací technologie a crackery na získávání přístupových hesel.

Zneužití ovladačů koncových zařízení – ovladače fungují na nejnižší úrovni operačního systému. Cílem zneužití je kompletně vyřadit cílový stroj, systém z provozu.

Zranitelnost rozšířených operačních systémů – operační systémy se přenáší do prostředí koncových zařízení, například PDA, bankomaty, procesní kontrolery… kvůli kompatibilitě s běžnými operačními systémy. Tyto koncová zařízení jsou však hůře chráněná proti hrozbám a je tu riziko přenosu hrozeb do centrálního systému.

Hrozby regulatorních, auditorských společností – tyto společnosti požadují po firmách mnoho kritických informací. Hrozí pak velké ztráty v případě úniku těchto informací ke konkurenci.

Úniky dat z přenositelných médií – za použití přenositelných médií, jako jsou USB flashdisky, externí disky, CD nebo DVD vypalovačky, iPody, PDA, které umožňují přenesení velkého množství dat, hrozí instituci odcizení citlivých dat, protože tyto přenosy nemusí být autorizovány.

Hrozby RFID – zaměřují se na útoky na majetek, záměnami identity osob, zboží… jejich klonováním.

Sdílený kód/SOA – nebezpečí zde představují služby postavené na architektuře SOA díky sdíleným programovým kódům, které mohou obsahovat chyby, nebo jiná slabá místa a v konečném důsledku představují hrozbu pro kompletní aplikace na nich postavené.

Reverzní inženýrství firemních zdrojových kódů – je to reverzní analýza zdrojových kódů podnikových aplikací, která zkoumá zranitelnost technologického, procesního, algoritmického know-how a následného odcizení.

Rootkity – je to modifikovaný soubor nebo skupina souborů, které zaměňují útočníci za původní originální soubory, kvůli získání kontroly nad systémem a nebylo je možné na úrovni administrace systému detekovat. Rootkity mají většinou stejná souborová jména, velikost, datum vzniku jako originální soubory. Rootkity můžeme dělit na systémové a aplikační.

Nespravovaná koncová zařízení – jsou to zařízení, která nejsou registrována, tedy nejsou řízena, i když jsou připojena do sítě. Můžou to být třeba osobní notebooky zaměstnanců, tiskárny, kopírky atd. Nad těmito zařízeními nemá centrální útvar IT dohled.

Hrozby nechráněného dne – jsou to útoky na slabá místa nebo jiné nedostatky softwaru ještě před nainstalováním opravných patchů.

Generátory zákeřných kódů – jsou to generátory škodlivých kódů, které vygenerují velké množství kódů v různých variantách, které pak můžou prolomit ochranu antivirového systému.

Zneužití malých kancelářských nebo domácích aplikací – tyto aplikace nejsou profesionálně podporovány, řízeny ani zabezpečeny, což vede k jejich zranitelnosti.

3 FYZICKÉ ZABEZPEČENÍ SÍTÍ

Fyzickým zabezpečením kabeláže, serverů a aktivních prvků jejich vhodným umístěním. Pracovní stanice, tiskárny, terminály fyzicky zabezpečit hardwarovými klíči, biometrickými systémy, smart-card systémy, bezpečnostními kalkulátory a dalším autentizačním zařízením.

3.1 Zabezpečení kabeláže, serveru, rozbočovačů

Umístění kabeláže tak, aby nebyla snadno přístupná, například do stropních podhledů. Tam, kde to nejde, schovat kabeláž do krycích lišt.

Pro server vyčlenit speciální místnost s omezeným přístupem zaměstnanců. Přístup by měl mít pouze správce sítě, případně jeho zástupce. Místnost se serverem by měla být dostatečně zabezpečená, nejlépe bez oken, jeden přístup dveřmi, které budou zabezpečené prvky mechanických zábranných systémů. Ty můžou být kombinované prvky elektronických zábranných systémů, například přiložením čipové karty, zadáním hesla. Celá místnost se serverem by měla být střežena detektorem pohybu a protipožárním detektorem.

Aktivní prvky, jako switche, huby a jiné rozbočovače a přepínače umístnit do uzamykatelných skříní.

3.2 Další možnosti zabezpečení

3.2.1 Proprietární metody

Existuje poměrně široká škála produktů, které umožňují nastavit na port nebo na celý prvek seznam oprávněných MAC adres. Přepínač pak na portu přijme pouze konkrétní MAC adresu a pro jiné zůstane v zablokovaném stavu, případně se zablokuje celý port. Tato vlastnost je také používána v bezdrátových sítích.

V případě přepínačů nemá útočník možnost odposlechnout jaké MAC adresy se na síti objevují. V okamžiku kdy se do přepínače připojí, je port zakázán a to buď na určitou dobu nebo do zásahu administrátora (záležitost konkrétní implementace). Potenciální slabinou

tohoto systému jsou otevřené díry v podobě malých rozbočovačů nebo přepínačů v kancelářích s nedostatkem zásuvek.

Nároky na údržbu jsou poměrně vysoké (samozřejmě jsou jiné v prostředí malé kanceláře s několika počítači a jiné v prostředí s více přepínači nebo access pointy a velkým pohybem lidí nebo techniky).

Doplňkovými funkcemi mohou být např. omezení počtu MAC adres na port. To je výhodné jako obrana proti MAC spam útokům, kdy útočník vygeneruje velké množství různých MAC adres, čímž ucpe FDB (CAM) tabulky a přepínače se začnou chovat jako rozbočovače - pak již stačí pouze spustit sniffer a má vše jako dlani.

3.2.2 Externí sběr informací

Součástí některých softwarových balíků (např. OpenView) jsou aplikace, které jsou schopné hlídat na síti výskyt MAC adres a pokud se vyskytne adresa, která není vedena v databázi, případně vedena je, ale jako zakázaná, spustí se poplach, případně aplikace provede definovanou akci.

Ty nejjednodušší aplikace fungují stylem snifferu, kdy poslouchají broadcasty na segmentu do něhož jsou připojeny a z paketů si vyzobávají zdrojové MAC adresy. Lepší software je schopen číst data z L3 aktivních prvků a zjišťovat tak stav ve více segmentech (např. VLAN).

3.3 Autentizační zařízení

3.3.1 Hardwarové tokeny

Nejjednodušší možností je použít nějaký typ vyjímatelného média, jako je např. disketa, CD-ROM nebo populární USB flash disk, na které se soukromý klíč uloží místo pevného disku. Po dobu práce je médium s klíčem zapojeno do počítače a aplikace s klíčem pracují stejně, jako by byl přímo na pevném disku počítače, tj. přistupují k souboru na výměnném médiu. Po ukončení práce uživatel vyjme médium z počítače a klíč tak není v počítači nadále dostupný a nemůže se stát předmětem útoku. Tento postup je sice jednoduchý, ale neposkytuje žádnou ochranu pro klíč v okamžiku, kdy je médium s klíčem připojeno

k počítači. Navíc se zvyšuje riziko prozrazení klíče, protože médium je přenosné a může se ztratit nebo být ukradeno. Naopak výhodou tohoto přístupu je fakt, že jej lze začít používat okamžitě a nejsou potřeba žádné změny v aplikacích.

3.3.2 Čipové karty

Další možností je použití čipových karet a příbuzných technologií, které obsahují jak chráněný prostor, do kterého lze uložit soukromý klíč s certifikátem, tak i samostatný procesor, který je schopen s těmito klíči pracovat a provádět s nimi základní kryptografické operace. Karta je k počítači připojena pomocí čtečky zapojené přes USB nebo sériový port, pomocí které komunikují aplikace s kartou. Aplikace tak nepoužívají přímo soukromý klíč, ale předávají kartě data, která jsou zpracována procesorem na tokenu a výsledek je vrácen zpět aplikaci. Klíč tak nikdy neopustí kartu a není jej možné nijak zkopírovat. Přístup ke kartě je autentizován, tj. aplikace se musí procesoru na kartě nejprve prokázat znalostí příslušného PINu, který zadá uživatel. Je tak zabráněno zneužití informací z karty v případě její ztráty. Většina karet je konstruována tak, že se po zadání určitého počtu chybných PINů zablokuje a jedinou možností jak ji zprovoznit je její nová inicializace, která však nevratně smaže všechny informace na kartě.

Obrázek 2 Čtečka čipových karet

3.3.3 Čipové tokeny

Vedle čipových karet s čtečkami také existují čipové tokeny připojitelné do USB, které kombinují funkcionalitu karty a čtečky v jednom kusu hardware. Vzhledem se podobají

USB flash diskům, ale vnitřní architektura je totožná s čipovými kartami, tj. obsahují vlastní procesor a není možné přistupovat přímo k citlivým datům na tokenu. Výhodou tokenů je jejich vyšší mobilita, protože není potřeba s sebou nosit kartu i čtečku. Další výhodou je jejich tvar, protože vzhledem k jejich malé velikosti je lze připojit např. ke svazku klíčů, takže se snižuje riziko, že zůstanou zapomenuté v počítači.

Technologie čipových karet a tokenů výrazně zvyšují ochranu soukromých klíčů, protože umožňuje jejich bezpečné uložení a přístup k nim. Zavádí pojem tzv. dvoufaktorové autentizace (*two-factor authentication*), kdy uživatel musí prokázat znalost nějakého tajného kódu (tj. PINu k tokenu) a také fyzické držení tokenu.

Obrázek 3 USB čipový token

3.4 Autentizační kalkulátory

Skutečně univerzální řešení v oblasti autentizace uživatelů a ochrany přenášených dat představují autentizační kalkulátory, známé též pod názvy PIN kalkulátor, elektronický klíč či generátor jednorázových hesel. Vedoucí firmou na trhu těchto technologií je bezesporu společnost VASCO. Jedná se o zařízení, která umožňují ověření klienta a přenášené zprávy a splňují i nejvyšší nároky na bezpečnost.

Autentizační kalkulátory svým vzhledem nejčastěji připomínají běžné kalkulačky, existují však i v čistě softwarové formě.

Kalkulátor generuje posloupnost kódů v závislosti na interních parametrech kalkulátoru (unikátních pro každý kalkulátor). Obě komunikující strany znají interní parametry kalkulátoru, přičemž je zajištěno, že tyto parametry nejsou známy třetí straně. Na základě

předchozích kódů nelze (bez znalosti interních parametrů kalkulátoru) vypočítat (ani předpovědět) kód následující.

Odesilatel (klient) vygeneruje pomocí svého kalkulátoru autentizační kód, který předá příjemci (například bance). Autentizační server příjemce vypočte očekávaný kód a porovnáním ověří identitu odesilatele.

Použití autentizačního kalkulátoru je chráněno zadáním PIN. Takto je bráněno zneužití kalkulátoru v případě odcizení.

