

Šifrování

- co to je bezpečný informační systém
- autentizace, bezpečné heslo, jednorázové heslo
- zásada důvěrnosti
- co to je kryptografie
- jaké jsou role šifrování při každodenní komunikaci a práci počítačem
- pojmy: šifrovací algoritmus, šifrovací klíč, délka klíče, šifra
- šifrování z historického pohledu, příklady
- steganografie
- moderní kryptografické algoritmy s privátním klíčem (symetrické – DES, RC)
- moderní kryptografické algoritmy s veřejným klíčem (asymetrické – RSA, Diffie-Hellman)
- hybridní kryptosystémy, jak funguje HTTPS
- metody uložení privátních klíčů

Kódování

- co to je kód a kódování, důvody proč se v IT kóduje
- komprese dat (ztrátová, bezztrátová)
- kompresní poměr, příklad: 10MB do 2MB – 5:1 (80% úspora)
- příklady kompresních algoritmů pro účely archivace dat
- příklady kompresních algoritmů používaných v grafických formátech
- samodetekující kód (EAN)
- kódování používané při přenosu zprávy elektronické pošty podle standardu SMTP
- kódová stránka = znaková sada (ASCII, čeština Windows a ISO, tabulka znaků Unicode, UTF8)
- výpočet UTF-8 při znalosti pořadového čísla znaku v Unicode tabulce
- co to je kodek
- HTML kód

Digitální podpis

- zásada neodmítnutelnosti odpovědnosti (autorství)
- zásada integrity (nezměněnost)
- kryptografické algoritmy s veřejným klíčem (RSA)
- schéma digitálního podepisování zprávy elektronického mailu
- co to je HASH (MD5, SHA-1), vlastnosti hashování funkce
- co to je certifikát veřejného klíče a co obsahuje
- PKI, certifikační autorita (konkrétní příklad státem uznávané CA pro účely komunikace s úřady státní správy, úřady veřejné správy a finančními úřady), registrační autorita (konkrétní příklad)
- úložiště pro certifikáty s podpisovým klíčem
- formáty souborů certifikátů (PKCS#12, DER)
- jak konkrétně funguje digitální podepisování zprávy elektronického mailu v poštovním klientovi (standard S/MIME)

Elektronická pošta

- co to je email, jaké jsou jeho výhody
- kompletní schéma funkce systému přenášejícího email, jaký se používá klientský (2 příklady) a serverový (1 příklad) software
- portálová varianta klienta elektronické pošty (příklad)
- koncepce elektronické pošty podle standardu RFC821 (SMTP protokol a část přenosové cesty, které se říká distribuční systém)
- formát adresy a obsahu zprávy elektronického mailu definovaný standardem RFC822
- jak se na funkci distribučního systému podílí DNS
- protokoly pro práci s mailovou schránkou (POP3, IMAP4)
- proč byl zaveden standard MIME
- přenosové kódování (Quoted-printable, Base64)
- MIME typy
- MIME typ Multipart (Mixed, Alternative, Signed, Encrypted)
- nejčastější SMTP hlavičky (From, To, Cc, Subject, Received)
- jak se zabezpečuje obsah zprávy elektronického mailu (šifrování i podepisování), popis činností v libovolném vybraném poštovním klientovi
- nežádoucí aktivity spojené s elektronickou poštou, co to je SPAM a jak se mu bráníme

DNS a doménová jména

- co to je DNS
- jaký zdrojový port používá DNS server
- software pro DNS servery (BIND)
- jak „naučíme“ klientský počítač, aby se dotazoval příslušného lokálního DNS, který mu přidělí poskytovatel jeho připojení do Internetu
- co to jsou kořenové (root) DNS servery
- konkrétní příklad DNS dotazování z prohlížeče webových stránek
- konkrétní příklad DNS dotazování SMTP serveru při distribuci zprávy elektronického mailu
- zónové soubory a typy záznamů (SOA, A, AAAA, CNAME, NS, MX, PTR)

Popsat příklad:

@	IN	SOA	server.kdesi.cz. franta.kdesi.cz. (
			200605140
			1h
			5m
			1w
			1d
)
	IN	NS	server
	IN	NS	ns.jinde.cz.
	IN	MX	10 server
	IN	MX	20 mail.jinde.cz.
cosi	IN	A	1.2.3.4
	IN	AAAA	2001:718:1c01:1:02e0:7dff:fe96:daa8
server	IN	A	1.2.3.1
www	IN	CNAME	server

