Západočeská univerzita v Plzni
FAKULTA PEDAGOGICKÁ

BAKALÁŘSKÁ PRÁCE

ŠIFROVÁNÍ V OBLASTI POČÍTAČŮ – DOKUMENTACE TVORBY E-KURZU

Denisa Wágnerová

Plzeň 2012

Prohlašuji, že jsem bakalářskou práci vypracovala samostatně s použitím uvedené literatury a zdrojů informací.

Plzeň, 29. červen 2012

……
vlastnoruční podpis

OBSAH

1 ÚVOD

Tvorba e-learningových materiálů je v poslední době velice oblíbenou doplňující součástí přípravy výuky. Zvláště, když vyučování probíhá distanční formou, nebo má studující upravenou formu studia, a tedy vytvořený individuální plán. Výuka probíhající distanční formou nebo upravená forma studia může vypadat tak, že prostřednictvím sdíleného prostoru na internetu dáme k dispozici studentům potřebné kurzy, cvičení, podklady či celé přednášky, a student sám si rozhodne, kdy se aktivnímu učení bude věnovat. Celý proces učení tedy může probíhat (a probíhá) bez nutného osobního kontaktu mezi vyučujícím a studentem a e-learningové materiály můžeme také chápat jako velmi efektivní výukovou metodu. Autorský systém ProAuthor, ve kterém je vytvořen přiložený e-kurz, umožňuje i načasování jednotlivých aktivit a student se tedy orientačně dozví čas, jenž na danou aktivitu potřebuje.

Textová část této bakalářské práce tvoří dokumentaci tvorby podpůrného elektronického materiálu, kterým je výukový kurz zabývající se problematikou šifrování. Vedle důvodů výběru tohoto tématu, objasnění struktury e-kurzu, úskalí při práci s autorským systémem ProAuthor či grafickým editorem SmartDraw a dalšími programy, které byly při vytváření použity, lze zde nalézt i obecné informace a rady pro vypracování podobných výukových kurzů.

Nejdříve tedy nastíníme problematiku šifrování, která je náplní výukového kurzu. Dále se podíváme na obsah kurzu, provázanost a strukturu jednotlivých kapitol, které jsou doplněny o cvičení a autotesty. Vybrané programy pro zpracování dat jsou zmíněny rovněž, především pak jejich světlé i stinné stránky, či problémy, které bylo nutno při jejich použití řešit. Jedná se o programy sloužící k tvorbě tabulek a jednoduchých schémat či aplikace pro ukázku typu šifrování. Závěrem je shrnuta celková práce a její možný přínos jejím budoucím studentům.

Bakalářská práce si tedy především klade za cíl vytvořit kvalitní podpůrný elektronický materiál, který by bylo možné v příštích letech používat jako součást výuky předmětu KVD/UIN (Úvod do informatiky pro vzdělávání). Především je snaha o komplexní zobrazení a vysvětlení principů vybraných šifrovacích algoritmů, které provází člověka od starověku až dodnes.

2 PROČ ŠIFROVÁNÍ

Šifrování provází člověka už od pradávna. V dřívějších dobách šlo především o utajení existence zpráv. Důležité bylo zachování některých vojenských taktik, aby se o nich nedozvěděl nepřítel. Postupem času lidé začali vytvářet různé stroje pro šifrování a dnes již jednoduché šifry postupně zdokonalovali. Důležité je ovšem zmínit, že základ dnešních šifer stojí právě na těchto jednoduchých transpozičních a substitučních algoritmech.

Samozřejmě s vývojem informačních a komunikačních technologií se šifrování změnilo do podoby, v jaké ho známe teď. Pokud pomineme letní dětské tábory a skautské oddílové vedoucí, kteří pro své svěřené děti vymýšlejí různé šifrované zprávy či je učí Morseovu abecedu, tak jen málokdo si vezme do ruky tužku a papír a bude šifrovat svou práci pomocí substituční šifry, poté dlouho hledat, kam spis ukryje, aby se nedostal do obávaných rukou. Každý raději vytvoří složku v počítači, kterou zahesluje a heslo poté zašifruje přijatým standardem, jenž by měl být neprolomitelný, aby se k heslu nedostala obávaná osoba a data tak zůstala chráněna. Tyto standardy se samozřejmě časem mění. Některé přestávají být dostačující hned po otestování, jiné používají příliš krátký klíč, u dalších se najde šikovný kryptoanalytik, který algoritmus prolomí bez znalosti správného klíče, ale hlavní problém je stejný – šifra přestává být bezpečná.

Celkově je zde nutno říci, že algoritmy se vymýšlí a koncipují tak, aby současná technika nebyla schopná je bez znalosti klíče dešifrovat. Pokrok ale zastavit nelze a vývoj kvantových počítačů zaručuje v budoucích letech prolomení většiny současných standardů.

2.1 OBSAH KURZU

V přiloženém kurzu se právě postupně díváme na šifry z historického hlediska s důrazem na změny, které se v kryptografii a kryptoanalýze děly. Vývoj je mapován jak u kryptografie – tedy vědy, která nám říká jak šifrovat, tak u kryptoanalýzy, která nám objasňuje dešifrování. Dešifrování může být dvojího typu. První metoda je známá pro nás všechny. Odesílatel pošle zašifrovanou zprávu, my známe klíč a pomocí algoritmu, kterým je zpráva zašifrovaná, ji zpětně dešifrujeme a získáme otevřený text. Druhá varianta je taková, že klíč nemáme, ale přirozeně nás zajímá utajené. Jak tedy zjistit otevřený text? Zde nám přichází na pomoc matematika, statistika, pravděpodobnost či srovnávání

jednotlivých textů. Všechny tyto metody nás dovedou k možnému odhalení klíče a získání otevřeného textu. Samozřejmě je tu i útok hrubou silou (brutal force attack), kdy zkoušíme postupně každý možný klíč do té doby, než najdeme ten jediný správný.

Vedle historického přehledu šifrování, si představíme i některé významné algoritmy, které jsou či byly používány. Odhalíme si tajemství Caesarovy šifry, Vigenérovy šifry, s Alanem Turingem a polskou kanceláří Biura Szyfrow přijdeme na klíč k legendární Enigmě a to hlavní, vysvětlíme si podstatu symetrického a asymetrického šifrování a především jeho aplikaci v protokolech a při elektronickém podpisu.

Symetrické šifrování je vedle asymetrického jedním z pilířů kryptografie vůbec. Podstatou je použití **stejného klíče** jak pro šifrování, tak pro dešifrování textu. Logicky tedy vyplývá, že největší problém zde bude s transportem klíče mezi odesílatelem a příjemcem dané zprávy.

Naopak asymetrické šifrování je založeno na **použití odlišného klíče**. Můžeme si to představit jako zámeček s dvěma klíči. Odesílatel zprávu jedním, veřejným, klíčem zamkne (zašifruje), ale už se k ní nedostane. Adresát svým, soukromým, klíčem zprávu odemkne a dostane se tak i k otevřenému textu.

Schválené a standardizované algoritmy jako např.: **DES, AES, IDEA**, z rodiny symetrických šifer a např.: **RSA či Diffie-Hellmann**, z rodiny asymetrických šifer, jsou používány u protokolů SSL (Secure Sockets Layer), WEP (Wired Equivalent Privacy) i WPA (WiFi Protected Access), jiné jsou součástí **PGP (Pretty Good Privacy)**, další jsou využívány u aplikací společnosti Microsoft. Kurz je sestavený tak, aby potencionální student dokázal pochopit princip vybraného algoritmu, porozuměl jeho filosofii, a na základě vysvětlení a praktického cvičení dokázal tento algoritmus aplikovat. Samozřejmě jsou jednotlivé informace doplněny i o srozumitelný text přibližující vznik a vývoj algoritmu a v některých případech i známé úspěšné i méně úspěšné pokusy o prolomení.