Obrázek 4 Autentizační kalkulátor

4 LOGICKÉ ZABEZPEČENÍ SÍTÍ

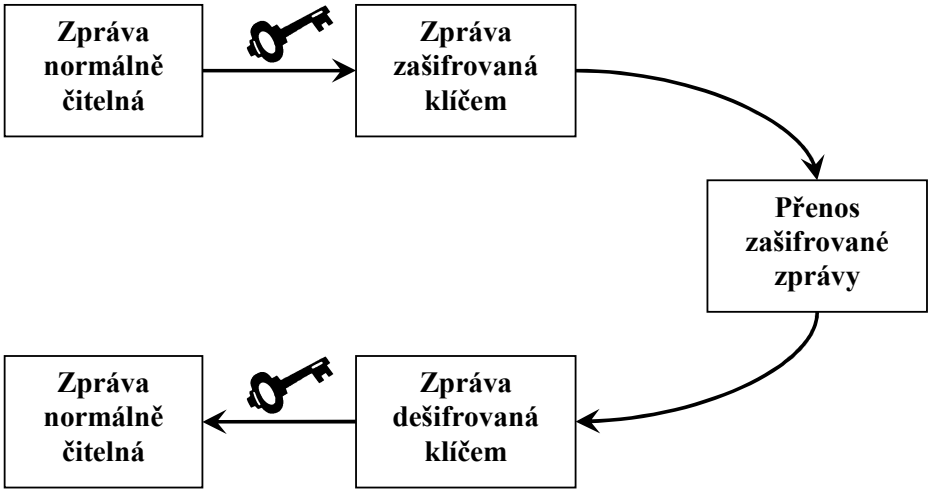
4.1 Šifrování

Šifra (nebo také šifrovací algoritmus) je matematická metoda, pomocí které se za „účasti“ šifrovacího klíče převede čitelný text do nečitelné podoby (šifrovaného textu).

K tomu, aby bylo možno zašifrovaný text převést zpět do otevřené (čitelné) podoby, musíme logicky kromě konkrétního použitého algoritmu znát také šifrovací klíč. Největším problémem tedy zpravidla není jak zprávu zašifrovat, ale jak adresátovi bezpečně předat potřebný klíč. I z tohoto důvodu byly postupem času vyvinuty dva druhy šifrovacích algoritmů: symetrické a asymetrické.

5 SYMETRICKÉ ŠIFROVÁNÍ

V případě symetrického šifrování se pro zašifrování i pro dešifrování dat používá jeden šifrovací klíč. Stejný klíč musí mít k dispozici všichni, kdo se šifrovanými daty pracují. Logicky tedy vyplývá potřeba zajistit jeho bezpečné předání určeným osobám. Ve chvíli, kdy dojde k jeho prozrazení byť jen jedinou zúčastněnou osobou, jsou všechny jím zašifrované informace prozrazeny. Mezi nejznámější symetrické šifrovací algoritmy patří DES, 3DES, IDEA, BlowFish a CAST.



Obrázek 5 Symetrické šifrování

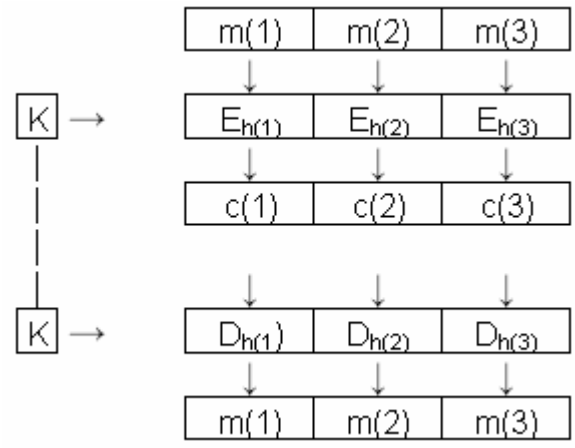
5.1 Proudové šifry

Citace: „Definice: Nechť **A** je abeceda q symbolů, nechť **M = C** je množina všech konečných řetězců nad **A** a nechť **K** je množina klíčů. Proudová šifra se skládá z transformace (generátoru) **G**, zobrazení **E** a zobrazení **D**. Pro každý klíč **k** náležící **K** generátor **G** vytváří posloupnost hesla **h(1), h(2)**, … , přičemž prvky **h(i)** reprezentují libovolné substituce **Eh(1), Eh(2),** … nad abecedou **A**. Zobrazení **E** a **D** každému klíči k náležící **K** přiřazují transformace zašifrování $\mathbf{E_k}$ a odšifrování $\mathbf{D_k}$. Zašifrování otevřeného textu **m = m(1), m(2),** … probíhá podle vztahu:

$$C(1) = E_{h(1)}(m(1)),\ c(2) = E_{h(2)}(m(2)) \quad (1)$$

a dešifrování textu **c = c(1), c(2)**, … probíhá podle vztahu:

$$m(1) = D_{h(1)}(c(1));\ m(2) = D_{h(2)}(c(2)),\ \text{kde}\ D_{h(i)} = E_{h(1)}^{-1} \quad (2)$$



Obrázek 6 Schéma proudové šifry

Využití proudových šifer je tam, kde do komunikačního kanálu přicházejí v pravidelném nebo nepravidelném intervalu jednotlivé znaky, které je nutné v daném okamžiku rychle zašifrovat a nelze tedy čekat na další znaky bloku. Proudové šifry používáme také u šifrovacího zařízení, které má malou paměť na průchozí data.

Velkou výhodou proti blokovým šifrám je, že v případě chyby jednoho znaku v komunikačním kanálu je rekonstrukce textu jednodušší, protože se chyba objeví pouze u jednoho znaku v tomto textu. U blokové šifry by se tato chyba projevila na celém bloku znaků.

5.2 XOR

XOR je zkratka pro exkluzivní disjunkci (někdy též nonekvivalence, exkluzivní OR) je to logická operace, jejíž hodnota je pravda, pravě když se vstupní hodnoty liší. XOR se používá jako jedna z nejjednodušších šifrovacích algoritmů.

Tabulka 1 Logická operace XOR

x	**y**	**x** XOR **y**
0	0	0
0	1	1
1	0	1
1	1	0

Šifrování provádíme tak, že si zvolíme periodický klíč (heslo), které pak aplikujeme metodou XOR na proud zprávy, kterou chceme zašifrovat a tím nám vznikne zašifrovaná zpráva. Následné dešifrování se pak provádí stejným způsobem.

5.2.1 Příklad šifrování metodou XOR:

Zvolíme si periodický šifrovací klíč: 1011001110

Zpráva, kterou chceme zašifrovat: 10100010101011011101010100100 1010

Šifrování je znázorněno v tabulce:

Tabulka 2 Příklad šifrování metodou XOR

Zpráva	1	0	1	0	0	0	1	0	1	0	1	0	1	1	0	1	1	1	0	1	0	1	0	1	0	0	1	0	0	1	0	1	0
Heslo	1	0	1	1	0	0	1	1	1	0	1	1	0	1	1	0	0	1	1	1	0	1	1	0	1	1	0	0	1	1	1	0	1
Šifr. zp.	0	0	0	1	0	0	0	1	0	0	0	1	1	0	1	1	1	0	1	0	0	0	1	1	1	1	1	0	1	0	1	1	1
Heslo	1	0	1	1	0	0	1	1	1	0	1	1	0	1	1	0	0	1	1	1	0	1	1	0	1	1	0	0	1	1	1	0	1
Zpráva	1	0	1	0	0	0	1	0	1	0	1	0	1	1	0	1	1	1	0	1	0	1	0	1	0	0	1	0	0	1	0	1	0

Z hlediska bezpečnosti záleží hlavně na délce klíče (hesla). Je nutné, aby klíč nebyl moc krátký, protože pak by se častěji opakoval a některé části textu by byly zašifrovány stejným způsobem. To by pak následně zjednodušilo případnou kryptoanalýzu.

5.3 Vermanova šifra

Vermanova šifra je pojmenovaná po Gilbertu Vermanovi, který ji nechal v roce 1917 patentovat pro ochranu telegrafických zpráv. Navrhl ji však krátce po první světové válce major americké armády Joseph Mauborgn. Tato šifra šifruje otevřený text stejně dlouhým náhodně vygenerovaným heslem, které se po použití zničí, takže je zaručeno, že nikdy nebudou dva různé texty zašifrovány stejným heslem.

Potřebujeme mít klíče stejně dlouhé, jako šifrovaná zpráva a klíč použijeme jen jednou. To nám zaručí, že je tento kryptosystém absolutně bezpečný. Můžeme proto použít nějaký jednoduchý šifrovací algoritmus, dost často se používá logická funkce XOR.

5.3.1 Příklad šifrování Vermanovou šifrou

Nejprve potřebuji dvě zprávy stejné délky a také klíč stejné délky. Pak spočítám:

$$K_A = A \text{ xor } K \text{ a } K_B = B \text{ xor } K \tag{3}$$

$$X = A \text{ xor } B \text{ a } Y = X \text{ xor } K \tag{4}$$

Z toho plyne:

$$A = Y \text{ xor } K_B \tag{5}$$

$$B = Y \text{ xor } K_A \tag{6}$$

Při dešifrování zprávy Y klíči K_A a K_B dostaneme dvě různé zprávy. Tím můžeme zmást nepřítele, například mu podstrčíme jeden z dešifrovacích klíčů.

Důkaz absolutní bezpečnosti:

Definice: abychom mohli šifru označit za absolutně bezpečnou musíme dokázat, že šifrovaný text nenese žádnou informaci o otevřeném textu.

Citace:

„Nechť h(i), o(i) a c(i) jsou po řadě bit hesla, otevřeného a šifrovaného textu.

Máme P{o(i) = 0} = P{c(i) – h(i) = 0} = P{h(i) = c(i)}.

Tento výraz je roven

P{h(i) = 0}, v případě, že c(i) = 0

P{h(i) = 1}, v případě, že c(i) = 1.

Protože P{h(i) = 0}= P{h(i) = 1} = ½, je v obou případech výraz roven ½, tedy celkově P{o(i) = 0} = ½. Podobně ukážeme, že P{o(i) = 1} = ½ nezávisle na hodnotě šifrovaného textu.“

Největší bezpečnostní riziko tak vyplývá z uložení příliš velkého klíče, což je nevýhoda tohoto algoritmu.

