# Bezpečnost v sítích

# Cíl

Cílem je povolit bezpečnou komunikaci mezi dvěma částmi distribuovaného systému. To vyžaduje realizovat následující bezpečnostní funkce:

1. authentikaci:
    a. zajištění, že zpráva je opravdová, byla přijata tak, jak byla odeslána a přišla od daného zdroje
    b. verifikace identity individua, jako je osoba u vzdáleného terminálu nebo odesílatel zprávy
2. integrita dat: vlastnost, že data nebyla změněna nebo porušena neautorizovaným způsobem
3. důvěrnost (utajenost): vlastnost, že informace nebyla přístupná nebo prozrazená neautorizovaným individualitám, entitám nebo procesům.

Implementace těchto funkcí zásadě vyžaduje použití kryptografických protokolů.

# Kryptografické funkce

1. **Tajný klíč:** použití jednoho klíče k šifrování otevřeného textu a dešifrování šifrovaného textu. Vyžaduje, aby odesílatel i adresát sdíleli tajný klíč.
2. **Veřejný klíč:** Použití různých klíčů pro šifrování a dešifrování. Jeden z nich je tajný a druhý veřejný.
3. **Hashování:** použití hashovaní funkce nad posílanou zprávou. Nejedná se o šifrování, ale o verifikaci.

# Existují čtyři oblasti bezpečnosti v sítích

1. Utajení
2. Ověření pravosti (autentikace)
3. Nepopiratelnost (Nonrepudiation)
4. Kontrola integrity

# Každá úroveň se může podílet na bezpečnosti

1. Aplikační: PGP
2. Transportní: SSL
3. Síťová: IPSec
4. Linková: šifrování, speciální spoje

Utajení spočívá v udržení informace mimo dosah neautorizovaných uživatelů

1. Fyzická bezpečnost – zámky, trezor, ostraha
2. kryptografie

# Pojmy, definice

- Kryptoanalýza – umění rozlomit šifru
- Kryptografie – umění vymyslet šifru (šifrování)

- Kryptologie – studium kryptoanalýzy a kryptografie
- Šifrování tajným klíčem – používá tentýž klíč pro šifrování i dešifrování. Klíč musí být držen v tajnosti.
- Šifrování veřejným klíčem – používá veřejný klíč pro šifrování a tajný klíč pro dešifrování. Držen v tajnosti musí být pouze tajný klíč.

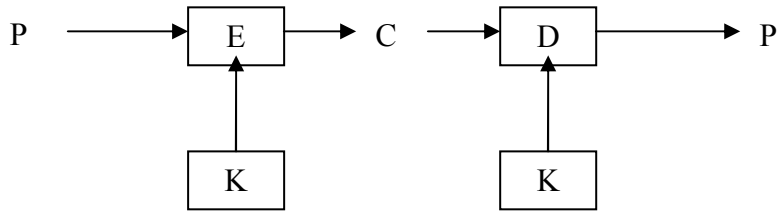
# Základní mechanizmy šifrování

**Substituce:** pouze náhrada některých znaků jinými podle předem definovaného mapování → realizace prostředky S–box.

**Transpozice:** přeskupení znaků následujících za předem definovaným příznakem (např. transpoziční tabulka) → realizováno prostředky P-box.

**Kombinace:** kaskádní použití S a P boxů.

**Model šifrování:**




Šifrování tajným klíčem, symetrické metody šifrování.