- složení doménového jména (typy TLD, domény II. úrovně)
- správce TLD .CZ
- registrátoři domén II. úrovně

Informační systém

- co to je informace a co data
- co to jsou metadata
- co to je informatika (pčítačová simulace, kybernetika, robotika, teorie automatů, programovací jazyky, algoritmizace, archivace dat, zabezpečení dat)
- co to je informační gramotnost
 - gramotnost funkční tj. schopnost zpracovávat informace – porozumět textu, najít informaci a použít jí, numerická gramotnost
 - gramotnost počítačová tj. schopnost práce s počítačem
- co to je informační systém
- cíle informační systémů
 - strategické (řídící, plánující, logistické, výrobní, finanční)
 - taktické (kontrolní, auditové, marketingové, propagační)
 - operační (pro každodenní práci uživatelů, pro zpracování informací)
 - vzdělávací (pro vědu a výzkum)
 - komunikační a informační (redakční, rezervační, knihovnické)
- příklady IS podle oblasti či oboru použití
 - řídicí a manažerské (BI)
 - taktické
 - operativní a komunikační
 - konstrukční (CAD)
 - kancelářské/administrativní (OIS)
 - řízení vztahů se zákazníky (CRM, B2B – Bussines to Bussines)
 - řízení výroby (ERP)
 - správa obsahu (CMS, DMS, redakční systémy)
 - bankovní

- docházkové
 - geografické (GIS)
 - personální
 - IS státní správy
 - IS škol
 - knihovnické
- co to je e-Government
 - co to je e-Learning
 - co to je e-Banking
 - co to je outsourcing informačních služeb
 - co to je bezpečný informační systém
 - zásady bezpečného IS a jakým způsobem se dodržují
 - přerušení aktiva
 - odposlech
 - pozměnění obsahu
 - vytvoření falsifikátu
 - architektura informačního systému
 - klient – server
 - 3-vrstvá architektura (prezenční, funkční a datová vrstva)
 - systémy řízení databází jako základ pro realizaci datové vrstvy (příklady)

Programovací jazyky

- co to je program
- co to je algoritmus, způsoby jeho zápisu (vysvětlit předložený algoritmus znázorněný pomocí vývojového diagramu)
- vlastnosti algoritmu
- dělení programovacích jazyků: procedurální (imperativní) x neprocedurální (deklarativní)
- dělení programovacích jazyků: kompilované (Visual Basic, C#, Pascal) x interpretované (JavaScript, PHP, Visual Basic for Application, VBScript)
- dělení programovacích jazyků: vyšší (většina jazyků) x nižší (Assembler)
- dělení programovacích jazyků: pro událostmi řízené programování x pro tvorbu konzolových aplikací
- procedurální programovací jazyky: strukturované (Basic, Pascal, PHP) a objektově orientované (C#, Java, JavaScript)
- neprocedurální programovací jazyky: např. databázové (SQL)
- jaké programovací jazyky lze použít k přepisu algoritmu, který je zakreslen pomocí vývojových diagramů
- jak program napsaný v jazyce Visual Basic 6.0 komunikuje s databázovým serverem (vysvětlit předložený program)
- Java Platforma (důvody použití jazyka Java)
- vysvětlit pojmy: zdrojový text, binární kód (strojový), bajtový kód
- syntaktické chyby, logické chyby
- rozpoznat zdrojový program: Visual Basic, SQL, JavaScript, PHP

Programové struktury

- způsob zápisu algoritmu pomocí vývojových diagramů, používané značky
- procedury (událostní x obecné), napsat příklady ve vybraném programovacím jazyce
- funkce (vestavěné x obecné) , napsat příklady ve vybraném programovacím jazyce
- předávání parametrů procedurám a funkcím (odkazem, hodnotou), napsat příklady ve vybraném programovacím jazyce
- struktura větvení (binární větvení), příklady ve vybraném programovacím jazyce, zakreslení pomocí vývojových diagramů
- struktura cyklu s předem daným počtem opakování, příklady ve vybraném programovacím jazyce, zakreslení pomocí vývojových diagramů
- struktura podmíněného cyklu, příklady ve vybraném programovacím jazyce, zakreslení pomocí vývojových diagramů
- co to je objekt
- co to je modul v prostředí jazyka Visual Basic 6.0