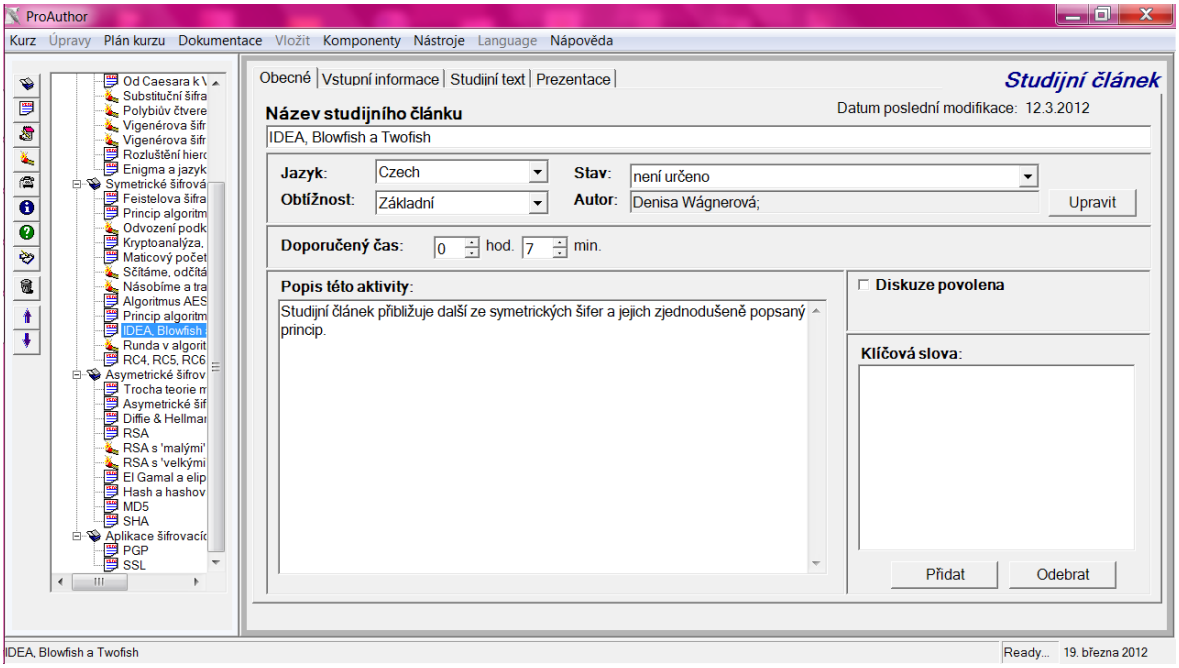
Zajímavou částí je poté závěrečná kapitola, která je věnována problematice hashování, digitálního a **elektronického podpisu**, s nímž se setkáváme prakticky každý den a je součástí veškeré komunikace mezi námi a jakoukoli institucí používající šifrovanou komunikaci. Doplňující pak zůstávají certifikáty a některé obecné informace o problematice legislativy a elektronického podpisu.

3 STRUKTURA KURZU

O celkovém obsahu práce již byla řeč. Nyní je na místě objasnit, v jakých programech byl samotný výukový materiál vytvořen. Budou zde zmíněny programy pro úpravu obrázků, tvorbu schémat či tabulek, ale i samotný autorský systém ProAuthor. Rovněž je zde také na místě vysvětlení členění, provázanosti a struktury jednotlivých kapitol. Není zde kladen důraz na náplň dané kapitoly, spíše tu je snaha zdůvodnit hojný výskyt připravených **studijních článků**, **cvičení a autotestů**, které jsou v kurzu zastoupeny. Také si zde pokládáme otázku, proč je užito cvičení namísto úkolů a autotestů namísto testů. K čemu slouží klíčová slova? Kdo je student, tutor a autor? Co je to studijní aktivita a aktivizační prvek. A co je to vlastně studijní článek…

3.1 PROAUTHOR

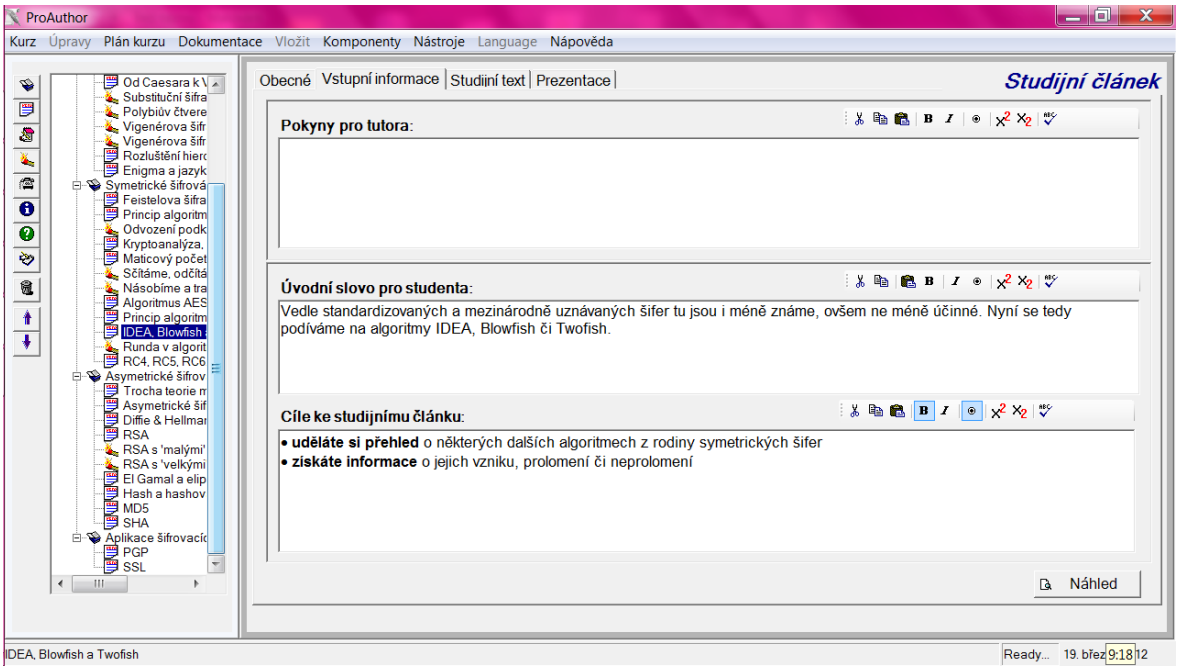
Kurz je vytvořen v autorském systému ProAuthor verze 6.5.1. Nyní se blíže podíváme na některé používané aktivity, jejich tvorbu, použití a především na problémy, ke kterým může docházet. Pro lepší představu o tomto programu je vložen obrázek.



Obrázek 1 – ProAuthor – obrazovka záložky Obecné

Pro přiblížení tohoto vývojového prostředí si popíšeme nejčastěji používané části. Začneme zleva. Vlevo vidíme spoustu ikonek ve sloupečku pod sebou. Tyto ikonky zobrazují vložení dané aktivity. Aktivitou zde rozumíme kapitolu, studijní článek, úkol,

cvičení, diskuzi, anketu, autotest a některé další. Vedle toho sloupečku s ikonkami je panel, ve kterém se postupně ukazují jednotlivé přidávané aktivity, jak po sobě v kurzu následují. Tyto aktivity lze mezi sebou posouvat pomocí šipek či v případě potřeby jednoduše odstranit pomocí ikonky odpadkového koše. Dále pak vidíme vyplněné jednotlivé údaje jako Název dané aktivity, Doporučený čas či Popis aktivity.



Obrázek 2 – ProAuthor – obrazovka záložky Vstupní informace

Po přepnutí do záložky Vstupní informace se zobrazí následující. Levé dva sloupečky už známe – a budou se nám takto zobrazovat neustále po dobu práce v celém kurzu. Klíčové zde je vyplnit tři podstatné složky, které jsou u každé aktivity.