5.4 Blokové šifry

Citace:

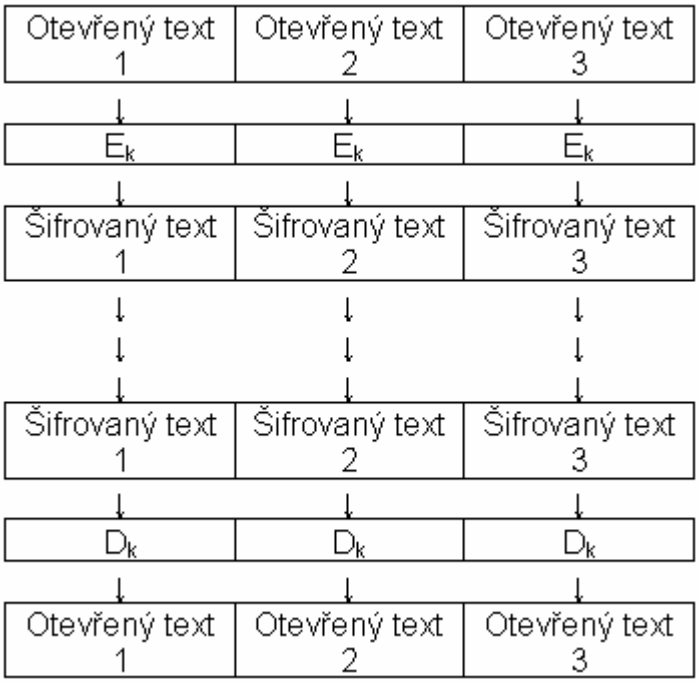
„Definice: Nechť A je abeceda q symbolů, t náleží N a M = C je množina všech řetězců délky t nad A. Nechť K je množina klíčů. Bloková šifra je šifrovací systém (M,C,K,E,D), kde E a D jsou zobrazením, definující pro každé k náleží K transformaci zašifrování E_k a dešifrování D_k tak, že zašifrování bloků otevřeného textu m(1), m(2), m(3), … (kde M(i) náleží M pro každé N) probíhá podle vztahu:

$$C(i) = E_k(m(i)) \text{ pro každé } N \tag{7}$$

a dešifrování podle vztahu:

$$m(i) = D_k(c(i)) \text{ pro každé i náleží } N. \tag{8}$$

Podstata blokové šifry je v tom, že se otevřený text rozloží na jednotlivé bloky a tyto bloky jsou pak šifrovány stejnou transformací. Při dešifrování jsou opět jednotlivé bloky dešifrovány stejnou transformací.



Obrázek 7 Schéma blokové šifry

Základní význam pro bezpečnost celého algoritmu je velikost vstupního bloku blokové šifry, protože blokové šifry zašifrují najednou celý blok. Při malé velikosti vstupního bloku by bylo možné vytvořit něco jako slovník, to znamená vytvořit za použití určitého klíče seznam vstupních a jim odpovídajících výstupních hodnot algoritmu. To by značným způsobem snížilo bezpečnost celého algoritmu. Proto se doporučuje volit dostatečně velkou velikost prvního bloku, aby pak slovník vytvořit nešel. Například při zvolení prvního bloku o velikosti 32 bitů by musel slovník obsahovat 2^{32} slov. Což je řádově 4 miliardy výrazů. V praxi se používá se spíše 64 bitová délka prvního bloku.

5.5 DES

DES - Data Ecryption Standart. Byla vyvinutá v 70. letech. V roce 1977 byla zvolena za standard (FIPS 46) pro šifrování dat v civilních státních organizacích v USA a následně se rozšířila i do soukromého sektoru. Je to pravděpodobně nejznámější šifra, která byla standardem více jak 20 let. Jedná se o blokovou šifru, která je v současnosti již zastaralá, protože používá klíč o délce jen 56bitů, který lze v dnešní době prolomit hrubou silou za

24hodin, ale přesto se ještě někde používá. DES má dnes spíše historický význam, ale stal se vzorem a inspirací pro spoustu dnes používaných algoritmů.

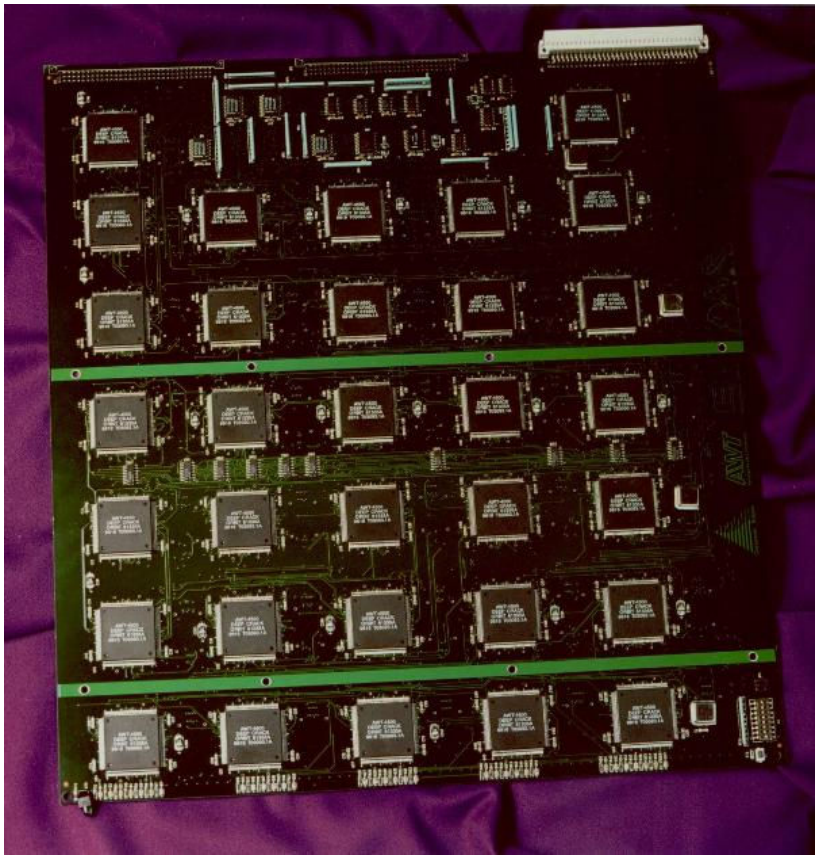
Jak už bylo popsáno víš, DES používá klíč dlouhý 56 bitů, někdy se udává 64 bitů. V takovém případě se nejnižší byt v bajtu považuje za licho paritu od horních sedmi bitů. Celá bezpečnost šifry je založena na síle klíče, proto je nutné výběru správné klíče věnovat čas a pozornost. Při výběru se doporučuje vyloučit tzv. slabé klíče.

DES používá k šifrování bloky o délce 64bitů. Při šifrování se stále opakují dvě operace a to substituce a permutace, které se opakují v každém cyklu. Těch má algoritmus DES 16, z nichž každý se skládá z jednoduchých aritmetických operací. Pro vlastní operace se 64 bitové bloky rozdělují na dvě 32 bitové části. Tyto části se znovu spojí až po skončení posledního cyklu.Nakonec je celý blok podroben transformaci.

5.5.1 Kryptoanalýza DES

Největší slabinou algoritmu DES je v dnešní moderní době již příliš krátký klíč. V průměrném případě nám k nalezení klíče hrubou silou, například lineární nebo diferenciální kryptoanalýza, která se už v praxi vyzkoušela a byla úspěšná, stačí vyzkoušet 2^{55} možností.

V roce 1998 byl sestrojen luštící stroj DES-Cracker za cenu asi 250 milionů dolarů, který je schopen na šifrovaném textu ověřit 2^{56} klíčů. Tento stroj má v sobě 1856 čipů, které zkouší kíče z různých částí klíčového prostoru. Rychlost tohoto stroje je 90 miliard zkoušek klíčů za sekundu. K prozkoumání všech 2^{56} klíčů mu tak stačí 9 dní. (na obrázku je jedna z 29 desek stroje DES-Cracker)



Obrázek 8 Jedna z 29 desek stroje DES-Cracker

5.6 TripleDES

Slabinou algoritmu DES byl krátký (slabý) klíč. To se vyřešilo algoritmem TripleDES. Jedná se o algoritmus DES aplikovaný 3x po obě s třemi různými klíči. Výsledná délka klíče je pak 3x56 = 168bitový klíč. TripleDES se již považuje za spolehlivý.

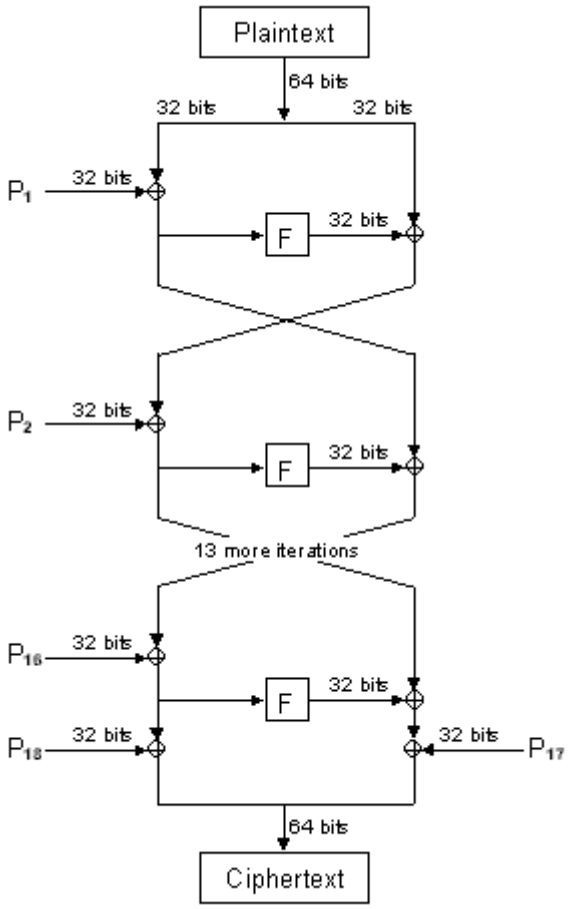
Obrázek 9 Schéma šifrování TripleDES

5.7 Blowfish

Šifru Blowfish navrhl B. Schneier a poprvé ji publikoval v roce 1993. Šifra je zcela volná – nepatentovaná, nelicencovaná a bez copyrightu. Podle autora to měla být alternativa k algoritmu DES. Přestože byla tato šifra poskytnuta veřejnosti a měla k ní tedy přístup celá řada cryptoanalytiků, doposud není veřejně znám případ prolomení této šifry v podobě, v jaké byla definována.

Blowfish pracuje s bloky o velikosti 64 bitů a stejně jako DES je při svých operacích rozděluje na dva 32bitové subbloky a používá klíče o velikosti maximálně 448 bitů.