Proměnné a datové typy

- jednoduché proměnné v jazyce Visual Basic 6.0, zásady označování
- datové typy v jazyce Visual Basic 6.0, základní rozdělení, jak velký je Integer a Byte
- explicitní a implicitní deklarace, napsat příklady ve vybraném programovacím jazyce
- co to je kolekce proměnných – pole, napsat příklady deklarací ve vybraném programovacím jazyce, vysvětlit pojem velikost pole a rozměr pole, pojem index, asociativní pole
- platnost proměnných (globální, lokální)
- datové typy u databází
- operace ve vyšším programovacím jazyce (matematické, logické, relační), napsat příklady ve vybraném programovacím jazyce
- priorita operátorů
- co to znamená, když se řekne strukturovaný datový typ
- ukázat, jak lze načíst číselnou řadu z textového souboru (celá čísla oddělená koncem řádku) do celočíselného pole

Číselné soustavy

- co to jsou číselné soustavy (způsob reprezentace čísel)
- dělení číselných soustav: poziční (každá číslice je dána pozicí v sekvenci symbolů a má v čísle svou váhu, soustava je charakterizována základem) a nepoziční (hodnota číslice není dána jejím umístěním v dané sekvenci číslic: například římské číslice)
- co jsou čísla a co číslice
- vysvětlit příklad římského čísla
- obecný způsob zápisu čísla v poziční číselné soustavě

$$N = n_{k-1}r^{k-1} + n_{k-2}r^{k-2} + n_{k-3}r^{k-3} + \dots + n_0r^0, \text{ kde } r \text{ je základ}$$

vysvětlit poziční číselné soustavy používané v informatice (dvojková = binární, desítková = dekadická, šestnáctková = hexadecimální)

- co to je nibl
- obecný postup převodu z desítkové do libovolné soustavy (postupně celočíselně dělíme základem cílové soustavy, tak dlouho, dokud nedojdeme k hodnotě nula, přičemž zbytky po dělení v opačném pořadí představují hodnoty číslic v cílové soustavě)
- obecný postup převodu z libovolné soustavy do desítkové (sčítáme hodnoty součinů jednotlivých číslic se základem zdrojové soustavy umocněným na pořadové číslo pozice číslice zprava, počítáno od nuly)
- příklady na převody mezi soustavami
 - z dec (do 255) do bin, z bin do dec (do 255)
 - z dec (do 255) do hex, z hex do dec (do 255)
 - z bin do hex (do FFFF), z hex (do FFFF) do bin
- způsoby zápisu příkladů čísel různých soustav v programovacích jazycích, jaké jsou pro ně vyhrazeny datové typy

Operační systémy

- první počítač
- co to je základní programové vybavení (systémové) a co aplikační programové vybavení
- co to je a z čeho se skládá operační systém (jádro – kernel, systémové nástroje)
- základní funkce operačního systému
 - ovládání počítače (spouští programy, předává jim vstupy a získává výstupy)
 - abstrakce hardware (obsahuje API funkce ovladačů, které zjednodušují programátorům práci s hardware)
 - správa prostředků (přiděluje programům systémové prostředky – operační paměť, procesor, pevný disk, I/O zařízení)
- historie operačních systémů (první Unix - 1969, MS DOS - 1981, Mac OS - 1984, první Windows pro DOS - 1990, první Windows NT - 1993, první Linux - 1991)
- rozdělení aktuálních OS a vyjmenovat jejich verze: Linux, Mac OS, Windows, BSD – Solaris
- rozdělení aktuálních OS: serverově orientované, desktopově orientované
- rozdělení aktuálních OS: OpenSource, uzavřený vývoj
- operační systémy PDA, komunikátorů a smartphonů
- co to je BIOS
- uživatelské rozhraní OS (GUI – Graphical User Interface, příkazový interpret – konzolové)
- co to je souborový systém (FAT, NTFS)
- co to je multitasking
- co to je Linuxová distribuce
- virtualizace operačních systémů
- Java platforma
- jak lze administrovat Linux a Windows (uživatelé, práva, nastavení systémových služeb – konfigurace OS, nastavení komunikačního rozhraní počítačové sítě)
- vzdálená administrace operačních systémů