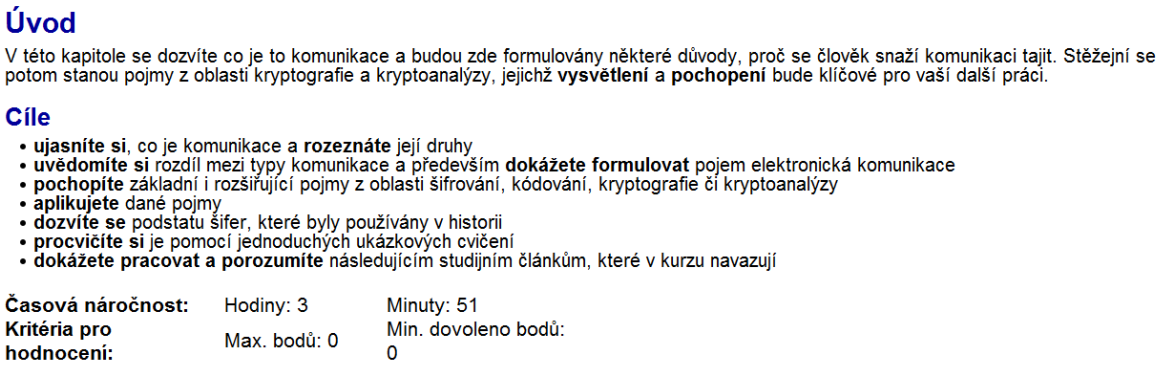
- **Pokyny pro tutora**
- **Úvodní informace pro studenta**
- **Cíle dané aktivity**

Pokyny pro tutora jsou určeny pouze tutorům a jsou rovněž viditelné pouze tutorům. Úvodní informace pro studenta jsou důležité především pro studující jedince. Z těchto informací se dozví prvotní informace, co je ve studijním článku čeká, na co se mají připravit a co nového se dozví. Stejně tak jsou poté formulovány *Cíle* dané aktivity, kde se student přesně dozví, čemu novému se naučí, jaké nové informace se dozví, popř. co si zopakuje ze starší látky.

V kurzu jsou cíle formulovány formou přívětivou především pro studenta, kdy je přesně stanoven cíl, jehož se daná aktivity snaží dosáhnout. Pro příklad uvedeme některý z cílů:

- budete umět aplikovat daný algoritmus
- procvičíte si na jednotlivých ukázkách dané typy šifrování
- uvědomíte si rozdíl mezi symetrickým a asymetrickým typem šifrování
- zopakujete si pojmy, které byly formulovány ve studijním článku Základní pojmy

Cíle také přesně vymezují, čeho by měl studijní článek či daná aktivita dosáhnout. Student potom „*úvod*“ k dané aktivitě vidí například takto.



Úvod

V této kapitole se dozvíte co je to komunikace a budou zde formulovány některé důvody, proč se člověk snaží komunikaci tajit. Stěžejní se potom stanou pojmy z oblasti kryptografie a kryptoanalýzy, jejichž **vysvětlení** a **pochopení** bude klíčové pro vaší další práci.

Cíle

- **ujasníte si**, co je komunikace a **rozeznáte** její druhy
- **uvědomíte si** rozdíl mezi typy komunikace a především **dokážete formulovat** pojem elektronická komunikace
- **pochopíte** základní i rozšiřující pojmy z oblasti šifrování, kódování, kryptografie či kryptoanalýzy
- **aplikujete** dané pojmy
- **dozvíte se** podstatu šifer, které byly používány v historii
- **procvičíte si** je pomocí jednoduchých ukázkových cvičení
- **dokážete pracovat a porozumíte** následujícím studijním článkům, které v kurzu navazují

Časová náročnost:	Hodiny: 3	Minuty: 51
Kritéria pro hodnocení:	Max. bodů: 0	Min. dovoleno bodů: 0

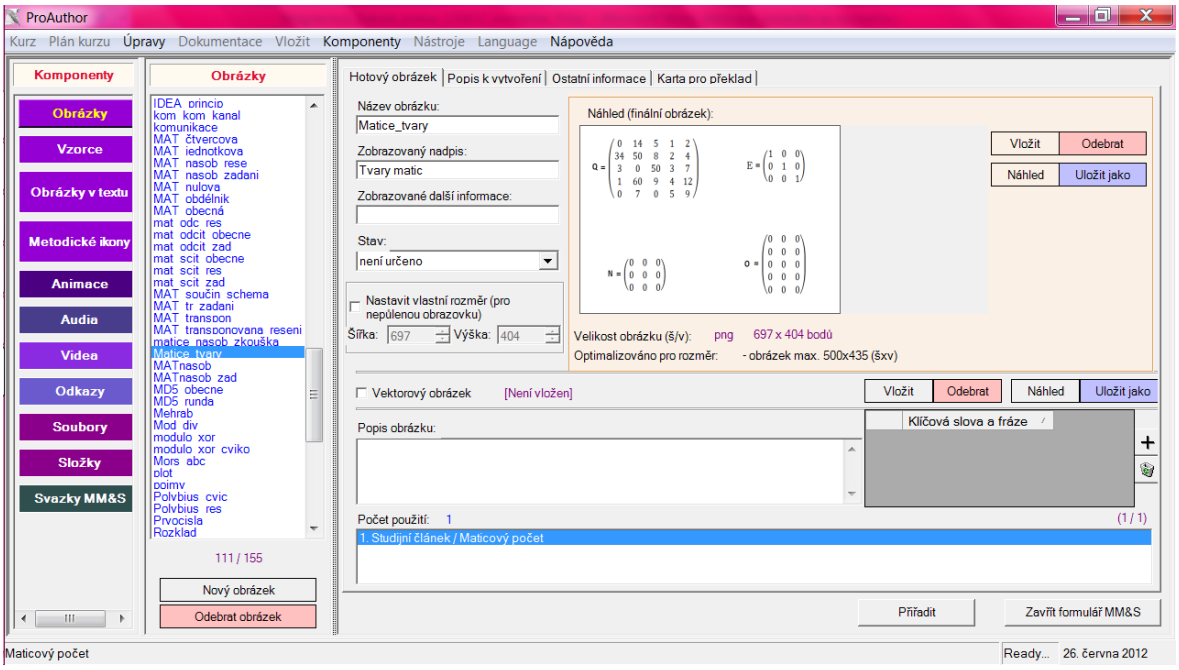
Obrázek 3 – Jak vidí „úvod“ k dané aktivitě student

3.1.1 PROAUTHOR VERZE 6.5.1 – EXPORT A UŽITEČNÉ FUNKCE

Autorský systém ProAuthor představuje možnost tvorby podpůrného výukového elektronického materiálu, který má jednotný vzhled a tudíž může nezávisle na sobě tvořit několik autorů, kteří společnými silami vytvoří obsahovou stránku a vzájemně se již nemusí starat o formátování celého kurzu.

ProAuthor má přednastaveno několikeré formátování nadpisu, obyčejné písmo a dokonce i hypertextový odkaz. Vkládat lze odrážky i číslování. Problematické může býti odsazení řádků, či celého odstavce, neboť nefunguje klávesa tabulátor a musí se tedy myší naklikat a ručně naformátovat potřebné odsazení.

Vkládání MM&S komponent je rovněž velmi jednoduché a intuitivní. Po kliknutí na příslušnou ikonku se zobrazí následující formulář. Zde vlevo vybereme, co chceme vložit, vzorec, obrázek, animaci či kupříkladu soubor. Následuje druhý panel, kde se jednotlivé vkládané komponenty abecedně řadí. Níže uvedený obrázek ukazuje seznam vložených obrázků a popis jednoho z nich. Žádoucí je vyplnění názvu a samozřejmě zobrazovaného nadpisu. Kolonka další informace byla použita právě pro již zmíněné citace k obrázkům, neboť zde napsaný text se zobrazí vpravo dole pod vloženým obrázkem. Užitečným zobrazením je i náhled obrázku a poté dole možnost přiřazení k jednotlivým studijním aktivitám. Kam a kolikrát obrázek (či jakoukoli jinou multimediální komponentu) přiřadíme, se přehledně zobrazí v posledním podlouhlém vodorovném panelu.