Při inicializaci šifry se nejprve vytvoří 1042 32 bitových polí, které pak postupně nahrazujeme vždy 64 bitů tohoto pole. Z toho vyplývá, že pro náhradu celého pole budeme potřebovat 1042/2 = 521 kroků. Každý krok je modifikován zadaným klíčem a sledně šifrován algoritmem Blowfish. Následné šifrování již probíhá po 64 bitech. Abychom dostali zašifrovaný text, musí se na každých 64 bitů textu použít 18x algoritmus Blowfish. Blowfish používá k šifrování operace XOR a Sčítání modulo 2^{32}.



Obrázek 10 schéma šifrování Blowfish

Vstupem (označujme ho x) je 64-bitové slovo, které se rozdělí na dvě 32-bitová slova xL a xR (xL zahrnuje bity 32..63, xR pak bity 0..31 vstupu x). Šifrování probíhá v 16-ti rundách, což můžeme zapsat následujícím cyklem:

for i = 1 to 16 do

begin

xL = xL XOR Pi

xR = F(xL) XOR xR

swap xL, xR {provede záměnu obou parametrů}

end;

Po tomto cyklu následuje ještě tato série příkazů:

swap xL, xR {odstraní poslední swap v cyklu}

xR = xR XOR P17

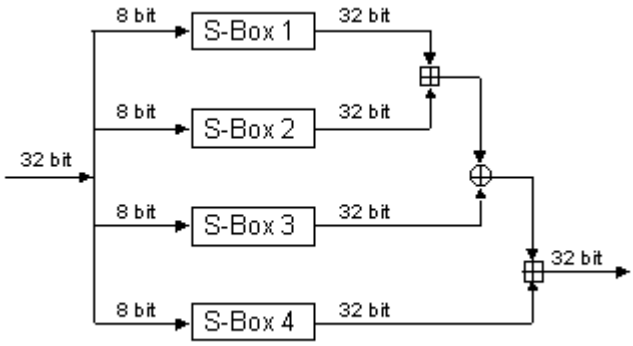
xL = xL XOR P18

Posledním krokem je spojení xL a xR do výstupního 64-bitového bloku zašifrovaného textu.

Dešifrování pak probíhá přesně opačným způsobem.

Funkce F rozdělí 32-bitové vstupní slovo y na 4 čtvrtiny a, b, c, d. Tyto části po řadě představují jednotlivé byty (tj. 8 bitů) vstupního slova zleva doprava (tj. a představuje bity 24..31, b bity 16..23, atd.) a používají se jako indexy do S-boxů. Výstupní hodnota funkce je pak definována následovně:

$$F(y) = ((S1,a + S2,b \bmod 232) \text{ XOR } S3,c) + S4,d \bmod 232 \quad (9)$$



Obrázek 11 Grafické vyjádření funkce F

Ještě před šifrováním, nebo dešifrováním šifrou Blowfish je potřeba vygenerovat velké množství podklíčů, které tato šifra potřebuje ke své činnosti. Tyto podklíče jsou pak uloženy v pěti polích označovaných jako P-pole, nebo P-box. Je jich celkem 18, každé pole má 32 bitů. Označují se pak P1, P2, … P18. Ostatní pole se označují jako S-pole, nebo S-box. Těch je celkem 256 a každé pole má opět 32 bitů. Označují se Si,0, Si,1, Si,255, kde i=1,2,3,4.

5.7.1 Generování podklíčů

Citace:

1. Inicializace P-boxu a S-boxů pomocí pevně definovaného řetězce, který tvoří desetinná část čísla p v hexadecimálním zápise. Inicializace probíhá v tomto pořadí: P1, P2,…, P18, S1,0, S1,1,…, S1,255, S2,0, S2,1,…,S2,255, S3,0, S3,1,…, S3,255, S4,0, S4,1,…, S4,255.
2. XOR P1 s prvními 32 bity klíče, XOR P2 s dalšími 32 bity klíče, a tak pokračujeme dále pro všechny bity klíče (což nám při nejdelším možném klíči vyjde až na P14). Pak opakujeme stejný postup pro zbývající položky P-boxu s cyklickým procházením bitů klíče.
3. Nyní vezmeme podklíče vytvořené v P-boxu pomocí předchozích kroků a aplikujeme Blowfish-algoritmus šifrování na nulový řetězec (tj. 64-bitové vstupní slovo pro algoritmus má všechny bity nulové).
4. Výsledek předchozího kroku (tj. 64-bitové výstupní slovo z algoritmu) použijeme k náhradě 64 bitů tvořených P1 a P2.
5. Výstup kroku (3) zašifrujeme pomocí Blowfish-algoritmu (nyní již s pozměněnými podklíči v P1 a P2).
6. Nahradíme P3 a P4 výstupem z kroku (5).
7. Tímto způsobem (tj. šifrový výstup Blowfish-algoritmu použijeme k náhradě dalších podklíčů a znovu zašifrujeme) pokračujeme v nahrazování dalších podklíčů v P-boxu a pak v jednotlivých S-boxech.

Bezpečnost šifry Blowfish je založena na délce použitého klíče. Také záleží na počtu kol šifrovacího procesu. Při snížení počtu kol se zvýší rychlost šifrování, ale zvýší se i riziko prolomení kryptoanalýzou. Naopak při zvýšení počtu kol se sníží rychlost šifrování, avšak riziko se zásadním způsobem nesníží. Velká výhoda této šifry je, že není patentovaná ani jinak licencovaná, čili je volně k použití.

5.7.2 Kryptoanalýza šifry Blowfish

Jediný způsob, jak prolomit tento algoritmus je hrubou silou. Při použití nejvyšší možné délky klíče, to je 448 bitový klíč, by bylo nutné vyzkoušet 2^{448} možných kombinací.

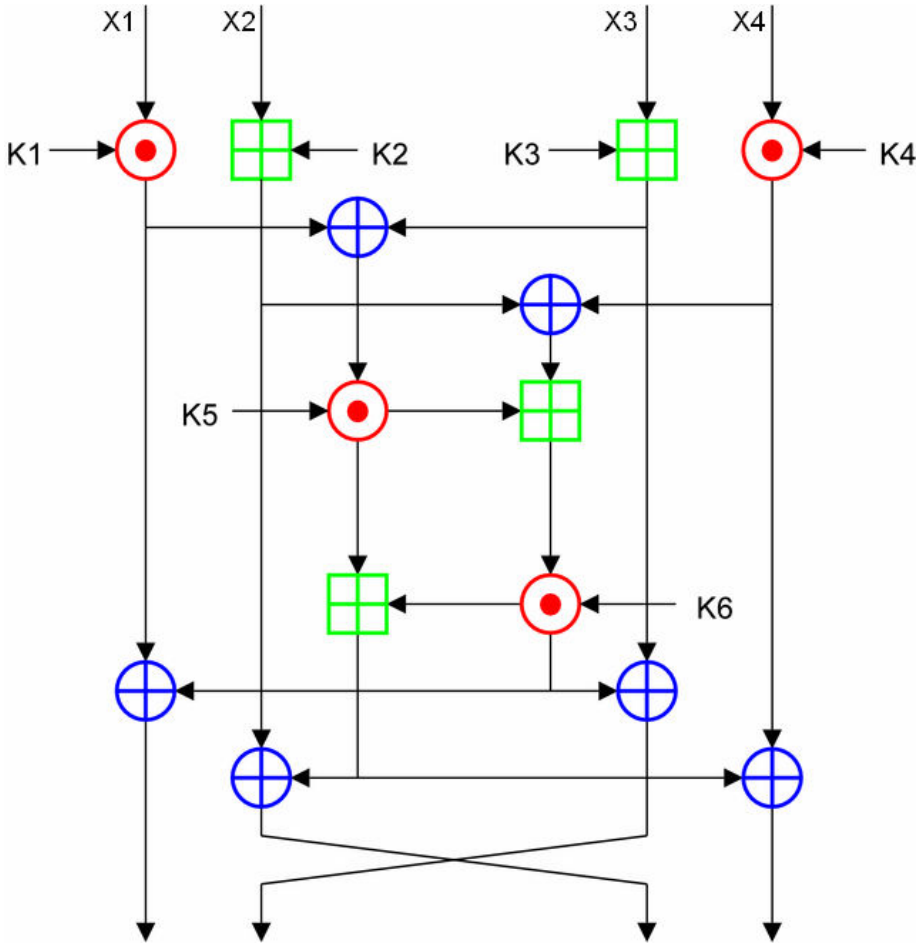
5.8 IDEA

International Data Encryption Algorithm (IDEA, „Mezinárodní algoritmus pro šifrování dat“) je bloková šifra, kterou navrhli Xuejia Lai a James L. Massey ze Švýcarského národního technologického institutu (ETHZ) v Zürichu. IDEA je patentována v Rakousku, Francii, Německu, Itálii, Holandsku, Španělsku, Švédsku, Švýcarsku, Spojeném království (Evropský patent EP-B-0482154), Spojených státech (americký patent #5,214,703) a Japonsku (JP 3225440). Ale je volně dostupná pro nekomerční použití. Poprvé byla popsána v roce 1991. Tento algoritmus měl nahradit Data Encryption Standard. IDEA je drobným přepracováním dřívější šifry PES (Proposed Encryption Standard), původně se nazývala IPES (Improved PES). IDEA je vylepšena, aby odolala moderním kryptoanalytickým útokům. Je založená na kombinování různých matematických operací. IDEA pracuje s bloky o velikosti 64 bitů, které dělí na subbloky o velikosti 16 bitů. Používá klíč o velikosti 128 bitů. Skládá se z řady osmi identických transformací a vstupní transformace (poloviční průchod). Šifrování i dešifrování probíhá podobně. IDEA střídá operace z různých skupin, které jsou v jistém smyslu algebraicky neslučitelné. Tyto tři základní operace pracující s 16 bitovými řetězci jsou:

* bitová nonekvivalence XOR (na obrázku znázorněno $\oplus$),

* sčítání modulo 2^{16} (znázorněno $\boxplus$),

* násobení modulo $2^{16}+1$ (znázorněno $\odot$).



Obrázek 12 Schéma šifrování IDEA

Systém algoritmu je řešen tak, že výstup z operace jednoho typu není nikdy použit ke vstupu operace stejného typu.

Šifrování:

Každý 64bitový blok je rozdělen na 4 subbloky X1, X2, X3, X4. V každém cyklu probíhá několik operací, nakonec se zamění 2. a 3. subblok. Během šifrování je použito 52 subklíčů (6 pro každý cyklus K1, K2, K3, K4, K5, K6 a 4 pro závěrečnou transformaci) které získáme rozdělení hlavního 128 bitového klíče na 8 16-bitových subklíčů. V každém cyklu je použito 6 subklíčů. Po ukončení cyklu je hlavní klíč otočen o 25 míst a pak znova rozdělen na 8 subklíčů.

