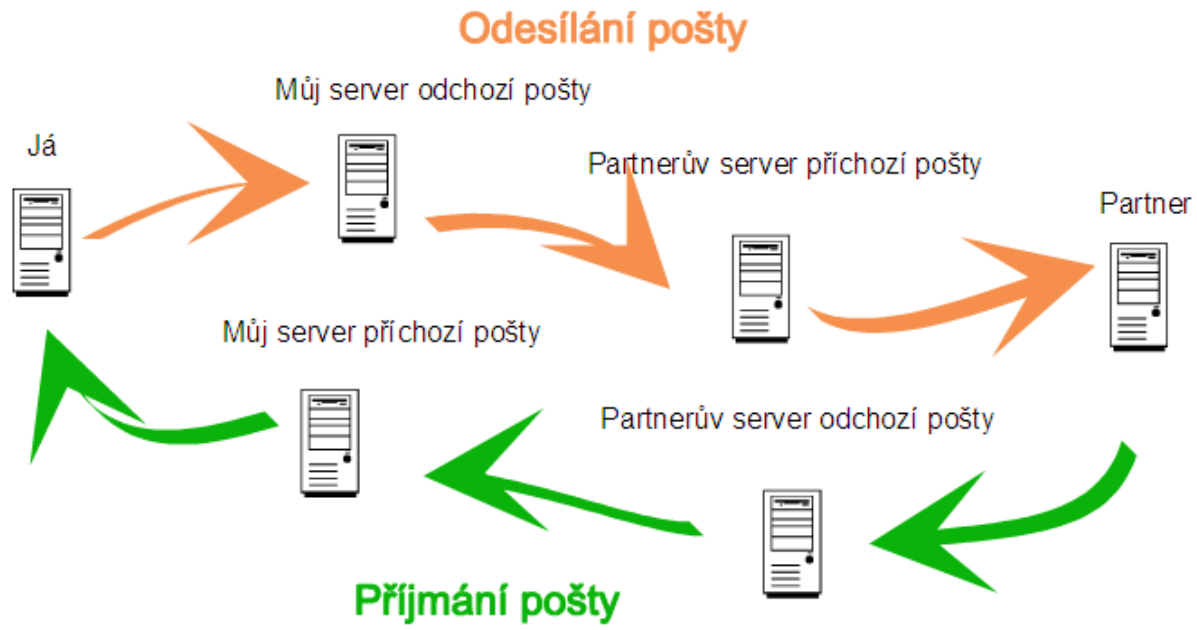
# 1 ELEKTRONICKÁ POŠTA

## 1.1 ODESÍLÁNÍ ELEKTRONICKÝCH ZPRÁV

Já, jako odesílatel elektronických zpráv mám u poskytovatele služeb elektronické pošty zřízenou elektronickou schránku s adresou ***já@poskytovatel.cz*** a odesílám zprávu partnerovi do jeho elektronické schránky s adresou ***partner@jehoposkytovatel.cz***. Zpráva putuje ode mne na **můj server odchozí pošty**, který ji podle adresy partnera odešle na **partnerův server příchozí pošty**, kde zpráva čeká na vyzvednutí.

## 1.2 PŘÍJMÁNÍ ELEKTRONICKÝCH ZPRÁV

Můj korespondenční partner odešle zprávu na **jeho server odchozí pošty**, který ji podle adresy odešle na **můj server příchozí pošty**, kde zpráva čeká do té doby, než si ji vyzvednu.




**Elektronickou poštu lze provozovat:**

- přes webové rozhraní (k tomu je na mém počítači třeba pouze internetového prohlížeče)
- pomocí klienta elektronické pošty

**Klienti elektronické pošty:**

- Outlook Expres - součástí příslušenství OS Windows..
- Mozilla Thunderbird – kvalitní volně šiřitelný poštovní klient použitelný i v OS Linux

Ke zřízení účtu v **poštovním klientovi** je třeba znát jména poštovních serverů pro odchozí a příchozí poštu, protokol, který naše servery používají a čísla portů připojení.

**Jméno, protokol a port serveru pro příchozí poštu** najdeme na webových stránkách provozovatele elektronické pošty, u něhož jsme si zřídili schránku. Jméno může vypadat třeba takto: pop3.quick.cz, protokol může být POP (port 110) nebo IMAP (port ???).