Obrázek 4 – Ukázka vložení MM&S komponenty (formulář pro MM&S)

Velmi důležité také je správně „napůlit“ obrazovku, kterou student uvidí v rámci vygenerovaného kurzu. Je důležité dbát správného rozdělení, neboť u většiny článků jsou přiloženy obrázky, pokud by toto rozdělení nebylo nastaveno, mohlo by dojít k tomu, že přiložený obrazový materiál by se nemusel vůbec zobrazit. Naopak u cvičení ProAuthor nenabízí rozdělení žádné a tudíž vše, co je vloženo jako zadání tipy pro řešení i samotné řešení daného cvičení, je poskládáno pod sebe a logicky na sebe navazuje.

Nesmírně důležitou funkcí je náhled. Náhled toho, tak vytvořená aktivita bude vypadat jako vygenerovaná součást e-kurzu.

Další, velice užitečnou funkcí autorského systému ProAuthor je možnost exportu do několika možných zobrazení. Pro studenty je kurz zpřístupněn formou e-booku. Jednou z možností exportu je tedy přímo e-book – elektronická učebnice. Další z možností je vygenerovat kurz pro prostředí moodle. Užitečné a zajímavé poté je si exportovat vytvořený kurz do .rtf souboru jako textový dokument.

3.2 STUDIJNÍ AKTIVITY A AKTIVIZAČNÍ PRVKY

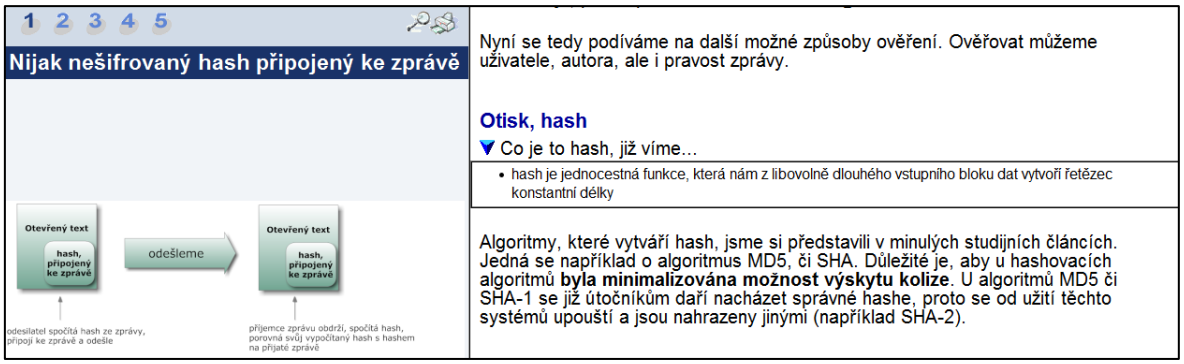
Jak již bylo řečeno, kurz může obsahovat mnoho doplňujících prvků = aktivit. Blíže se budeme věnovat těm, které byly přímo použity, ale pro zajímavost můžeme vložit např.: anketu, diskuzi, úkol, či video s připraveným zadáním. Klíčovým ale zůstává především studijní článek, dále pak připravená cvičení a několik autotestů. Nyní si tedy přiblížíme, proč je použito právě těchto prvků, když ProAuthor jich nabízí mnohem více.

Znovu zopakujeme, že kurz je určen především pro distanční studenty. Je tedy předpokládáno, že se výuce budou věnovat sami. Aby tedy mohli plnit cvičení, měla by jim být k dispozici kontrola. Stejně tak jako u testů je žádoucí, aby se student co nejdříve dozvěděl správnou odpověď.

Studijní článek je studijní aktivita a je zde chápán jako učební text. Je rozčleněn na několik odstavců, obvykle dle částí tématu, kterému je článek věnován. ProAuthor umožňuje do studijního článku vkládat **MMS komponenty**. MMS komponenta je multimediální komponenta, obvykle přehledně zobrazující probíranou látku. Může jí zastupovat jak obrázek, schéma či tabulka, tak video, prezentace, různé typy animací, zvuková stopa, či vložený matematický vzorec. Všechny tyto komponenty mají jeden jediný úkol – usnadnit pochopení probíraného učiva studentům a názorněji poukázat na daný problém.

Vedle doplňujících obrázků a dalších jmenovaných multimédií se student může setkat i s **aktivizačními otázkami,** které většinou doplňují text studijních článků. Tyto aktivizační otázky jsou chápány jako aktivizační prvky a představují je graficky **modré šipečky.** Ty jsou umístěny pod položenou otázkou, a když se student zamyslí, v duchu si odpoví a poté si chce svou odpověď zkontrolovat, stačí na modrou šipku kliknout a v rozbaleném náhledu se připravená odpověď přehledně zobrazí. Otázky jsou oblíbenou

formou zapojení studenta, neboť ho „donutí“ se zamyslet, popř. najít odpověď v jiném článku dříve, než si správnou odpověď rozklikne.



Obrázek 5 – Ukázka aktivizačního prvku – modrá šipka

U výuky, která je vedena distanční formou nebo student má individuální plán, je kladen důraz na pochopení. Je třeba tedy zvážit, jak studijní článek pojmout, čím ho doplnit a jakým stylem ho psát. V kurzu se objevuje snaha o komunikaci se studentem, jsou pokládány otázky k zamyšlení, či takové, na něž již bylo během kurzu odpovězeno a je potřeba opakování, dále jsou vloženy právě již zmíněné modré šipečky. Ovšem ne vždy se zapojení studenta daří a v některých pasážích je minimalizováno z důvodu vyložení těžší látky. Potom je tedy důraz kladen spíše na správný výklad nového učiva a aktivizace probíhá v podobě následného připraveného cvičení.

Úkol nebo cvičení? Tuto otázku by si měl položit každý autor, který bude chtít kapitoly obohatit těmito studijními aktivitami. Každé cvičení má své zadání, tipy pro řešení a i zobrazené řešení. Toto řešení je viditelné autorovi, tutorovi i studentovi. Funguje vlastně obdobně jako aktivizační modré šipečky. Kliknutím na šipečku si rozbalíme řešení daného cvičení. Na rozdíl od cvičení jsou řešení úkolu viditelná pouze pro tutora a autora. Autor kurzu by si měl také uvědomit, že úkol může sloužit především jako kritérium, podle kterého je možné hodnotit práci studenta. Cvičení poté slouží spíše pro upevnění a pro ucelení představy o daném problému (například jaké jsou jednotlivé operace u algoritmu AES a jak po sobě následují). Jednotlivé úlohy jsou v kurzu chápány výhradně jako cvičení. Studentovi je tedy vždycky pomocí modré šipečky odhalen správný výsledek i s postupem řešení.

Obdobný „konflikt“ je řešen u otázky výběru mezi **testem nebo autotestem**? Problematika je zde dosti podobná. Test je určen pro učitele, který si chce s výsledky pohrát sám, opravit je a přihlédnout k možným plusovým bodům, student napíše něco navíc, neví sice přesně, co je daný pojem, ale v problematice se orientuje. Test může být, obdobně jako úkol, chápán jako hodnotící kritérium. Proti tomu autotest je přesně daný a systém ProAuthor ho na základě autorem zadaných správných odpovědí umí vyhodnotit, takže student si může otestovat své dosavadní znalosti a hned se dozví výsledek, na který by v případě klasického testu musel čekat trochu déle.

U obou verzí testů se nabízí nastavení několika typů otázek i odpovědí. Otázka může být otevřená i uzavřená.

Otevřená otázka je taková otázka, na kterou student musí odpovědět sám, vlastními slovy. Již z tohoto je ale jasně patrný hlavní kámen úrazu ve vyhodnocení, kdy ProAuthor není v tomto ohledu zrovna správný kontrolor. Tento typ otázek v kurzu volen není nikdy, neboť se nepředpokládá, že by testy někdo kontroloval. Je také nežádoucí, aby student napsal svými slovy správnou odpověď, kterou by ProAuthor na základě autorovy odpovědi, vyhodnotil jako špatnou.