Popis operací v každém cyklu:

Citace:

1. X^1 vynásob s K^1
2. X^2 sečti s K^2
3. X^3 sečti s K^3
4. X^4 vynásob s K^4
5. výsledek kroku 1 xoruj s výsledkem kroku 3
6. výsledek kroku 2 xoruj s výsledkem kroku 4
7. výsledek kroku 5 vynásob s K^5
8. výsledek kroku 6 sečti s výsledkem kroku 7
9. výsledek kroku 8 vynásob s K^6
10. výsledek kroku 1 sečti s výsledkem kroku 9
11. výsledek kroku 1 xoruj s výsledkem kroku 9
12. výsledek kroku 3 xoruj s výsledkem kroku 9
13. výsledek kroku 2 xoruj s výsledkem kroku 10
14. výsledek kroku 4 xoruj s výsledkem kroku 10

Výstupem tohoto cyklu jsou pak výsledku kroků 11, 12, 13 a 14. Subbloky 2 a 3 se mezi sebou zamění, čili vstupem pro další cyklus jsou výsledky kroků 11, 13, 12 a 14. Tento postup se pak ještě 7krát opakuje. Po posledním opakování se provede konečná transformace:

1. X^1 vynásob s K^1
2. X^2 sečti s K^2
3. X^3 sečti s K^3
4. X^4 vynásob s K^4

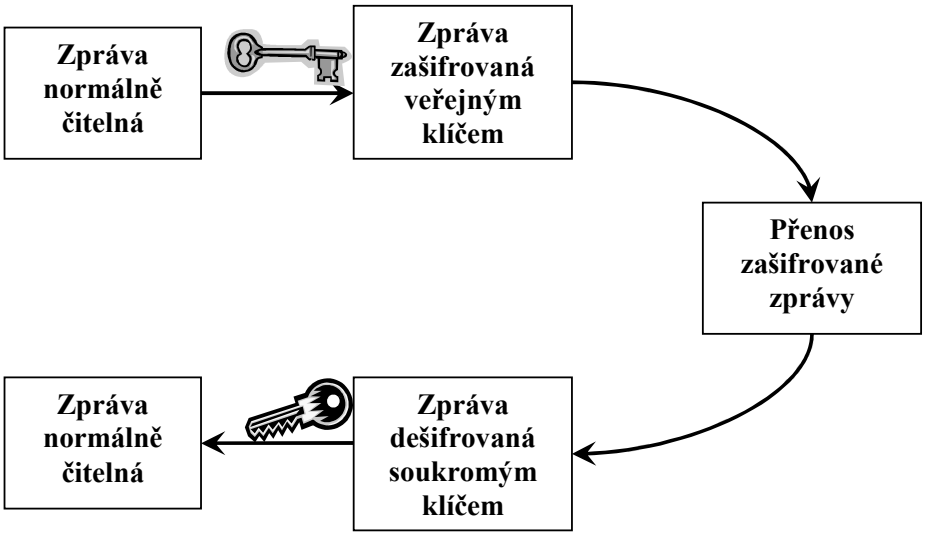
Nakonec se výsledné subbloky spojí v jeden 64 bitový zašifrovaný text. Dešifrování se provádí stejným způsobem, pouze použití klíče je odlišné.

5.8.1 Kryptoanalýza algoritmu IDEA

Návrháři analyzovali šifrování pomocí IDEA, aby zjistili jeho odolnost vůči diferenční kryptoanalýze a usoudili, že šifra je za jistých předpokladů odolná. Žádná úspěšná lineární nebo algebraická slabost nebyla zjištěna. Nejlepší způsob kryptoanalýzy je v dnešní době použití hrubé síly. Protože IDEA používá 128 bitový klíč, bylo by nutné vyzkoušet 2^{128} možných kombinací. Proto se dá šifra IDEA označit za bezpečnou.

6 ASYMETRICKÉ ŠIFROVÁNÍ

Při asymetrickém šifrování je situace poněkud složitější. Místo jediného klíče zde totiž používáme tzv. klíčový pár, který se skládá z klíče veřejného a soukromého. Veřejný klíč (jak již jeho název napovídá) je určen k volnému šíření a je distribuován všem osobám, se kterými komunikujeme. Naproti tomu soukromý klíč musí zůstat přísně utajen.To, co bylo zašifrováno veřejným klíčem, lze dešifrovat pouze soukromým a naopak. Jeden jediný klíč nelze použít k zašifrování i opětovnému dešifrování. Asymetrické šifrovací algoritmy jsou v porovnání se symetrickými obecně výrazně pomalejší. V praxi se nejčastěji používá algoritmus RSA a algoritmy na bázi eliptických křivek (ECC).



Obrázek 13 Asymetrické šifrování

6.1 RSA

RSA – název je odvozen od jmen jeho autorů – Ron Rivest, Adi Shamir a Joe Adleman. Autoři tento algoritmus objevili roku 1977. Princip tohoto systému je jednoduchý. Vynásobíme dvě prvočísla (100místná i vícemístná), výsledkem je pak součin, který použijeme jako veřejný klíč. Bez znalosti obou prvočísel je téměř nemožné provést rozklad na původní prvočísla. Bez původních prvočísel nelze provést dešifrování. Bezpečnost RSA spočívá v tom, že není znám rychlý algoritmus na faktorizaci, což je rozklad čísla na dvě

prvočísla. Hledání dostatečně velkých prvočísel pro tvoření klíčů by bylo dosti pomalé, proto se hledají čísla, která jsou prvočísla s velmi velkou pravděpodobností.

6.1.1 Vygenerování páru veřejný — soukromý klíč

Postup:

1. Zvolíme si dvě různá velká náhodná prvočísla **p** a **q**.
2. Spočítáme jejich součin **n = pq**.
3. Spočítáme hodnotu Eulerovy funkce **φ(n) = (p − 1)(q − 1)**.
4. Zvolíme celé číslo **e** menší než **φ(n)**, které je s **φ(n)** nesoudělné.
5. Nalezneme číslo **d** tak, aby platilo **de ≡ 1 (mod φ(n))**.

Veřejný klíč je pak dvojice **n** a **e** (**n** se označuje jako modul, **e** jako exponent). Soukromý klíč je dvojice **n** a **d** (**d** se označuje jako dešifrovací).

Prvočísla **p** a **q** už nebudeme potřebovat, proto je bezpečně zničíme.

6.1.2 Příklad šifrování

Potřebujeme zašifrovat zprávu **M = 123**

1. dvě prvočísla zvolíme například **p = 29 a q = 19**
2. jejich součin **n = 551**
3. hodnota Eulerovy funkce **φ(n) = (29 − 1)(19 − 1) = 504**
4. **e = 17**
5. **$d = 17^{-1}$ mod504 = 89**
6. vypočítáme zašifrovanou zprávu: **$c = 123^{17}$ mod 551= 169**
7. při dešifrování počítáme: **$m = 169^{89}$ mod 551 = 123**

Na příkladu je vidět, že i za použití malých prvočísel p a q byl výpočet velmi náročný. Při použití velkých prvočísel, 100 a více místných, početní náročnost velmi vzroste. To dělá

algoritmus RSA velmi pomalý, i v době dnešní poměrně rychlé výpočetní techniky. To značně omezuje jeho použití v praxi. Výpočet je možno mírně zjednodušit použitím nižšího čísla exponentu **e**.

6.1.3 Generování prvočísel

Volba správných prvočísle značně ovlivňuje bezpečnost celého systému RSA, proto by jsme měli věnovat pozornost volbě těchto čísel. Prvočísla by měla mít následující vlastnosti:

1. Měla by být přibližně stejné délky, ale zároveň by měla být odlišná.
2. Měla by splňovat určitá doporučení, které znesnadní použití existujících faktorizačních algoritmů.
3. Nejlepší je používat silná prvočísla

Silná prvočísla mají následující vlastnosti:

- prvočíselný rozklad čísel $\mathbf{p \pm 1}$, $\mathbf{q \pm 1}$, $\mathbf{p - 2}$ a $\mathbf{q - 2}$ by neměl obsahovat malá čísla
- $p - 1/2$ a $q - 1/2$ by měla být prvočísla

Pro generování prvočísel existují efektivní algoritmy, které nám vygenerují náhodné x-bitové prvočíslo. Takový algoritmus nejprve vygeneruje náhodné x-bitové prvočíslo p. Na tomto prvočísle pak nastaví první a poslední bit na hodnotu 1. To nám zaručí, že číslo bude liché a bude x-bitové. Poté se provede kontrola, pro všechna prvočísla menší než 2000 a naše prvočíslo p, jestli platí nejmenší společný dělitel 1. V případě, že neplatí, musíme se vrátit na začátek a generovat prvočíslo p znovu. V případě, že tato podmínka platí použijeme speciální pravděpodobnostní algoritmus na testování prvočísel. Tyto algoritmy nám určují, zda jde o prvočíslo s určitou pravděpodobností. Tuto pravděpodobnost lze snížit na minimum tím, že algoritmus několikrát opakujeme. Například máme algoritmus s úspěšností 50%. Už při 10 opakování se pravděpodobnost, že jde o prvočíslo zvýší na 99,99%.

Zatím největší známé prvočíslo objevili vědci Curtis Cooper a Steven Boone z univerzity ve Warrenburgu v americkém státě Missouri. S pomocí 700 osobních počítačů propojených

do sítě. Toto prvočíslo je $2^{30402457}$-1. Pro běžný počítač je nemožné takové číslo vypočítat v reálném čase. Takový výpočet by trval přibližně 4500let.

6.1.4 Bezpečnost RSA

Je spousta důvodů si myslet, že je algoritmus RSA bezpečný. Vědci dokázali, že získání soukromého klíče z veřejného je složité stejně jako faktorizovat **n**, tj. rozložit číslo na dvě prvočísla, jejichž součinem je **n**. V tom je taky hlavní síla tohoto kryptosystému. K získání dešifrovacího exponentu **d** je nutné znát hodnotu Eulerovy funkce $\varphi(n) = (p-1)(q-1)$ a tu nelze vypočítat bez faktorizace n. Číslo n potenciální útočník zná, neboť je součástí veřejného klíče. Bezpečnost RSA by mohl vážně ohrozit jen náhlý pokrok v teorii čísel, který by umožňoval faktorizaci velkých čísel. Algoritmus RSA je vystaven již po mnoho let mnoha kryptoanalýzám, takže můžeme věřit, že zůstane bezpečný i a na dále. Podmínkou je však vhodná velikost prvočísel **p** a **q**.

Jak už bylo popsáno výše, bezpečnost celého systému je založena na faktorizaci čísla n. Rizikem je proto i stálý pokrok ve výpočetní technice, která by časem mohla umožnit faktorizaci velkého čísla.