Databáze

- co to je databáze
- typy databází (relační, objektové, speciální)
- struktura relačních databází (tabulka, záznam - entita, atribut, primární klíč, cizí klíč, index), na předloženém příkladu vysvětlit
- vztahy definované mezi entitami (1:1, 1:N, N:M), na předloženém příkladu vysvětlit
- co to je referenční integrita
- co to je systém řízení báze dat (databázový systém)
- vyjmenovat databázové servery (freeware či shareware: MySQL, PostgreSQL, Firebird a licencované: Oracle, MS SQL server, Sybase)
- historie jazyka SQL (vznik 70-tá léta 20. století)
- mezi jaké programovací jazyky patří SQL
- popis jazyka SQL (dotazy manipulující s daty, dotazy pro definici dat, ostatní – pro řízení komunikace a pro definici práv k datům), na předloženém příkladu sestavit dotazy manipulující s daty
- univerzální nástroje pro správu dat SQL databází (PHPMyAdmin, Adminer)
- MS Access (nástroj pro správu relačních databází, který umí pracovat s daty MS-Jet, MS SQL server, Oracle a je součástí kancelářského software MS Office), popsat uživatelské prostředí
- jak program napsaný v jazyce PHP komunikuje s databázovým serverem (vysvětlit předložený program)
- jak program napsaný v jazyce Visual Basic 6.0 komunikuje se souborovým systémem (vysvětlit předložený program)
- systémové databáze (definice uživatelů a skupin v OS Linux, Windows registry apod...)

Tvorba webových stránek

- co to je webová stránka
- statická a dynamicky generovaná webová stránka
- jaký software se používá pro provoz webového obsahu (klient: Windows Explorer, Mozilla FireFox, Opera, Google Chrome a server: Apache webserver, IIS)
- popis HTML (vznik 1991, správa W3C, tagy: párové a nepárové, atributy)
- struktura HTML dokumentu (doctype, html, head, body)
- základní tagy (seznamy, odstavce, nadpisy, tabulky, obrázky, odkazy a kotvy)
- CSS = jazyk pro popis vzhledu dokumentu, způsoby zavedení CSS do dokumentu, syntaxe zápisu
- klientské skriptování = JavaScript, způsoby zavedení skriptu do dokumentu, událostmi řízená technika, syntaxe zápisu
- HTML formuláře
- DOM (Dokument Object Model = API rozhraní pro přístup k obsahu webové stránky z JavaScriptu)
- vysvětlení příkladu webové stránky obsahující CSS, JavaScript a HTML formulář
- co to je DHTML = dynamické HTML (HTML, DOM, JavaScript, CSS)
- rozšiřující technologie webové stránky ActiveX a JavaApplet, důvody použití, způsoby zavedení do dokumentu, v jakém prostředí jsou jednotlivé komponenty prováděny, jak je to s přenositelností mezi jednotlivými platformami, jak je to s bezpečností provozu těchto komponent, příklady použití z praxe

Webová aplikace

- co to je webová aplikace, důvody zavedení této platformy, výhody
- struktura webové aplikace: třívrstvá architektura (vrstva uživatelského rozhraní, vrstva aplikační logiky, vrstva datová)
- příklady webových aplikací z praxe
- co to je Application Service Provider
- vyjmenovat známé webové servery (Apache web server, Internet Information Services, Sun Java System Web Server)
- protokoly http a https, jaké se používají standardně porty
- uživatelské rozhraní webové aplikace pomocí HTML formuláře, popsat HTTP metody GET a POST
- technologie tvorby aplikační logiky webové aplikace
 - serverový scripting (PHP, ASP) – webová aplikace je skript provozovaný v interpretru, který je v přímé vazbě k webovému serveru, často se jedná o modul tohoto serveru
 - CGI a FAST CGI rozhraní – webová aplikace je externím programem, který běží pod operačním systémem serverového počítače a s webovým serverem komunikuje přes speciální rozhraní
 - moduly serverů (ISAPI) – webová aplikace je přímo přeložený modul pro webový server, často se tato technologie používá ve spojení s webovým serverem IIS
 - serverové aplety (servlety) – webová aplikace je javovským bajtovým kódem, který běží na straně serverového počítače v jeho javovém prostředí, vyžadován je speciální webový server, který má povolenu komunikaci s javou
- technologie tvorby datové vrstvy webové aplikace (vyjmenovat SQL servery)
- popsat předložené zdrojové texty webové aplikace napsané za využití PHP a MySQL (v rozsahu projektů PVY z 3. a 4. ročníku)