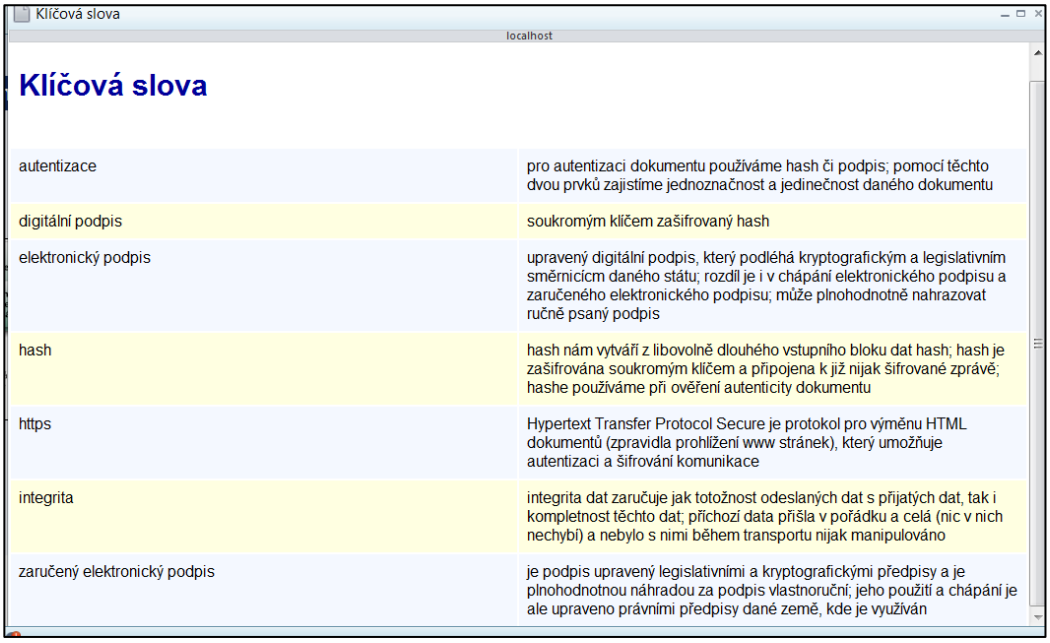
Naopak u **uzavřených otázek**, kdy správná odpověď může být jedna nebo více je jasné, že vyhodnocení probíhá bez pochybení. Dokonce se zde dá navolit i přiřazování např.: pojem a jeho definice, vysvětlení příkladu. Vyhodnocení poté probíhá dle správného přiřazení.

Užitečnou funkcí je také doprovodný komentář, kterým je vhodné doplnit správné odpovědi. Je dobré uvést například, kde byla o této problematice řeč, v jakém studijním článku si student může osvěžit paměť, či v kterém cvičení se příklad rozebíral. Student, pokud si není jistý, se pak může na doporučený článek podívat a zjistit, proč udělal chybu. V kurzu je tedy vloženo několik autotestů, které ověřují dosavadní znalosti studentů. Problémem může být to, že autotest je jenom jeden a pokud si ho student pustí jednou, tak pokaždé se mu zobrazí ten samý. Nicméně co do procvičení se jedná o velmi dobrou formu zopakování probírané látky. Následující obrázek ukazuje jeden z vytvořených autotestů a jeho částečné řešení. Je zde vidět právě použití odlišného typu otázek –

zaškrtávací může mít několik správných odpovědí, označovací právě jednu. U poslední otázky je pak vidět i doplňující komentář.

Obrázek 6 – Ukázka autotestu

Klíčová slova jsou rovněž nedílnou součástí každé aktivity v kurzu. V tomto přiloženém kurzu jsou chápána jako slovníček pojmů. Tento slovníček pojmů je naplněn vysvětleními a definicemi, jež jsou v daném studijním článku těmi důležitými a hlavními. Důvodem je neopakování pojmů. Například rozdíl mezi pojmy kryptoanalýza a kryptografie je uveden hned v úvodních studijních článcích, pokud se k nim někde je možnost vrátit, odkazujeme se spíše přes modrou šipečku, či doporučíme dřívější studijní článek. Formou připomínají klíčová slova pojem a jeho definici, ovšem mají zde pouze doplňující vysvětlující význam. Hlavní vysvětlení stojí stále na souvětích studijního článku.



Obrázek 7 – Klíčová slova

Klíčová slova se mohou umístit jak k celé kapitole, tak k jednotlivým vloženým aktivitám. Zde jsou vloženy především ke studijním článkům, protože tam je dovysvětlení touto formou potřebné a efektivní. Pokud totiž student klíčová slova rozklikne, vybalí se mu v novém okně a může si zopakovat náplň celého studijního článku. Ke kapitolám vložena nejsou, neboť by byla vložena shodná klíčová slova jako u studijních článků. Byla by tedy využita neefektivně, až redundantně.

Časování, o kterém byla řeč již v úvodu bakalářské práce, je jedno z velmi dobrých a užitečných funkcí, které autorský systém ProAuthor nabízí. Časovat může autor vše, od studijního článku přes cvičení, test nebo anketu. Všechny načasované aktivity se poté sečtou a ukazují čas potřebný pro studium celé kapitoly. Analogicky se sečtou časy kapitol a tím se určí celkový čas potřebný pro studium kurzu. Pro autora může být časování v některých případech náročné. Zvláště když kurz po sobě několikrát čte, studijní články neustále upravuje a vylepšuje, vymýšlí a připravuje cvičení, které má poté vlastně sabotovat tím, že odkryje správný výsledek a ještě má odhadnout potřebný čas. Uvedený čas je tedy v kurzu orientační a zprůměrovaný. Je jasné, že student k němu může přihlédnout, nicméně musí brát ohled také na své dispozice. Jak rychle je schopný se učit, chápat, spojit si dohromady jednotlivé dílčí informace či vnímat novou látku. Jak a jestli některé informace znal již z dřívějšího studia a studijní články s touto problematikou bude přeskakovat. Či naopak zase student, který se s některou problematikou setkal v kurzu poprvé, musí přihlédnout k tomu, že bude muset vynaložit většího úsilí při pochopení a procvičení.

Kurz je ale vytvořen s ohledem na obě tyto skupiny studentů a snaží se býti kvalitním podpůrným materiálem.

3.3 STUDENT, TUTOR, AUTOR

V předchozích odstavcích padla slova jako tutor, student a autor – nabízí se tedy otázka komu je kurz určen?

Studentům, kteří si chtějí prohloubit své znalosti nebo získat nové. Kurz je koncipován tak, že informace podává jak pro začátečníky, tak i pro pokročilé. Konkrétně například u studijních aktivit, které se týkají maticového počtu. Maticovému počtu je věnován studijní článek a několik cvičení, kde si student může vyzkoušet připravené

operace. Pro začátečníka je vysvětlen a ukázán obecný postup i jednoduchý příklad; naproti tomu pokročilý student, který absolvoval matematiku a maticový počet tedy ovládá, může tyto aktivity chápat jako procvičení, nebo je vynechat úplně a věnovat je problematice jiné.

Základní informace o každém studijním článku jsou uvedeny v připravené sekci *Úvodní slovo pro studenta*, kde je obvykle dobré uvést, na co studijní článek navazuje, jaké problematice se bude věnovat, a co se student dozví nového. Společně s úvodním slovem pro studenta jsou důležité i cíle. **Cíle** jsou v kurzu vyplňovány formou přívětivou především pro studenta. Vedle studentů je kurz určen rovněž **pro tutory**, kteří podle něho mohou vyučovat.

Tutor je potencionální učitel, který díky návodným informacím v sekci *Pokyny pro tutora,* které jsou jak u kapitol, tak u každého studijního článku, každého cvičení, úkolu, testu i autotestu, dokáže porozumět tomu, co autor kurzu zamýšlel. Do těchto informací lze psát, s čím by mohl mít student problém, či kde nalézt podrobnější informace k probíranému tématu. Také je vhodné, aby na sebe jednotlivé pokyny navazovaly v závislosti na dosavadní úrovni znalostí studenta.