Bezpečnost algoritmu RSA však nezávisí jen na délce klíče, ale taky na jeho správné implementaci a mnoha dalších věcech. Útoky jsou většinou vedeny na nejslabší místo kryptosystému, kterým zpravidla bývá špatná implementace.

II. PRAKTICKÁ ČÁST

7 NÁVRH ZABEZPEČENÍ VNITŘNÍ SÍTĚ

Máme k dispozici jednoduchou vnitřní síť, která velikostně odpovídá síti LAN (Local Area Network). Tato síť se rozkládá v jedné budově. K síti je připojeno celkem 10 stolních počítačů, 2 tiskárny a jedna kopírka. Jedná se o vnitřní síť, s připojením do sítě internet tedy nepočítáme. K propojení všech počítačů byly použity kabely typu UTP zakončené koncovkou RJ45. Pro vedení kabelů mezi počítači se používáme hvězdicovou topologii. Od síťové karty každého počítače vede kabel do koncentrátoru. V našem případě to bude switch. Jelikož síť je v dvoupatrové budově, bude výhodnější použít dva koncentrátory, v každém patře jeden. Kabely můžeme vést po okrajích místnosti nebo mezi stoly a podobně. Bezpečnější způsob je však pomocí krycích lišt na zdech nebo v stropních podhledech. V takovém případě je zakončení kabelů pevná zásuvka se zdířkami RJ45. Z těchto zásuvek pak vedou kratší kabely přímo do síťové karty počítače. Je to sice nákladnější řešení, ale je spolehlivější Maximální vzdálenost kabelu mezi koncentrátorem a síťovou kartou počítače je 100m. V našem případě budou tyto vzdálenosti daleko menší.

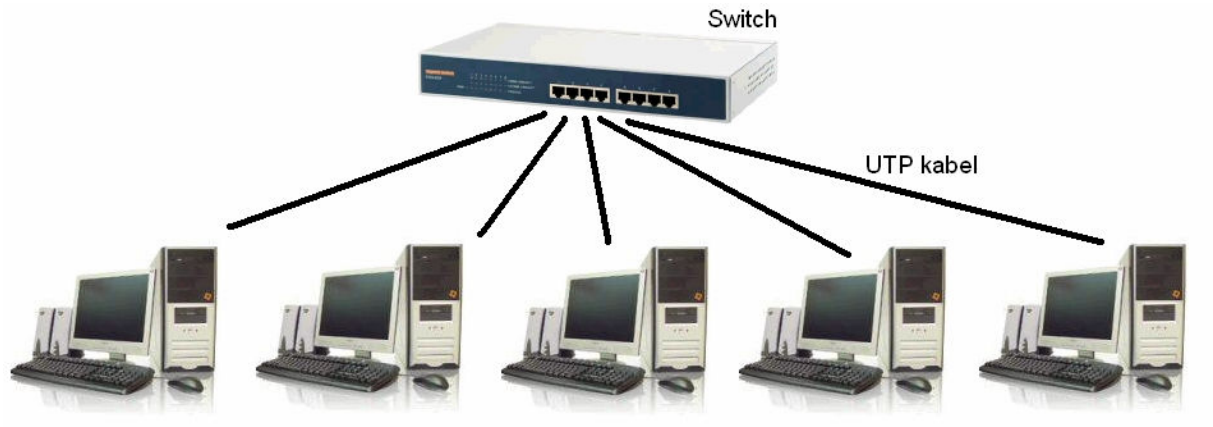
7.1 Rychlost přenosu

V sítích Ethernet, které jsou řešeny kabeláží UTP se můžeme setkat se dvěma přenosovými rychlostmi. Starší sítě měli rychlost 10Mb/s, dnešní standart je 100Mb/s.

Naše síť je moderní, poběží tedy na rychlosti 100Mb/s. Abychom této rychlosti dosáhli, je nutné volit všechny prvky naší sítě se stejnou rychlostí. To znamená, že všech 20 počítačů musí mít síťové karty s rychlostí 100Mb/s. Taky oba koncentrátory musí podporovat rychlost 100Mb/s.

7.2 Switch

Je to síťový přepínač. Kabely od síťových karet počítačů budou směřovat právě do něj. Říká se mu také „inteligentní přepínač“, protože při průchodu paketu si přečte cílovou adresu a data pošle právě tomu počítači, pro který jsou tyto data určená. Adresy připojených počítačů si switch získává automaticky. Výhodou switche je výrazně větší propustnost, než třeba u hubu, kde může docházet k zahlcení sítě.



Obrázek 14 Schématický nákres propojení počítačů se switchem

7.2.1 Propojení dvou switchů

Pokud chceme propojit dva koncentrátory, v našem případě switche, uděláme to pomocí UTP kabelu, který připojíme u prvního switche do zdířky UPLink a do druhého switche kabel zapojíme do jakékoliv jiné číselně označené zdířky. Nesmíme však kabel zapojit do obou switchů do zdířky UPLink.

Obrázek 15 Schématický nákres propojení dvou switchů

7.3 Paket

Data jsou v síti přenášena pomocí malých paketů, balíčků. Soubor, který chceme přenést je rozkouskován do malých přepravních jednotek – do paketů.Toto rozkouskování dělá z částí

síťová karta a z části software. Při doručení všech paketů je pak v cílovém počítače opět složen původní soubor.

Adresy jednotlivých počítačů jsou vlastně adresami jejich síťových karet. Každá síťová karta má již z výroby originální MAC adresu (Media Access Control Address).

Obrázek 16 Paket

7.4 Nastavení síťových vlastností v softwaru

Předpokládáme, že máme v každém počítači nainstalovanou síťovou kartu. A všechny počítače jsou správně propojeny s oběma koncentrátory. Do každého počítače nainstalujeme operační systém Windows XP Professional, který má lepší bezpečností prvky než XP Home.

Protože se jedná o malou vnitřní síť, použijeme systém sítí „peer to peer“ volně přeloženo do češtiny to znamená „rovný s rovným“. Všechno, co jednotlivé počítače sdílí, ať už to jsou data, nebo třeba tiskárny je dostupné pro všechny ostatní počítače v této síti. Počítače jsou si vzájemně rovné.

Ve složitějších sítí se používá systém „klient-server“ Zde jsou všechny data soustředěna na server a všechny ostatní počítače se připojují právě k tomuto serveru.

7.5 Síťové protokoly

K tomu, aby mezi sebou počítače uměly komunikovat potřebují mít nastavený stejný „jazyk“, odborně se tomu říká síťový protokol. Síťových protokolů existuje celá řada, například NetBEUI, IPX/SPX, TCP/IP… Nejpoužívanějším protokolem je TCP/IP. Tento protokol aplikujeme také na naši síť. Tento protokol je součástí operačního systému Windows.

7.5.1 Protokol TCP/IP

Skládá se ze dvou základních protokolů:

1. IP (Internet Protocol) – Posílá pakety na adresy zapsané v hlavičce paketu. Doručení však již neověřuje.
2. TCP (Transmission Control Protocol) – Dělí data na jednotlivé pakety, potvrzuje příjem dat, v případě nedoručení si vyžádá odeslání chybějících paketů. Spojení navazuje prostřednictvím adres a portů umístněných na každém počítači.

7.5.2 Adresy TCP/IP

Pro správné fungování protokolu TCP/IP je nutné, aby měl každý počítač v naší síti svoji jedinečnou adresu. Tyto adresy musíme přiřadit ručně. U velkých sítí se používá automatické přidělování adres DHCP (Dynamic Host Configuration Protocol). K tomu však potřebujeme server. Někdy tato funkce bývá integrovaná do koncentrátoru.

Adresa je tvořená čtyřmi trojciferných čísli oddělenými tečkou. Trojciferné čísla mohou nabývat hodnot 0-255. Adresa nepopisuje jen počítač, ale je z ní možné vyčíst i část sítě a podobně. To se však využívá až u složitějších sítí.

IP adresa se tedy skládá s adresy sítě a adresy počítače. Adresy jsou rozděleny do tříd, které se liší počtem číslic vyhrazených pro adresu sítě a adresu počítače. Základním znakem každé třídy je první trojčíslí:

Tabulka 3 Třídy adres TCP/IP

	Rozsah adres Prvního trojčíslí	Počet čísel vyhrazených pro adresu sítě	Umožňuje adresovat [sítí]	Počet čísel vyhrazených pro adresu uzlu	Umožňuje adresovat [uzlů]
Třída A	0-127	1	126	3	17 milionů
Třída B	128-191	2	16 tisíc	2	65 tisíc
Třída C	192-223	3	2 miliony	1	254

V sítích LAN pro soukromé účely můžeme použít následující adresy:

Třída A: 10.0.0.0 až 10.255.255.255

Třída B: 172.16.0.0 až 172.31.255.255

Třída C: 192.168.0.0 až 192.168.255.255

V naší síti použijeme třídu C a nastavíme IP adresy na hodnoty: 192.168.1.1 až 192.168.1.10

Maska podsítě se automaticky nastaví na 255.255.255.0

Výchozí bránu můžeme nastavit na 192.168.1.0

Dále je nutné všechny počítače pojmenovat, například PC1, PC2, PC3… a všechny zařadit do stejné pracovní skupiny.

8 OCHRANA DAT PŘED PŘÍSTUPEM Z LOKÁLNÍ SÍTĚ

Základem jsou uživatelské účty, hesla a oprávnění.

8.1 Ochrana složek

Pro výměnu dat mezi jednotlivými počítači v síti používáme sdílené složky. Sdílená složka je pak veřejně distribuována na síti a ostatní uživatelé sítě si můžou data z této složky zkopírovat, případně tam můžou nějaká data přidat.

V operačním systému XP Professional se ručně přepneme do rozsáhlých možností přidělování oprávnění. Základním pravidlem je, že se uživatel nedostane ke sdíleným datům, pokud mu to nepovolíme. I když mu zřídíme účet, musí se před přístupem nejprve přihlásit, musí znát uživatelské jméno a heslo a mít patřičná oprávnění.

Pokud chceme určitá data sdílet se všemi uživateli, je možné přidělit oprávnění celé skupině najednou, „Everyone“. Do takto sdílené složky se pak dostane každý, kdo je v síti připojen. To může znamenat potenciální nebezpečí, protože do takové složky se pak může dostat i anonymně přihlášený uživatel.

Nejvyšší bezpečnosti sdílených dat dosáhneme tím, že snížíme počet uživatelů, kterým přidělíme oprávnění, na minimum.

8.1.1 Anonymní přihlášení

Operační systém Windows umožňuje i přihlášení anonymním uživatelům, kteří nemusejí zadat přihlašovací jméno ani heslo. Tato funkce je však potenciálně nebezpečná, protože obchází prvotní bezpečnostní opatření, nutnost zadat uživatelské jméno a heslo. Anonymní uživatel pak může zjistit některé důležité informace o operačním systému, které by pak mohl zneužít. Doporučuje se tedy přístup anonymního uživatele zakázat.