**Jméno, protokol a port serveru pro odchozí poštu** nám sdělí internetový provider, přes kterého jsme připojeni k internetu, nebo správce školní či firemní sítě. Může vypadat třeba takto: smtp.sattnet.cz, protokol SMTP (port 25).

# 2 PRINCIPY BEZPEČNÉ KOMUNIKACE

Běžná komunikace elektronickou cestou **není** nijak zabezpečena proti odposlechu zpráv třetí osobou ani proti podvrhování zpráv. Jsou však situace, kdy je nutné data utajovat (armáda, banky, firemní databáze lékařů, právníků, manažerů...) a bezpečně předávat partnerovi. Během let vykrystalizovaly všeobecné principy bezpečné komunikace, které lze zformulovat takto:

- zprávu nemůže číst nikdo třetí
- zprávu nemůže nikdo třetí modifikovat
- je jisté, od koho zpráva přichází
- odesilatel nemůže popřít, že ji poslal

## 2.1 ŠIFROVÁNÍ

Způsob, jak zajistit nečitelnost zpráv pro třetí osobu je šifrování (kryptografie).

## 2.2 SYMETRICKÁ KRYPTOGRAFIE

"Konvenční" nebo-li "Symetrická" kryptografie (též substituční) využívá nahrazení znaku otevřeného textu jiným znakem pomocí šifrovacího algoritmu a klíče. **Stejný klíč se použije i pro rozšifrování zprávy**.

Jeden z nejjednnodušších a nejstarších šifrovacích algoritmů používal už Julius Caesar:
**algoritmus**: posunutí písmene o několik znaků v abecedě
**klíč:** počet znaků, o který se posouvá

př1: klíč = 4 AHOJ ------> EKTN

šifrování s tímto algoritmem v kombinaci s takto jednoduchým klíčem je však velmi snadno odhalitelné pouhým statistickým porovnáním s textem v příslušném jazyce. Jeho odhalení (při zachování algoritmu) se dá znesnadnit prodloužením klíče:

př2: klíč = 2, 5, 4, 3 (první písmeno otevřeného textu se posune o 2 znaky v abecedě, druhé o 5, …)

*ÚKOL 1: rozluštěte zprávu: OZN QGOQLNINVK USNTR NH LNHOQ s využitím klíče 2,5,4,3 (nepracujte s diakritikou, abeceda včetně W)*

*Úkol 2: rozluštěte zprávu Kryptoanalýza pomocí znalosti četnosti výskytu jednotlivých písmen na 100 znaků v českém textu.*

### 2.2.1 Tajnost klíče

Současné algoritmy šifrování jsou **obecně známé** a tajnost zprávy závisí pouze na **tajnosti klíče**. Délka klíče má podstatný vliv na znesnadnění kryptoanalýzy (rozluštění šifry). **Kryptoanalýza** k rozluštění šifry využívá znalosti o četnosti výskytu jednotlivých písmen nebo slov v daném jazyce. Takže vlastnost, že se stejné části otevřeného textu zakódují různě, znesnadní kryptoanalýzu. Jinak řečeno, čím je klíč delší, tím je lepší.
**Výhody a nevýhody symetrické kryptografie:**

Výhodou: rychlost (dá se dobře využít pro šifrování dat, která se nikam neposílají)
Nevýhodou: problém bezpečného předání klíče

*Úkol: Vyzkoušejte si jednoduché symetrické šifrování pomocí programu 7-zip. (Při komprimaci souboru můžete zadat heslo, které je klíčem pro šifrování)*

## 2.3 ASYMETRICKÁ KRYPTOGRAFIE

Existuje ještě další způsob kryptografie, a tím je "Asymetrická kryptografie" (Public key cryptography). Asymetrická je proto, že využívá **jiného klíče pro šifrování a jiného pro dešifrování** (narozdíl od symetrické)

Dvojice klíčů se skládá ze soukromého a veřejného klíče. Můžeme si je představit jako dvě velmi vysoká čísla, mezi nimiž je nějaká matematická souvislost. Z jednoho čísla však nelze (v krátkém čase) vypočítat to druhé ani s využitím nejvýkonější techniky.