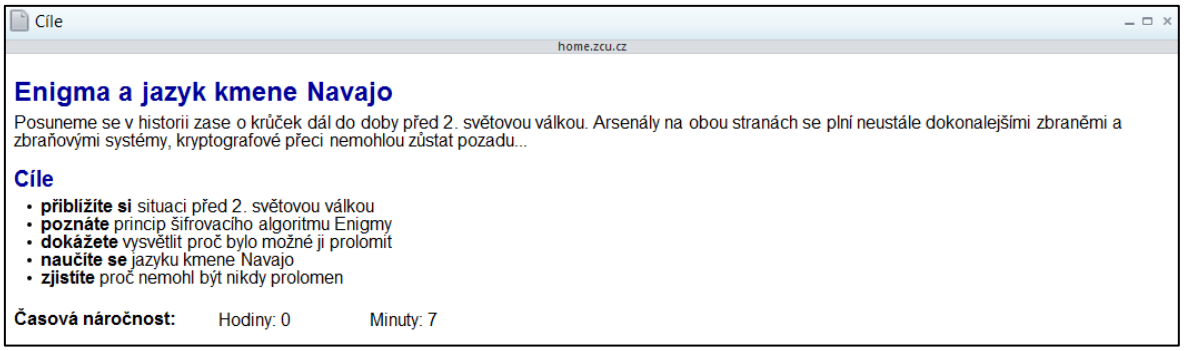
Autorem nazýváme člověka, který se v autorské databázi ProAuthor snaží vytvořit výukový kurz. Používá k tomu danou literaturu, kterou celkem problematicky odcituje přímo v kurzu. K citacím se během práce ještě několikrát vrátíme. Autor také vymýšlí všechna cvičení i autotesty a snaží se vytvářet kvalitní studijní články. Je zodpovědný za návaznost a logickou posloupnost jednotlivých aktivit, které do kurzu zařadí. Rovněž je na něm patřičné načasování jednotlivých aktivit, od čehož se odvíjí celkové načasování kurzu. ProAuthor je velice vhodným pomocníkem při tvorbě kurzu, na kterém se podílí více jak jeden autor. Autorů může být několik a v rámci jednotného vzhledu mohou tvořit kurz a jeho aktivity nezávisle na sobě.

3.4 CITACE

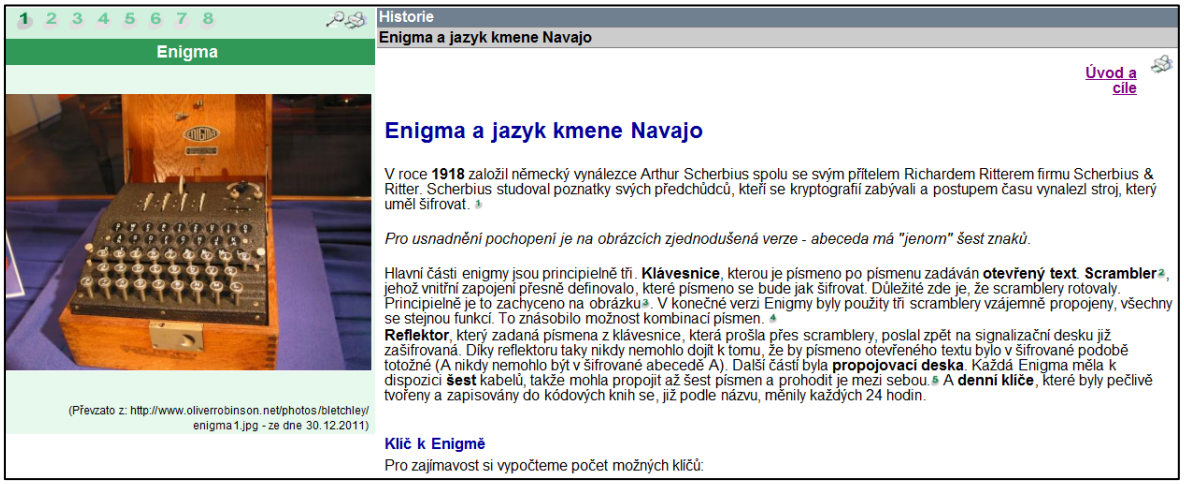
Kamenem úrazu při práci v autorském systému ProAuthor se zdají citace. Citacemi rozumíme jak bibliografické doslovné citace z knih, tak citace z odkazů na internetu. Vedle doslovných citací je zapotřebí uvést zdroj i u doplňujícího obrazového materiálu. V kurzu jsou citace uváděny u každého obrázku pod ním. Vložení citace probíhá ve formuláři

MM&S komponent, kam je v kurzu vkládán do kolonky popis obrázku a zobrazí se pod přiřazeným obrázkem. Obdobně je to u naskenovaných stránek z knih. Doslovné citace mají přiřazené číslo a jsou uvedeny přímo v daném studijním článku dole pod nadpisem Zdroje. Pod tímto nadpisem také najdeme knihy a další zdroje, ve kterých lze nalézt další informace o probírané látce.

Zde jsou za stěžejní pokládány tři knihy - Velký průvodce infrastrukturou PKI a technologií elektronického podpisu (1), Principy digitální komunikace (2) a Kniha kódů a šifer: tajná komunikace od starého Egypta po kvantovou kryptografii (3).



Obrázek 8 – Úvod, cíle a časování ke studijnímu článku – ukázka



Obrázek 9 – Ukázka citace obrázku v již vygenerovaném e-kurzu

4 DALŠÍ POUŽITÝ SOFTWARE

Vedle autorského systému ProAuthor, ve kterém je vytvořen elektronický podpůrný materiál, bylo zapotřebí užití několika dalších programů, které pomohly k finální podobě přiloženého kurzu. Jedná se o některé programy ze sady kancelářského balíčku od firmy Microsoft – především MS Word 2010 a MS Excel 2010, dále pak grafický editor SmartDraw 2010, dílčí úpravy byly prováděny i v Malování.

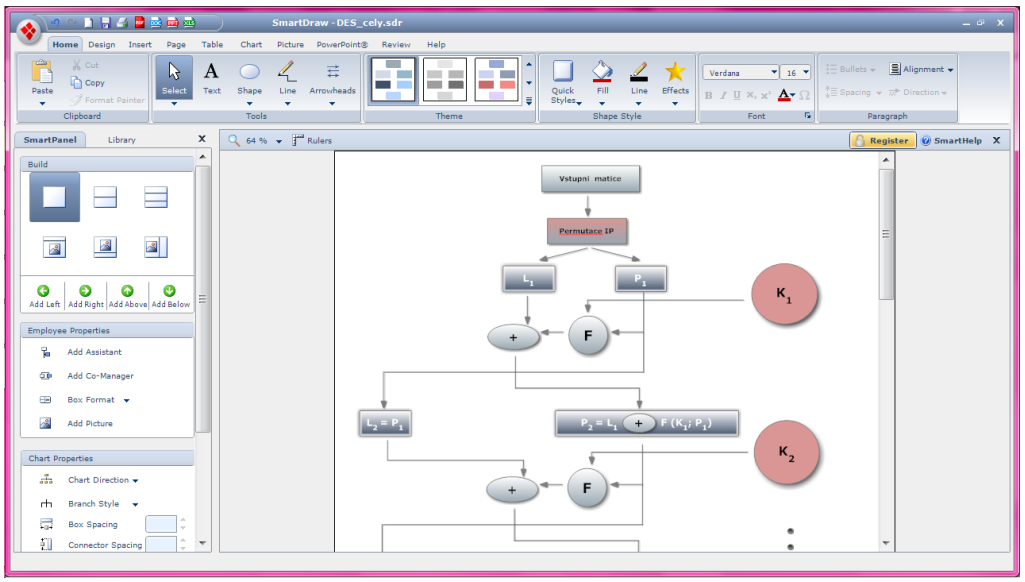
Programy, ve kterých byla vytvářena schémata, pojmové mapy, doplňkové obrázky ukazující jednoduché závislosti a posloupnosti jednotlivých činností, byly využívány především z důvodu větší přehlednosti a s důrazem na názornou ukázku jednotlivých algoritmů, či problematických pasáží v daných tématech.