8.2 EFS (Encrypting File System)

Obecně je ochrana ve Windows založena na uživatelských účtech, přístup k datům je možní pouze po správném přihlášení. EFS používá lepší způsob ochrany dat – šifrování

souborů používající elektronické certifikáty. Výhodou je, že při odcizení našich dat nepovolanou osobou (například krádež notebooku, nebo pevného disku) pachatel nebude schopen data bez dešifrování zobrazit. EFS je integrovaný do souborových systémů NTSF. Samotné šifrování a dešifrování se děje transparentně a nevyžaduje účast uživatele. Nebezpečí hrozí při ztrátě certifikátu, pak zakódovaná data nepřečte ani ten, kdo je zakódoval.

8.2.1 Zásady pro šifrování:

- Šifrovat lze pouze soubory a složky umístěné na svazcích souborového systému NTSF.
- Služba EFS je dostupná pouze u operačního systému Windows 2000 s Windows XP Professional
- Šifrování nelze kombinovat s kompresí
- Nelze šifrovat soubory ve složce, kde je operační systém nainstalovaný
- Nelze šifrovat celé disky, pouze jednotlivé složky a soubory.

8.2.2 Princip EFS

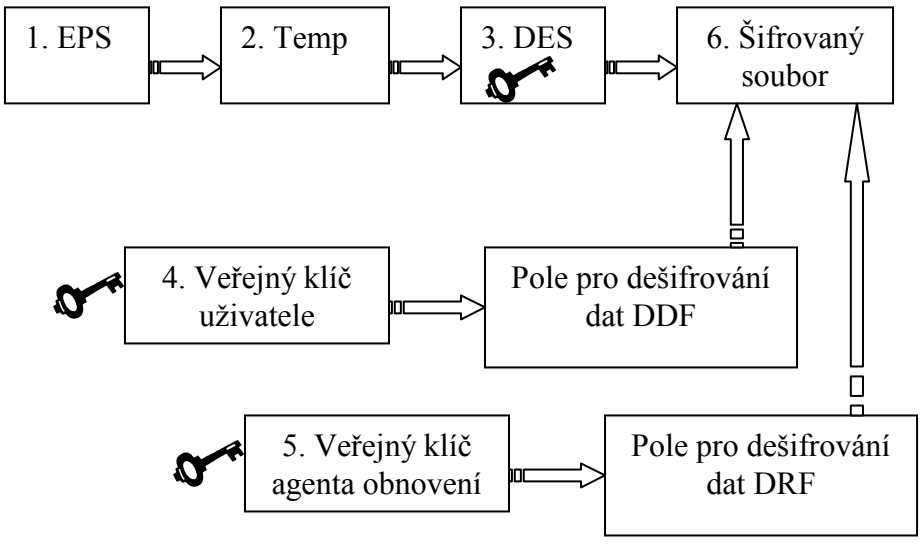
Šifrování a dešifrování se provádí pomocí soukromého a veřejného klíče. Požívá se trojice klíčů:

- souborový, tím šifrujeme soubor
- veřejný, tím se šifruje souborový klíč
- soukromý, tím se dešifruje souborový klíč

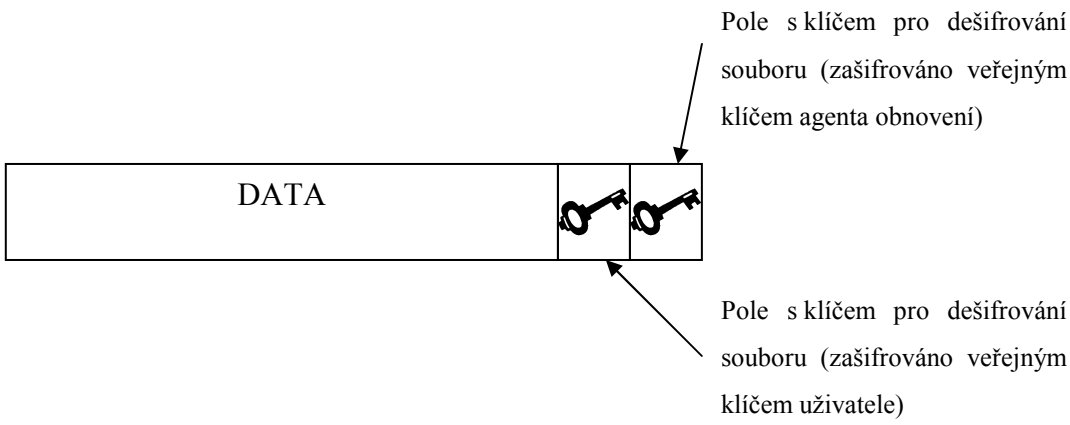
Souborový klíč je pak součástí zašifrovaného souboru. Pokud by došlo ke ztrátě soukromého klíče, je možné použít náhradní řešení – další klíč agenta obnovení. Klíče jsou pak přiřazeny k jednotlivým uživatelským účtům jako elektronické certifikáty.

8.2.3 Kódování dat

1. systém EFS otevře soubor nebo složku, kterou chceme šifrovat a převezme nad ním úplnou kontrolu
2. Během práce pak používá dočasné soubory, které jsou v případě kódování složky šifrované také, v případě šifrování souboru šifrované již nejsou. Proto se doporučuje šifrovat celé složky, nejen jednotlivé soubory.
3. Náhodně se vygeneruje klíč pro soubor, který se pak použije pro zašifrování podle systému DES.
4. vytvoří se pole pro dešifrování souboru, toto pole obsahuje šifrovací klíč, který je zakódován pomocí veřejného klíče. Pole je pak přidáno k šifrovacímu souboru.
5. Vytvoří se další pole pro obnovu souboru pomocí agenta obnovení. Pole obsahuje šifrovací klíč souboru, který je zakódován pomocí veřejného klíče agenta obnovení. Toto pole je přidáno k šifrovanému souboru. Klíč, kterým je soubor zašifrován, je tedy přiložen k samotnému souboru, ale je zakódován jiným klíčem – veřejným klíčem uživatele.



Obrázek 17 Kódování dat EFS

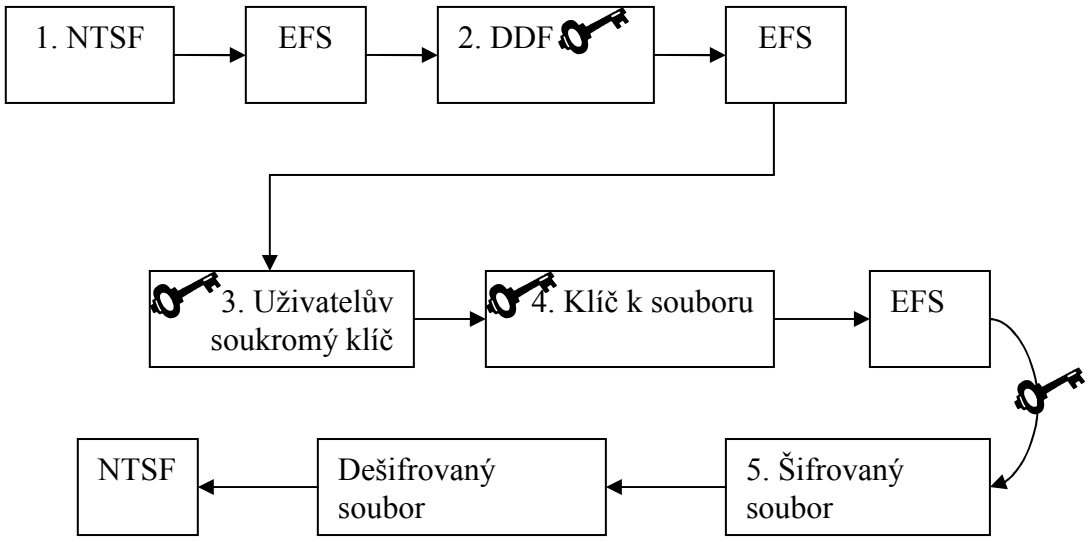


Obrázek 18 Zakódovaný soubor

8.2.4 Dekódování dat

Probíhá opačným krokem jako kódování, využívá klíče uložené v zašifrovaném souboru a soukromé klíče uložené v certifikátu, nebo agenta obnovení.

1. Souborový systém rozpozná zakódovaný soubor a odešle ovladači ESF požadavek na dešifrování dat.
2. Ovladač EFS přečte z datového pole zakódovaného souboru klíč k souboru a předá ho službě EFS.
3. Tato služba toto pole dešifruje pomocí soukromého klíče uživatele, který je součástí certifikátu a tím získá klíč pro dešifrování souboru.
4. Klíč je předán ovladači EFS.
5. Tento ovladač pak dešifruje soubor a následně jej předá souborovému systému NTSF, odkud je již pro uživatele čitelný.



Obrázek 19 Dekódování dat

Součástí uživatelova certifikátu je tedy soukromý a veřejný klíč. V případě poškození, nebo smazání tohoto certifikátu není možné dešifrovat klíč souboru a data již nelze dešifrovat. Proto je vytvořen záložní systém, kdy klíč k souboru je ještě dešifrován do dalšího pole, které je také součástí souboru. Tento klíč je pak šifrován náhradní veřejným klíčem, který patří agentovi obnovení. Tento fiktivní agent představuje náhradní certifikát, který umožňuje data dekódovat v případě problémům s uživatelským certifikátem.

8.3 Microsoft Baseline Security Analyzer

Může se nám stát, že bude potřeba zabezpečit ji fungující vnitřní síť. Nová instalace a by byla časově i technicky náročná a ne vždy je možná. Proto je vhodné použít program Baseline Security Analyzer od Microsoft, který nám výrazně pomůže vnitřní síť analyzovat a upozorní nás na případné chyby a nedostatky.

Tento program je volně dostupný na stránkách společnosti Microsoft a provádí kontrolu bezpečnostního nastavení operačního systému. Dokáže rychle analyzovat bezpečnostní konfiguraci. Ve Windows XP kontroluje:

- vypršení platnosti hesel
- typ systémového souboru

- zda je zapnuta funkce „autologon“
- zda používáme účet „Guest“
- restrikci anonymního uživatele
- počet administrátorských účtů
- prázdněná nebo jednoduchá hesla
- zda nejsou spuštěny zbytečné služby
- vytváří seznam sdílených složek
- zda je zapnut „auditing“
- chybějící „Hotfix a Servise Packs“

8.3.1 Prohlídka počítače

Program prohlídne počítač (je schopen kontrolovat i více počítačů najednou) a výsledky jsou zobrazeny graficky. Závažná chyba je označena červeným křížkem, méně závažná chyba žlutým křížkem a bezchybný parametr je označen zeleným zaškrtnutím. Kontrolované parametry zobrazí do jednotlivých částí:

Windows Scan Results – výsledky kontrol bezpečnosti Windows

Tento test kontroluje hesla, využívá funkce Local Account Password Test, a kontroluje parametry hesla, například zda není heslo prázdné, zda není heslo stejné jako jméno účtu nebo jméno počítače, zda není heslem slovo *password*, *admin* apod.