1. Substituční šifry
    a. Každé písmeno nebo skupina písmen je nahrazena jiným písmenem nebo skupinou písmen
    b. Např. Caesarova šifra – použita Caesarovými vojsky
    c. Jednoduše prolomitelné
2. Transpoziční šifry
    a. Přeuspořádání písmen, ale ne překódování
    b. Sloupcové šifrování – otevřený text je šifrován po sloupcích různými klíčovými slovy
    c. ne tak jednoduché prolomení jako u substitučních šifer.
3. Jednorázová hesla
    a. 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)
    b. Neprolomitelná šifra
    c. Klíč je obtížné si pamatovat – odesílatel i příjemce musí přenášet i kopii klíče
    d. Vyžaduje striktní synchronizaci mezi odesílatelem a příjemcem. Jeden chybějící bit může pomotat cokoliv

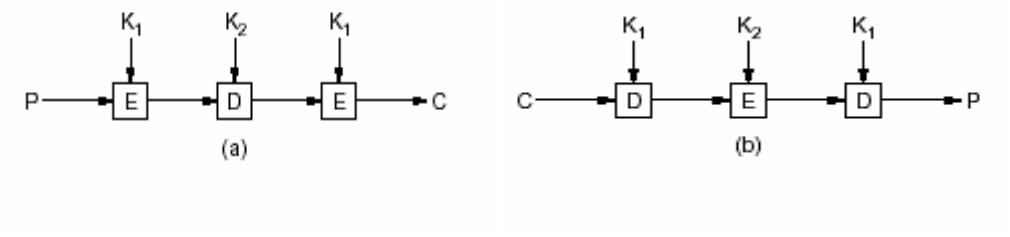
4. DES – Data Encryption Systém

- Každá iterace i používá jiný klíč $K_i$. Složitost závisí na komolící funkci *f*.
- Klíč $K_i$ je odvozován od počátečního 56 bitového klíče.

    a. Šifrovací algoritmus vyvinut v r. 1970 National Bureau of Standards and Technology a IBM.
    b. Používá délku klíče 56 bitů a 19 různých stavů
    c. Velmi silný, ale prolomitelný

5. Triple DES – řeší problém příliš krátkého klíče DES jeho rozšířením na 112 bitů

    a. Pro šifrování postupně používá algoritmus šifrování klíčem $K_1$, dešifrování klíčem $K_2$ a šifrování klíčen $K_1$.
    b. Pro dešifrování postupně používá algoritmus dešifrování klíčem $K_1$, šifrování klíčem $K_2$ a dešifrování klíčen $K_1$.




6. AES/Rijndael
    a. DES je nyní příliš slabý
    b. Nyní nahrazován vítězem konkurzu o šifrovací standard (AES – Advanced Encription Standard) – Rijndael.

7. IDEA – International Data Encription Standard
    a. Publikován v r. 1990
    b. Používá klíč délky 128 bitů
    c. Velmi silné šifrování, nebyly publikovány žádné praktické útoky, útok hrubou silou není praktický
    d. Pokrytý různými mezinárodními patenty
8. Skipjack
    a. Tajný algoritmus vyvinutý NSA
    b. Je použit v šifrovacím čipu Clipper
    c. Využívá klíč délky 80 bitů

Metody šifrování veřejným klíčem

6. RSA – vytvořeno pány Rivest, Shamir a Adlemin v r. 1978
    a Velmi silná šifra
    b Podporuje proměnnou délku klíčů
    c Delší klíče zajišťují větší bezpečnost
    d Algoritmus založen na počítání s velkými prvočísly

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)

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

Certifikační autority

- Používají se k administraci a ověřování veřejného klíče.
- Musí být důvěryhodnou stranou.
- Umožňují ověřování uživatele v rozsáhlém systému – decentralizované oběřování.
- 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 (PFX), PKCS #12 (P12) (Public Key Cryptography Standard)

- Cryptographic Message Syntax Standard PKCS#7 (P7B)

Zřetězení certifikátů

Certifikačních autorit je hodně – získání certifikátu může být otázkou osobní návštěvy (důvěryhodné získání certifikátu)
V prohlížečích jsou certifikáty uznávaných autorit instalovány – musíme jim věřit. Existují ale i další certifikační autority, které nejsou uznávané – prohlížeč se na důvěryhodnost ptá. 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.

Zabezpečení elektronické pošty

PEM

PEM (Privacy Enhancement for Internet Electronic Mail) je dnes historický protokol pro vytváření a zpracování bezpečných zpráv. Vznikl v druhé polovině 80. let. Původní specifikace RFC989 byla několikrát přepracována. Poslední specifikace je z roku 1993 jako RFC1421 až RFC1424.