MS Word 2010 byl použit především pro napsání této dokumentace tvorby kurzu. Byla využita šablona, která byla nadále editována a upravována do finální podoby. Tento program byl ale využit i pro svou funkci počítání jednotlivých znaků v textu, ačkoli přímo na tuto operaci existuje funkce v programu MS Excel. Této funkce bylo využito u cvičení, která se týkala frekvenční analýzy. Rovněž byla tato funkce doporučena i pro budoucí studenty, protože výrazně urychlí práci při plnění daných cvičení.

MS Excel 2010 byl využit především při tvorbě tabulek, které jsou umístěny na několika místech v kurzu. Tabulky ukazují na procentuální výskyt znaků v české abecedě v článku Frekvenční analýza, či jsou využity při ukázkách principů algoritmu DES. MS Excel má rovněž funkci vzestupného či sestupného seřazení buněk, čehož je využíváno u cvičení a tato funkce je také doporučena pro studenty, kteří budou cvičení plnit.

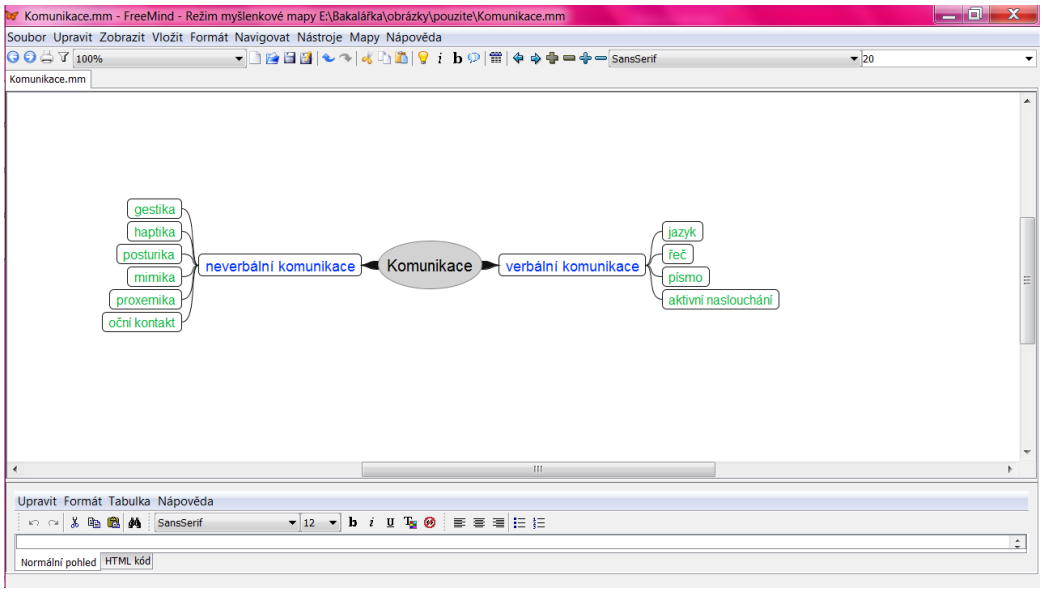
Grafický editor **SmartDraw 2010** nabízí spoustu možností využití. Zde byla využita funkce tvorby pojmových map a posloupnosti algoritmů. SmartDraw umožňuje vytvoření jednoduchých schémat, která podporují snazší pochopení dané problematiky. Bylo vytvořeno velké množství schémat algoritmů, řešení jednotlivých cvičení jsou rovněž pro větší přehlednost vytvořena právě v tomto programu. SmartDraw má také přednastavené možnosti, co se týče barevného vzhledu vytvořeného schématu, umožňuje využití nejrůznějších geometrických obrazců, u spojovacích linií lze nastavit malá šipečka na konci, která ukazuje daný směr, kterým se má jaké větev ubírat. Hlavní výhodou potom je

možnost exportu do mnoha formátů (pdf, doc, bmp, png a mnoha dalších), což je velmi výhodné, neboť všechna obrazová doplnění musí být ve formátu png.



Obrázek 10 – Obrazovka programu SmartDraw

Dobrý je zde i import ze souborů, v rámci další možné úpravy, či začlenění již hotového schématu do schématu většího. Výhodou je zde také vkládání komentářů k vytvořeným grafickým schématům. Toho je využito například u vysvětlení generování subklíčů u algoritmů DES a AES či při vysvětlení operace MixColumns.



Obrázek 11 – FreeMind – obrazovka programu

Menší korekce zvládly i programy **Malování** a **IrfanView**, především pak různé ořezy a dílčí jednoduché úpravy. Použití jednotlivých programů bylo ovlivněno prací, která probíhala buď na osobním notebooku, či na některém ze školních počítačů. Dílčí schémata

byla též vytvořena v programu FreeMind, který je přímo vytvořen pro tvorbu pojmových map.

4.1.1 VLASTNÍ PROGRAM PRO ALGORITMUS AES

Snaha byla i o vytvoření podpůrného programu, do kterého by student zadal hlavní klíč a otevřený text. Program by mu na základě takto zadaných dat ukázal všechny potřebné vygenerované klíče a samozřejmě i postup v jedné rundě. Jednalo se o algoritmus AES. Bohužel byl jako program, ve kterém by byl tento podpůrný prográmek vytvořen, vybrán MS Excel. Tento výběr se hned záhy stal závažnou chybou.

První problém spočíval ve zjištění, že MS Excel neumí sám binárně sčítat, natož sčítat modulo. Další problém se ukázal při operaci SubBytes, která spočívá v nahrazení každého bytu jiným bytem dle tabulky. MS Excel umí do jednoho vzorce dát „pouze“ šedesát čtyři vnořených dílčích vzorečků. Pro operaci SubBytes bylo žádoucí 256 nahrazení – tudíž 256 vnořených vzorečků. Programově to znamenalo místo jedné buňky vytvořit čtyři buňky se stejným vzorečkem, ovšem pokaždé s jinou oblastí nahrazení, a následně za pomoci if zabezpečit vytvoření správně substituované matice.

Operace ShiftRow proběhla sice bez komplikací, neboť se substituovaná matice po řádcích zrotovala a programově to tedy znamenalo pouze přiřazení správně se prohazujících buněk. Operace MixColumns byla tvrdým oříškem již v základech pochopení. Připravit násobení matice maticí v Excelu bylo velmi náročné. Následně ale bylo zapotřebí vymyslet generování deseti subklíčů z hlavního klíče, aby mohl být daný subklíč aplikován v operaci AddRoundKey. Celkově je tento prográmek použitelný pro typový příklad, který je uveden v prakticky všech pramenech, které se o algoritmu AES dají najít, protože byl podle něho konstruován. Byly tedy ošetřeny výjimky (výjimky zde rozumíme Excelové výjimky – sčítání >512, či operace modulo apod.) pouze tak, jak si žádal daný typový příklad. Pokud se zadá podobný, rovněž se šifrování ukáže. Jestliže ale zadáme výrazně odlišná čísla a dojde k přetečení na neošetřených místech algoritmu, jednotlivé buňky tabulek hlásí chybu. Toto se tedy nezdařilo dle představ, a ačkoli to nebylo přímo v náplni bakalářské práce, bude vyvinuta maximální snaha o zprovoznění.

5 JEDNOTLIVÉ AKTIVITY V KURZU

Nyní si popíšeme jednotlivé studijní aktivity podle toho, jak na sebe v kurzu navazují především z hlediska důvodu zařazení a návaznosti na sebe. Co zůstává jejich náplní, zůstává v této textové části upozaděno, neboť o tom je spíše samotný výukový kurz. V některých případech je ovšem nutné a žádoucí obsah zmínit z důvodu pochopení zařazení cvičení či některého studijního článku, který třeba s tématikou šifrování zase až tolik nesouvisí.