Additional Systém Information – pomocné informace o operačním systému, které také souvisejí z bezpečností.

Auditing je rozsáhlá služba, která sleduje například počet úspěšných a neúspěšných přihlášení.

Test sdílení nám vypíše všechny sdílené složky testovaného počítače. Její umístění a taky přístupová oprávnění.

Desktop Application Scan Results – informace o zabezpečení programů Office a Internet Explorer

Provádí kontrolu zabezpečení některých aplikačních programů, ovšem pouze těch, které vyvinula firma Microsoft.

Security Update Scan Results – informace o chybějících aktualizacích

Program si stáhne seznam všech aktualizací z webu Microsoft a porovnává ho se seznamem aktualizací již nainstalovaných v počítači.

ZÁVĚR

Práce řeší zabezpečení dat uvnitř sítě a jako nejvhodnější řešení se ukázalo být zabezpečení pomocí šifrování, které jsem blíže popsal včetně principů, na kterých jsou jednotlivé šifry založeny. Fyzické zabezpečení není podle mě moc efektivní z důvodu vyšších pořizovacích nákladů. Při vyšším stupni bezpečnostního rizika bych navrhl kombinaci obou systému s hlavním důrazem na šifrování.

Při šifrování vzájemné komunikace je nejvhodnější použití proudové Vermanovi šifry z důvodů její bezpečnosti. Nevýhodou je pak příliš dlouhý klíč. Pro zabezpečení velkých dokumentů je pak vhodná šifra Blowfish, protože není patentovaná a je volně přístupná. Při vyšším riziku je však lepší použít algoritmus RSA, nevýhodou je však jeho implementace, protože je náročný na výpočetní techniku. To ho dělá velmi pomalým.

Vzájemné srovnávání jednotlivých šifrovacích algoritmů lze provést z několika pohledů. Pokud budeme chtít šifrovat komunikaci mezi více účastníky, což v případě vnitřních sítí může nastat, je vhodnější použití asymetrického šifrování. Každý účastník takové diskuze pak bude mít pouze dva klíče. Veřejný, kterým bude šifrovat odesílané zprávy a soukromý, kterým bude šifrovat přijímané zprávy od všech účastníků. Každý účastník má tedy pouze jeden klíč, který si musí chránit. Veřejný klíč je pak volně distribuován. V symetrickém šifrování by jsme potřebovali pro každého účastníka této komunikace jiné heslo. Takže čím více účastníků, tím více hesel, které musíme chránit. Proto je výhodnější a jednodušší použití asymetrického šifrování.

Z hlediska bezpečnosti jsou kryptosystémy závislé především na délce klíče, protože u většiny dnešních kryptosystémů není jiná možnost prolomení, než hrubou silou na heslo u symetrického šifrování, nebo nemožnost faktorizace u asymetrického šifrování. U symetrického šifrování nám stačí menší délka klíče, například u blokových šifer je vhodná délka klíče od 56 do 109 bitů, u asymetrického šifrování je doporučená délka klíče větší, konkrétně u RSA je to od 417 do 4047 bitů.

Z pohledu rychlosti šifrování jsou vhodnější symetrické kryptosystémy, asymetrické jsou několika násobně pomalejší. V některých případech to může být až tisíckrát. Mezi symetrickým šifrováním je nejrychlejší algoritmus AES, Blowfish, středně rychlé jsou pak DES, IDEA a nejpomalejší je 3DES.

Co se týká využití, tak symetrické šifrování je vhodnější pro komunikační protokoly nebo pro šifrování velkého objemu dat, asymetrické kryptosystémy se používají spíš pro výměnu tajných klíčů symetrické kryptografie, také u digitálních podpisů a pro šifrování menších množství dat.

Velmi často se používají různé kombinace obou kryptosystémů, například při výměně tajného klíče k symetricky zašifrovaném souboru použijeme pro přenos po nezabezpečené přenosové trase asymetrické šifrování. Toho využívá například velmi populární program PGP, který slouží pro bezpečnou komunikaci. Využívá toho také výše popsaný EFS (Encrypting File System). Podle mě je to ideální řešení, které kombinuje rychlost symetrického šifrování a bezpečnost asymetrické šifry. Výhodou je, že je součástí operačního systému Windows XP Professional.

Při šifrování je také velmi důležitá správná implementace a správně zvolená délka klíče.

SUMMARY

The work is solving data security inside the network and as the best solution it has appeared to be security with the help of the cryptography. I have described them closely with the inclusion of principles, in which an individual ciphers are based. The physical security isn't from my point of view very effective on the ground of the higher acquisition cost. At the higher step of security risk. I would suggest a combination of both systems with the main insistence on the cryptography.

The most appropriate in the cryptography of mutual communication is to use turbojet Verman's ciphers for their safety reasons. The length of the key is disadvantage. For the security of more extensive documents is convenient Blowfish's cipher, because it hasn't been patent and it's freely available. However, at higher risk is better to use the algorithm RSA .The implementation is its disadvantage, because it's very difficult for the computer technology. That makes it too slow.

Mutual comparison of individual cryptography algorithms can be accomplished from several aspects. If we would like to cipher communication in between more participants, which in case of inner network can happen, it's more appropriate to use asymmetrical cryptography. Each participant of this discussion will only have two keys. The public key will cipher outgoing messages and the private key will cipher incoming messages from all of the participant. Each participant has only one key that he or she has to guard. The public key is then feely distributed. In the symmetrical cryptography we would need for each participant of this communication different password. More participants means more passwords that we have to guard. Therefore, it's better to use asymmetrical cryptography for its advantages and simplicity.

On the part of safeness are cryptosystem dependent above all on key length, because near most today's cryptosystem isn't alternative piping, than coarse by force on password near symmetrical encryption, or impossibility factorization near asymmetrical encryption. Near symmetrical encryption to us be enough smaller key length, for example near frozen credit cipher get past key length from 56 to the 109 bit location, near asymmetrical encryption is recommended key length bigger, in the concrete near RSA is that a from 417 to the 4047 bit location.

Look rate encryption get past symmetrical cryptosystem, asymmetrical are of several multiple slower. In some cases it can be up to thousand fold. Among symmetrical encryption is fastest algorithm AES, Blowfish, medium fast are then DES, IDEA and slowest is 3DES.

As a matter of usage, the symmetrical cryptographies are more convenient for communication's protocols or for the cryptography of large capacity of data. The asymmetrical cryptosystems are more likely to be used for exchange of secret keys of symmetrical cryptography as well as digital signatures and the cryptography of smaller capacity of data.

Very often different combinations of both cryptosystems are used. For example at exchange secret key to balanced cryptic set applied for transmission after unsecured program temporary carrier trace asymmetrical encryption. That derive benefit from for example very popular program PGP that the serves for safe communication. Derive benefit from that also height circumscribed EFS (Encrypting File System). From my point of view is that a ideal solution that the combines rate symmetrical encryption and safeness asymmetrical cipher. Advantage is, that belong surgical system Windows XP Professional.

It's very important to have correct implementation as well as right length of the key at cryptography.

SEZNAM POUŽITÉ LITERATURY

[1] Mgr. JAŠEK Roman Ph.D. *Informační a datová bezpečnost*. 1. vyd. [s.l.] : Univerzita Tomáše Bati ve Zlíně, 2006. 140 s. ISBN 80-7318-456-7.

[2] HORÁK, Jaroslav. *Bezpečnost malých počítačových sítí*. Praha : Grada Publishing, 2003. 200 s. ISBN 80-247-0663-6.

[3] HORÁK, Jaroslav. *Malá počítačová síť doma a ve firmě*. Praha : Grada Publishing, 2003. 184 s. ISBN 80-247-0582-6.

[4] BRABEC, F., et al. *Bezpečnost pro firmu, úřad, občana*. Praha : Public History, 2001. 400 s. ISBN 80-86445-04-06.

[5] MATĚJKA, Michal. *Počítačová kriminalita*. Praha : Computer Press, 2002. 106 s. ISBN 8072264192.

[6] *Počítačová síť - Wikipedie, otevřená encyklopedie* [online]. 2007, 13:10, 8.5.2007 [cit. 2007-05-09]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5#Pod.C3.ADvejte_se_tak.C3.A9_na>.

[7] ODVÁRKA, Petr. *Svět sítí* [online]. c1999 , 7. září 2000 [cit. 2007-02-07]. Dostupný z WWW: <http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&temaID=1&clanekID=20>

[8] *Autentizační kalkulátory* [online]. c2000-2005 [cit. 2007-03-27]. Dostupný z WWW: <http://www.alsoft.cz/cz/Products/Security/Security-Technology/Authentication-Tokens/>.

[9] KOUŘIL, D. *Správa soukromých klíčů pomocí hardwarových tokenů.* Zpravodaj ÚVT MU. ISSN 1212-0901, 2005, roč. XV, č. 5, s. 12-16

[10] RAK, Roman, KUMMER, Radek. Informační hrozby v letech 2007-2017. *Security*. 2007, č. 1, s. 2-5.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CD CD Compact Disc (Kompaktní disk)

DES Data Encryption Standard (Standart kódování dat)

DHCP Dynamic Host Configuration Protocol (Dynamický hostitelský konfigurační protokol)

DoS Denial of Service (popření služby)

DVD Digital Versatile Disc nebo Digital Video Disc (formát digitálního optického datového nosiče)

EFS (Encrypting File System)

IDEA International Data Encryption Algorithm (Mezinároodní algoritmus pro šifrování dat)

IP Internet Protocol (Síťový protokol)

IT Informační technologie

LAN Local Area Network

MAC Media access control (jedinečný identifikátor síťového zařízení)

MAN Metropolitan Area Network

PDA Personal digital assistant (osobní digitální pomocník)

PIN Personal Identification Number (Osobní identifikační číslo)

RFID Radio Frequency Identification (Rádiofrekvenční identifikace)

SW Software

TCP Transmission Control Protocol (Komunikační přenosový protokol)

USB Universal Serial Bus (univerzální sériová sběrnice)

UTP Unshelded Twisted Pair (kroucený pár)

VoIP Voice over Internet Protocol (Hlas přes internetový protokol)

WAN Widea Area Network

XOR Exkluzivní disjunkce

SEZNAM OBRÁZKŮ

SEZNAM TABULEK