

Identifikátor materiálu: **ICT-2-04**

Předmět – Téma sady	Informační a komunikační technologie
Téma materiálu	Zabezpečení informací
Autor	Ing. Bohuslav Nepovím
Anotace	Student si procvičí / osvojí kryptografii.
Druh učebního materiálu	Prezentace (Výklad / Test)
Typ vzdělávání	Střední škola / SOU
Ročník	1. – 3.
Datum vytvoření	Prosinec 2012
Aktualizace	Srpen 2016

Informační a komunikační technologie

Zabezpečení informací

Zabezpečení dat

Zabezpečit data před cizí osobou lze např.

- zabezpečením přístupu k počítači
- vázáním spuštění počítače na heslo nebo použití identifikační karty
- využíváním šifrovacích programů
- přidělováním přístupových práv v síti

Zabezpečit data před poruchou počítače lze **zálohováním** (archivací).

Zálohování je přepis dat z pevného disku na jiné zápisové médium (externí disky, flash disky, DVD, místa v síti, cloudová řešení).

Zálohovat musíme:

- často (podle objemu dat)
- pravidelně (nezapomínat)
- pečlivě (nerozptylovat se)
- na kvalitní média či nosiče

Kryptografie

Nejmocnějším prostředkem pro zajištění bezpečnosti dat je užití šifrování. Převedením dat do tvaru nesrozumitelného pro vnějšího pozorovatele se význam sledování a poté možnost nepozorovatelné modifikace nebo padělání dat snižuje téměř na nulu. Ovšem šifrování data neochrání před zachycením při přenosu po síti, pouze při dostatečné síle šifrování (tzn. při vhodné délce klíče) znemožní útočníkovi taková data přečíst.

Kryptografie může být použita k:

- utajení obsahu zpráv
- autentizaci - Zajistitelnost původu zprávy
- kontrole integrity zprávy – informaci může modifikovat a generovat jen autorizovaný subjekt
- K zajištění nepopiratelnosti – příjmu, doručení či původu citlivé informace

Pro ochranu dat se běžně používají různé šifrovací algoritmy se symetrickým nebo asymetrickým klíčem.

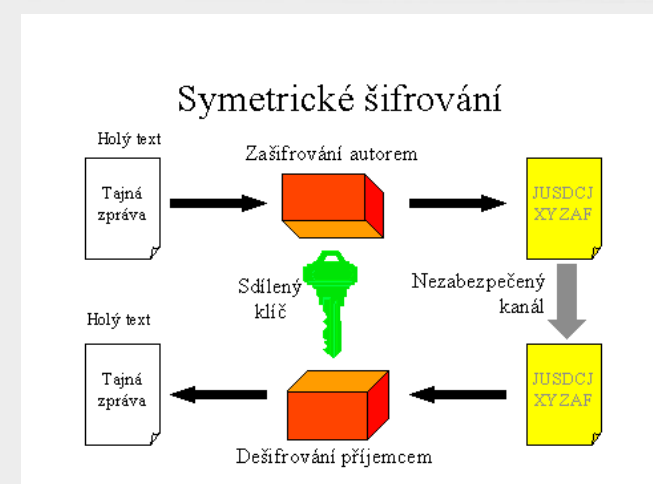
- V případě, že se k zašifrování a dešifrování používá stejný klíč, říká se, že šifra používá symetrickou funkci. Odesílatel i příjemce musí vlastnit stejný klíč. Symetrické šifry jsou rychlé a bezpečné. Příkladem symetrické kryptografie jsou blokové šifry (DES, AES, IDEA) a proudové šifry (RC₄).
- V případě asymetrického šifrování se používají dva klíče, veřejný a privátní klíč. Veřejný klíč slouží k šifrování prostého textu a privátní klíč k jeho dešifrování. Jsou mnohem pomalejší než symetrické šifrování, někdy až tisíckrát. Příkladem asymetrické kryptografie je RSA.

Symetrická kryptografie

Symetrické, též konvenční šifrování je založeno na principu jednoho klíče (také nazývaného sdílený klíč), kterým lze zprávu (data) jak zašifrovat, tak i odšifrovat. Je ale nutné, aby se příjemce i odesílatel (pokud šifrování užíváme při přenosu zpráv) dohodli na jednom (sdíleném) klíči, který budou znát pouze oni dva.

Problémem je tedy distribuce klíče, jak dostat klíč k příjemci, aniž by se ho chopil někdo nepovolaný.