V praxi nedošlo k jeho masovému využití nejširší veřejností. Nebyl totiž běžně dostupný software, který by jej podporoval. Příčin bylo bezpochyby více, ale asi tou nejdůležitější je skutečnost, že na přelomu 80. a 90. let nebyla ještě masová poptávka po software tohoto druhu.

Protokol PEM se však stal základem pro novější protokoly. Dnes se právě S/MIME zdá být východiskem a přitom S/MIME je PEM filozoficky velmi blízké. Zejména se jedná o správu šifrovacích klíčů pomocí certifikátů.

S_MIME

S/MIME podporuje následující algoritmy:

- Pro kontrolní součet: SHA-1 a MD5
- Asymetrické šifrovací algoritmy (šifrování symetrických šifrovacích klíčů a elektronický podpis): RSA s délkou klíče minimálně 512 bitů.
- Symetrické šifrovací algoritmy (šifrování textu zprávy): FOO, FOO/40, DES-CBC, triple DES.

Zdá se, že S/MIME bude prvním systémem pro bezpečnou poštu, který najde masové uplatnění. Důvodem je skutečnost, že S/MIME podporují klienti firmy Netscape.

S/MIME řeší problematiku bezpečných zpráv z praktického pohledu. Vychází z toho, že má k dispozici normu PKCS-7 pro tvorbu bezpečných zpráv. PKCS-7 umí zprávu elektronicky podepsat, šifrovat i podepsat a zároveň šifrovat. Definují proto jen příslušnou MIME hlavičku Content-Type typ/subtyp:

```
Content-Type: Application/pkcs7-mime
```

Čili zprávu zabezpečí podle normy PKCS-7 a aby se vyhověl MIME, tak definuje `application/pkcs7-mime`.

PGP

PGP nepřináší filozoficky nic nového. Vzniklo z iniciativy jednoho člověka, jehož snahou bylo vytvořit uživatelsky jednoduchý program dostupný nejširší veřejnosti. Tohoto cíle bezpochyby dosáhl. Dodnes je PGP nejrozšířenější prostředek pro zpracování bezpečných zpráv. Proto v této kapitole popíšeme jednotlivé příkazy PGP. Zájemce o podrobnější popis odkážeme na RFC1991. Na závěr kapitoly ještě uvedeme poznámku o vztahu PGP a MIME.

PGP (Pretty Good Privacy) vytvořil Američan P.R.Zimmerman. První verze PGP jsou z roku 1991.

PGP je určeno pro bezpečný přenos elektronické pošty běžnou "ne-bezpečnou" elektronickou cestou (tj. protokoly SMTP, POP, IMAP apod.) . PGP nezavádí nový síťový protokol - nezavádí prezentační vrstvu, používá běžné elektronické cesty. Nepotřebuje tedy rekonfigurovat počítač. Využijete to co pro komunikaci běžně používáte. Musíte si pouze obstarat program PGP a pomocí něj zprávu předem šifrovat i elektronicky podepisovat. Přijatou zprávu je třeba nejprve uložit do souboru, na který se následně aplikuje program PGP.

PGP používá:

Pro asymetrické šifrování algoritmus RSA (pro šifrování symetrického klíče relace -klíče, kterým se šifruje text zprávy).
Pro symetrické šifrování algoritmus IDEA.
Pro kompresi dat před šifrováním používá PKZIP (po šifrování jsou data těžko komprimovatelná).
Pro výpočet kontrolního součtu algoritmus MD5.
Pro převod binárních dat na ASCII používá algoritmus Radix-64. Převod binárních souborů do ASCII se provádí proto, aby je bylo možné posílat elektronickou poštou (tj. protokolem SMTP), která je obecně v Internetu jen sedmibitová (tj. ASCII) i když některé oblasti Internetu umožňují osmibitový přenos, tak obecně s tím nelze počítat.

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 (Transprt 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.