Použití dvojice klíčů k šifrované komunikaci se dá shrnout do následujícího postupu:

1. Romeo a Julie chtějí komunikovat šifrovaně.
2. **Romeo** získá **svoji dvojici klíčů** – **veřejný a soukromý** (obvykle ji vygeneruje nějaký kryptografický program, pro domácí pokusy lze použít volně dostupný GPG). Oba klíče spolu **souvisejí**.
3. **Soukromý si nechá**, **veřejný klíč předá** Julii, či komukoliv jinému, s nímž chce šifrovaně komunikovat.
4. Julie **zašifruje** svoji tajnou zprávu **Romeovým veřejným klíčem**.
5. Romeo r**ozšifruje** Juliinu tajnou zprávu **svým soukromým klíčem**.
6. Jestli Romeo svůj soukromý klíč ztratí, nikdy se nedozví, co mu Julie chtěla sdělit.
7. Chce-li Julie dostávat od Romea tajné zprávy, musí i ona mít svoji dvojici klíčů. Soukromý klíč si nechá, veřejný klíč předá Romeovi...

A jak Romeo pozná, že obdržená tajná zpráva zašifrovaná jeho veřejným klíčem (a ten zná kde kdo) je skutečně od Julie? No jedině tak, že **Julie zprávu „podepíše" pomocí svého soukromého klíče**. Asymetrické šifrování se dá použít k **elektronickému podepisování**.

**Výhody a nevýhody asymetrického šifrování:**

| | |
|---|---|
| Výhodou: | odpadá problém bezpečného předání klíče |
| Nevýhodou: | při dlouhých zprávách je asymetrické šifrování pomalé;<br>není jisté, zda veřejný klíč patří skutečně příslušné osobě, či je podvržený |
| Využití: | jakákoliv bezpečná komunikace po internetu<br>internetové obchodování<br>internetové bankovnictví<br>komunikace s úřady (daňové přiznání, odevzdávání evidenčních listů na OSSZ...) |

## 2.4 ELEKTRONICKÝ PODPIS

**Elektronický podpis** v širším slova smyslu znamená **připojení identifikačních údajů** (jméno, adresa, rodné číslo...) **k elektronické zprávě**.

Identifikační údaje se v běžné, **nešifrované komunikaci** dají velice snadno **podvrhnout**.

**Zaručený elektronický podpis** však musí splňovat všechny **principy bezpečné komunikace.**
Proto se:

- Využívá asymetrického šifrování
- Při komunikaci s úřady je nutné získat bezpečnostní certifikát, který zaručuje, že veřejný klíč je skutečně spojen s příslušnou osobou

## 2.5 CERTIFIKAČNÍ AUTORITA A CERTIFIKÁTY

Pro bezpečnou komunikaci elektronickou poštou stačí k vygenerování veřejného a soukromého klíče použít některý z SW (PGP – komerční, nebo volně šiřitelný GPG).

Ne tak při komunikaci s úřady a institucemi. Zde musí existovat nějaká autorita, která zaručí splnění principů bezpečné komunikace. Takovými institucemi jsou **Certifikační autority** (u nás po 1. CA vzniklo několik dalších). Tyto instituce se podobají státním notářům. Certifikační autorita vystupuje při vzájemné komunikaci dvou subjektů jako třetí nezávislý důvěryhodný subjekt, který prostřednictvím jím vydaného certifikátu (asi 800 Kč) **jednoznačně svazuje identifikaci subjektu s jeho dvojicí klíčů.** Certifikát se tak stává jakýmsi elektronickým průkazem totožnosti. Certifikáty obsahují ve své nejjednodušší formě veřejný klíč, jméno a další údaje zajišťující nezaměnitelnost subjektů. Běžně používané certifikáty též obsahují datum počátku platnosti, datum ukončení platnosti, jméno certifikační autority, která certifikát vydala, sériové číslo a některé další informace. Certifikační autorita garantuje jedinečnost subjektů podle užité identifikace subjektu. To je zajištěno legislativními a technickými pravidly provozu instituce Certifikační autority.

*Úkol: Zjistěte a vypište 5 certifikačních autorit v České republice*

# 3 VIRY, ČERVY A JINÁ HAVĚŤ

## 3.1 O CO JDE

**Virus:** Škodlivý program, který se aktivuje až když ho uživatel spustí.
**Červ:** Program běžící na cizím počítači využívající chyb v síťových službách k tomu, aby váš počítač ovládl.
**Trojský kůň:** Program, který když spustíte, zajistí bezproblémový průnik a ovládnutí vašeho počítače cizím počítačem – útočníkem.
**Spyware:** Program zjišťující a odesílající informace o vašem počítači a osobních datech.
**Keylogger:** Program monitorující klávesy, které používáte – hledá tak hesla a čísla platebních karet.
**Spam:** Nevyžádaná pošta. Neničí, ale obtěžuje.
**Antivirový program:** Software, který rozpozná a zlikviduje počítačové viry.
**Rezidentní ochrana:** Je-li u antivirového programu zapnuta, program kontroluje všechny prováděné operace (málo výkonné počítače to značně zpomaluje).
**Phishing:** Podvržené e-mailové zprávy a webové stránky předstírající třeba uživatelovu banku, aby získaly uživatelovo heslo.