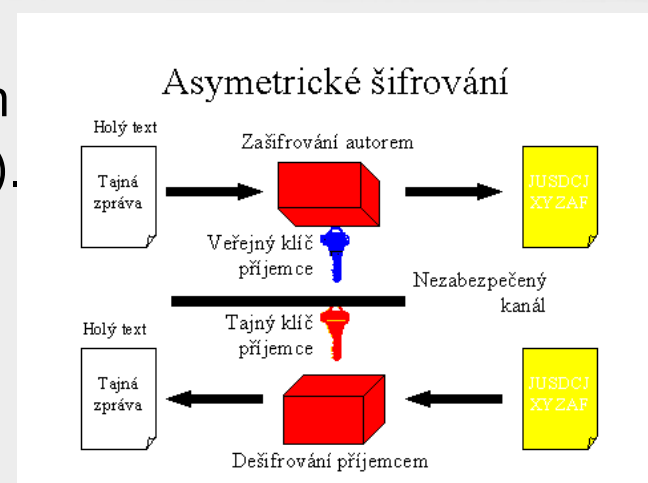
Tento problém ovšem odpadá, pokud šifrování používáme ne při přenosu zpráv, ale při uložení dat na počítači. Zde je pak pouze problém, kde uchovat klíč. Šifrování disků zejména přenosných počítačů se velmi doporučuje.



Asymetrická kryptografie

- Asymetrické šifrování tzv. algoritmy s veřejným klíčem pracují na zcela jiném principu. Pro používání je třeba, aby každý měl své dva klíče - veřejný a soukromý (tajný, privátní). Tyto dva klíče se navzájem doplňují a je-li zpráva zašifrována jedním z nich, lze ji druhým klíčem dešifrovat. Veřejný klíč je znám veřejně, není tedy nijak utajován.

Naopak je vhodným způsobem zveřejňován např. pomocí tzv. certifikačních autorit (CA). Soukromý klíč je naopak vlastnictvím jednoho člověka a je v jeho zájmu, aby se ho nikdo jiný nedozvěděl. Každý si tedy nějakým způsobem chrání svůj soukromý klíč a naopak zveřejňuje svůj veřejný klíč.



Postup asymetrického šifrování

Jestliže chceme něco zašifrovat při přenosu zprávy, tak použijeme veřejný klíč toho, komu je zpráva určena. A protože k dešifrování je potřeba odpovídající druhý klíč z páru (soukromý), na text se může podívat jen tento jediný člověk, který zná soukromý klíč.

Tímto postupem je zajištěno utajení, neboť pouze adresát může zprávu dešifrovat, ale není zajištěna autenticita, neboť dopis mohl kdokoliv poslat a šifrovat pomocí adresátova veřejného klíče.

Tyto algoritmy se dají použít i opačným postupem. Zprávu zašifruji svým soukromým klíčem, takže si ji mohou přečíst všichni, kteří znají můj veřejný klíč. Tento postup má jednu důležitou vlastnost. Dokazuje, že autorem dané zprávy jsem já.

To umožňuje používat kryptografii s veřejným klíčem jak k autentizaci (ověření autora zprávy), tak také k implementaci principu neodmítnutelnosti (tu zprávu jsem prostě napsal).

Chceme-li tedy zajistit jak autenticitu, tak utajení, je nutno použít postupně oba výše uvedené postupy šifrování a poté zase dvakrát postupně odšifrovat.

- privátním klíčem se podepisuje (autentizuje)
- veřejným klíčem toho komu zprávu posíláme se šifruje

Elektronický podpis

Elektronický podpis jsou elektronické identifikační údaje autora (odesílatele) elektronického dokumentu, připojené k němu.

Zaručený elektronický podpis je elektronický podpis v takové formě, která zaručuje i integritu dokumentu a autentizaci podepsaného. Zaručený elektronický podpis je aplikací asymetrické kryptografie (tj. kryptografie s veřejným klíčem).

Používání elektronických podpisů:

- u přiznání k DPH, při podání přehledu o příjmech a výdajích OSVČ
- u přihlášky a odhlášky k nemocenskému pojištění
- při elektronické komunikaci se státní správou, s krajskými a městskými úřady, se zdravotními pojišťovnami
- při podávání žádostí o dotace EU, při žádosti o sociální dávky
- při použití datové schránky
- při podepisování faktur
- jako elektronický podpis PDF dokumentů

Otázky:

- Proč zálohujeme data?
- Co je to kryptografie?
- Jak se jmenuje šifrování za použití jednoho klíče?
- Jak se jmenuje šifrování za použití dvou klíčů (veřejný, privátní)?
- Jaké šifrování používá elektronický podpis?
- Kde můžeme použít elektronický podpis?

- **Použité zdroje:**

THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí*. 1. vyd. Brno: Computer Press, 2005. 344 s. ISBN 80-251-0417-6.

<http://cs.wikipedia.org/wiki/Kryptografie>, [9.12.2012]

http://cs.wikipedia.org/wiki/Digit%C3%A1ln%C3%AD_podpis, [9.12.2012]