Počítačová grafika

- z technického hlediska je to obor informatiky, který používá počítač k tvorbě umělých grafických objektů a k úpravě nasnímaných obrazů z reálného světa
- historie počítačové grafiky: 1960 vznik pojmu PG, konec 70. let rozvoj PG, konec 80. let 3D PG, 1995 1. 3D animovaný celovečerní film Toy Story
- 2D počítačová grafika (vektorová, rastrová) a příklady použití
- vektorová grafika: výhody, nevýhody, Bézierova křivka, formáty vektorové grafiky, grafické editory pro vektorovou grafiku
- rastrová grafika: výhody, nevýhody, pixel, DPI, barevná hloubka, barevná paleta (RGB a CMYK), formáty bitmapové grafiky, komprese, grafické editory pro vektorovou grafiku, práce s vrstvami
- hardware: plotter, tiskárna, skener, digitální fotoaparát, tablet
- 3D grafika – příklady použití, základní techniky 3D modelování a reprezentace těles (referování, texturování)
- počítačová animace (animovaný GIF)
- významné firmy na poli počítačové grafiky: Silicon Graphics, Adobe Systems, Netscape, Pixar
- výpočetní příklady podobné těmto:
 - vypočtete velikost souboru s obrázkem, který vytvoří na paměťové kartě digitální fotoaparát s těmito parametry: rozlišení 6 Mpix, bar. hloubka RGB, pro ukládání se používá formát JPG s kompresí 1:5
 - jakou kapacitu paměťové karty potřebujete na dovolenou, pokud chcete nafotit alespoň 200 snímků svým digitálem 4 Mpix, který ukládá při vysoké kvalitě obrázku s kompresí 1:10
 - jak velká musí být videopaměť grafické karty (pro dvourozměrné zobrazení) s maximálním rozlišením 2048x1536 pixelů, karta nabízí až 32 bitovou barevnou hloubku

Multimédia

- co to je multimediální informace (často spojení pohyblivého obrazu s kvalitním zvukem a počítačem jako řídicím systémem za účelem zprostředkování nějaké informace, obecně se jedná o spojení alespoň dvou informačních složek: zvuk, obraz, text, grafika, animace a interaktivita)
- význam multimédií (názornost daná interaktivitou s uživatelem, rychlost a přehlednost předání informace)
- historie multimédií (90. léta 20. století)
- dvě pojetí multimédií:
 - multimediální služby (zpracování a přenos informací – konverzační služby, vyhledávací služby, distribuční služby)
 - multimediální technologie (souhrn postupů a prostředků pro zpracování, archivaci a přenos multimediálních informací)
- dva druhy nosičů multimédií:
 - statická média (text, grafika)
 - dynamická média (animace, zvuky, interaktivita ...)
- jak vypadá multimediální systém (počítač, zvuková karta, grafická karta s reproduktory, videokarta, mechanika DVD, obslužný software, kamera, vizualizér, dotyková tabule, projektor, hlasovací zařízení apod.)
- informace mají velkou kapacitu – z důvodu přenosu a archivace se používá komprese, vyjmenovat kompresní algoritmy ztrátové (jpeg, mpeg, wmv, mp3, wma, aac) a bezztrátové komprese (gif, png, tiff), co to je kodek (program, který dokáže transformovat datový proud – stream, např. DivX, Xvid)
- co to je digitalizace signálu (vzorkování analogového signálu a kódování) – u zvuku vzniká kvalitní signál, když zvolená frekvence vzorkování je alespoň dvojnásobkem nejvyšší frekvence ve zvuku (ucho slyší max. 20kHz – frekvence vzorkování 44kHz)
- jak vzniká zvuková informace

- vytvořená počítačovými nástroji
 - snímáním (ripování) nahrávky
 - syntézou řízených generátorů – MIDI
- jak vzniká video informace
 - snímáním videa kamerou a následná úprava (stříh, ozvučení a titulkování)
 - snímáním (ripování) nahrávky
 - obrazové animace (dynamická interpretace převážně objektů vektorové grafiky)
- formáty pro video
 - avi – obsahuje jednu či více datových stop (zvuk, video, efekty, text titulků), každá stopa obsahuje mediální tok zakódovaný pomocí speciálního kodeku, zaveden společností Microsoft jako součást multimediální technologie Video for Windows
 - mjpeg - používán v digitálních a IP kamerách, každý snímek je zde komprimován zvlášť podle standardu JPEG, MJPEG samotný nemá oficiální standard
 - mpeg - kódování audiovizuálních informací (obraz se zvukem) pomocí digitálního kompresního algoritmu (mpeg2, mpeg4)
- aplikace pro stříh videa (Adobe Premiere, Virtual Dub, Unlead Media Studio, Pinnacle Studio)
 - přehrávače multimediálních formátů (Windows Media Player, BSPlayer, QuickTime, PowerDVD, RealPlayer)
 - uplatnění multimédií (prezentace – např. PowerPoint, e-learningové multimediální vzdělávací programy – často na DVD-ROM nebo na internetu, herní software, simulační software atd...)