## 3.2 OBRANA

Uživatelé OS Linux mohou být bez obav, dosud není znám úspěšný virus. Uživatelé OS Windows jsou na tom mnohem hůř.
**Proti škodlivým programům** vás ochrání trojice: **zdravý rozum + antivirový program + firewall**
**Proti odposlechu vašich hesel a čísel platebních karet** vás ochrání jedině šifrovaná komunikace.

**Prevence proti škodlivým programům:**

- neotevírat přílohy e-mailů od neznámých osob (ani kdyby to byla Aneta Langerová)
- nestahovat a nespouštět programy z neprověřených zdrojů
- v systému Windows vypnout automatické spouštění programů (autorun)
- nepoužívat účet s administrátorskými právy kběžné činnosti na PC
- zálohovat, zálohovat, zálohovat
- používat antivirový program s rezidentní ochranou, pravidelně ho aktualizovat
- nestahovat a nespouštět aplikace z neprověřených zdrojů
- používat a správně nakonfigurovat firewall
- pravidelně aktualizovat OS

**Pravidla prohlížení internetu:**

- Podle statistik je nejméně bezpečným prohlížečem Internet Explorer od firmy Microsoft. Bezpečí lze zvýšit:
- výměnou prohlížeče za bezpečnější, třeba Mozilla Firefox, nebo Opera.
- nesurfovat v administrátorském účtu
- pravidelně aktualizovat prohlížeč
- vypnout pamatování hesel v prohlížeči

**Při napadení:**

V případě, že antivirový program nahlásí napadení počítače virem, máme několik možností:

- antivirový program nabídne léčení nebo smazání napadených souborů. Jsou to nejrychlejší možnosti ale nemusí vést ke stoprocentnímu odstranění nákazy.
- přeinstalujeme operační systém a ze záloh obnovíme uživatelské soubory. Tato možnost je pracná, ale spolehlivá (pokud nemáte virus v zálohovaných souborech :))

**Pozor! Antivirové programy umí rozeznat pouze zlomek počítačových virů, svým uživatelům přinášejí falešný pocit bezpečí.**

**Podezřelé chování PC:**

Přestože antivirový program nehlásí žádnou infekci, náš počítač může být napaden. Přitom nemusíme vůbec nic divného pozorovat. Někdy ale můžeme přítomnost virů odhadnout podle podezřelého chování našeho PC:

- pomalejší běh
- otevírají se okna, aniž bychom je pouštěli
- velký objem dat přenášených po síti (pomůže zjistit náš poskytovatel internetu)

Při těchto příznacích je nejlépe operační systém přeinstalovat a uživatelská data obnovit ze záloh.

## *3.3 FIREWALL*

Obvyklá komunikace po síti mezi dvěma počítači probíhá podle modelu **klient – server**. Například váš počítač jako **klient elektronické pošty** zašle žádost na **server příchozí pošty** (třeba pop3.quick.cz) o vyzvednutí zpráv. Chvíli si navzájem vyměňují informace o autentizaci až nakonec server vyhoví, a pošle vám vaše zprávy. Tato komunikace se rozběhla na popud vašeho počítače. Jindy se komunikace může rozběhnout impulzem z venku. Třeba když nabízíte svůj disk ke sdílení (jste v této službě serverem) a někdo jiný chce služby využít (jako klient). Pošle vám jako první žádost o sdílení.
**Firewall** je software, který kontroluje příchozí a odchozí pakety. Firewall systému Windows XP Ve svém nejjednodušším nastavení propouští všechny pakety související s komunikací, kterou jste začali vy jako první (všechny přicházející pakety jsou odpovědí na vaši žádost) a nepropustí žádný paket, který není reakcí na vaši výzvu. Firewall je součástí OS Windows od verze XP.

*Úkol: Prohlédněte si nastavení frewallu: Start/ Nastavení/ Ovládací panely/ Brána firewall systému Windows*