Když se začalo uvažovat nad prvotním obsahem kurzu, bylo jasné rozdělení na tři kapitoly – Úvod, Symetrické šifrování a Asymetrické šifrování. Po delší časové pauze, která následovala a byla využita především pro studium materiálů, bylo nutné uvažovat a přehodnotit toto prvotní rozdělení a přinejmenším ho rozšířit o kapitolu Historie. Ve finální podobě je tedy kurz rozčleněn do čtyř na sebe navazujících kapitol, První seznámení, Historie, Symetrické šifrování, Asymetrické šifrování a v závěru práce pak došlo k vytvoření páté kapitoly – Hashe, elektronický podpis a certifikáty, která uzavírá celý kurz.

V případech, kdy je nutné se danou problematikou více zabývat, jsou připravena cvičení, která byla vymyšlena především pro účely pochopení dané problematiky. Příklady tedy jsou originální.

Jednotlivé aktivity kurzu si tedy nyní představíme po kapitolách.

5.1 KAPITOLA: PRVNÍ SEZNÁMENÍ

Úvodní kapitola kurzu je věnována představení problematiky, kterou se bude celý kurz zabývat. Jsou zařazeny i některé pojmy z oblasti psychologie, například pojem komunikace a její složky, či složky neverbální komunikace. Použitá publikace pro definice psychologických termínů je od Zdeňka Vybírala. (4)

Základní pojmy poté představují základní stavební prvky celého pochopení problematiky šifrování. Pro definice základních pojmů bylo rovněž využito vyplnění Klíčových slov, která jsou pokaždé u studijních článků. Kapitola je zakončena autotestem, který zde slouží jako prověřovací prvek pro studenta.

5.1.1 STUDIJNÍ ČLÁNEK: KOMUNIKACE

Aby bylo možné studujícím představit možnosti elektronické komunikace a důležitost chránění a šifrování dat, bylo zapotřebí především definovat pojem komunikace. To proběhlo s důrazem na rozdíly mezi komunikací verbální, neverbální, skrytou a zjevnou a samozřejmě elektronickou a osobní. Jsou zde rovněž vymezeny pojmy z oblasti psychologie, které s problematikou až tolik nesouvisí nicméně v rámci všeobecného přehledu studenta, být zmíněny mohou.

5.1.2 STUDIJNÍ ČLÁNEK: ZÁKLADNÍ POJMY

Kryptografie, kryptoanalýza, soukromý klíč, veřejný klíč, adresát, odesílatel, či útok hrubou silou. To všechno jsou pojmy, kterými je celý kurz doslova protkán. Proto je velice důležité, aby si je student osvojil hned zkraje výukového kurzu a v případě potřeby věděl, kam se pro jejich vysvětlení má vrátit. Stejně tak je již zde definován rozdíl mezi symetrickým a asymetrickým způsobem šifrování.

Tento studijní článek, ač působí velice logicky a jeho začlenění je přinejmenším potřebné, byl jedním z prvních vytvořených studijních článků vůbec. Byl několikrát upravován a neustále obměňován až nakonec se dočkal finální podoby, kde tedy přes důležitost chránění a šifrování dat je studentovi podáno vysvětlení o základních principech šifrování a některých klíčových slovech.

5.1.3 STUDIJNÍ ČLÁNEK: FREKVENČNÍ ANALÝZA

Na základní pojmy plynule navazuje jeden z prvních kryptoanalytických postupů, kterým je frekvenční analýza. Vysvětlení postupu byla ale spíše otázka praktického cvičení. Proto bylo žádoucí zařadit cvičení již sem, do první kapitoly.

Cvičení, která následují, jsou dvě. V prvním je postup ukázán na poměrně rozsáhlém textu, kdy je tato metoda funkční a přínosná. Druhé cvičení naopak demonstruje na krátkém textu neúčinnost frekvenční analýzy.

„Návody“ a zašifrování jednotlivých textů existují i v papírové podobě, kdy byla vymyšlena posunová šifra, jíž byl zašifrován dlouhý i krátký text. Poté byly vytvořeny tabulky s posloupnostmi, které sdělují pravděpodobnosti výskytu znaků v české abecedě a byly čerpány z knihy Principy digitální komunikace. (2) V závěrečné fázi pak následovalo pouhé nahrazování dle pravděpodobností.

5.1.4 CVIČENÍ: FREKVENČNÍ ANALÝZA

Pro ukázku této metody byl vybrán text v českém jazyce; jedná se o úvod z knihy, kterou autorka v době zpracování bakalářské práce četla. Na tento vybraný článek byla aplikována monoalfabetická posunová šifra, která byla náhodně vymyšlená. Záměrně nebyl vybrán text v angličtině, na kterém je ve většině pramenů právě tato metoda ukázána. Český text byl vybrán a zašifrován i z důvodu toho, že frekvenční analýza je založena na procentuálním výskytu znaků v daném jazyce a podle četnosti jednotlivých znaků pak probíhá nahrazení. Toto nahrazení ale v konečné fázi může probíhat i dle úsudku kryptoanalytika a dle smysluplnosti jednotlivých slov či vět. Český text bude přece jen českému studentovi blíže, než text anglický.

5.1.5 CVIČENÍ: FREKVENČNÍ ANALÝZA 2

U tohoto cvičení byl stanoven jeden z cílů tak, aby bylo ukázáno, proč nelze frekvenční analýzu použít vždycky na jakýkoli text. Musel být vybrán text, který je relativně krátký a opakuje se v něm nějaké neobvyklé písmeno, které se v běžné řeči tolik nevyskytuje. Opět je to ve většině pramenů ukázáno na anglickém textu, což se pro studenta, jenž studuje česky a mateřským jazykem je čeština, zdá býti přinejmenším nevhodné. V kurzu je použitý upravený krátký úryvek známé říkanky *Hoří, hoří…* kde se nadmíru vyskytuje písmeno H.

5.1.6 AUTOTEST: ZÁKLADNÍ POJMY

Autotesty jsou si v jádru podobné. Jak již bylo zmíněno, jsou použity pouze uzavřené otázky s možností volby jedné nebo více správných odpovědí, či otázky, na něž je odpovězeno formou přiřazení. Zde jsou otázky zaměřeny na prověření znalosti základních pojmů a frekvenční analýzy.

Autotest je tvořen se záměrem prověřit znalost studenta většinou z dané kapitoly. Jsou v něm obsaženy klíčové momenty, které by si měl z kurzu odnést. Samozřejmě jsou připraveny i otázky typu chyták.

5.2 KAPITOLA: HISTORIE

Historie je součástí snad všech vědních disciplín, protože se v průběhu vývoje dějin, postupně vyvíjely i jednotlivé vědní disciplíny. S ohledem na téma jsou tedy vybrány některé známé šifry, které byly v průběhu dějin vynalezeny, používány, dešifrovány, a

některé z nich i prolomeny, ale na jejichž základě staví dnešní kryptologie. Do této kapitoly je zařazeno také několik cvičení, která mají za úkol ukázat princip jednotlivých šifer a nabízí studentovi možnost vyzkoušení šifrování či dešifrování při znalosti vysvětleného principu.

5.2.1 STUDIJNÍ ČLÁNEK: STEGANOGRAFIE A KRYPTOLOGIE

Proč je studijní článek Steganografie a kryptologie v této kapitole a ne v kapitole První seznámení? Důvod je čistě pedagogický – není dobré na studenta klást vysoké nároky. Je lepší základní pojmy definovat postupně a se stejnou frekvencí je také opakovat a přidávat nová klíčová slova a definice a navíc steganografické postupy jsou blíže rozvedeny v následujícím studijním článku.

5.2.2 STUDIJNÍ ČLÁNEK: OD CAESARA K VIGENÉROVI

Článek přibližuje historický vývoj šifer. Postupně jsou zmiňovány důvody a potřeby proč bylo nutné šifry měnit a vylepšovat. Zajímavé jsou rovněž steganografické postupy, které by v dnešní době již byly zcela nedostačující. Z hlediska důvodu zařazení tedy studijní článek provede studenta vybranými šiframi, které byly v dřívějších dobách používány. Čerpáno bylo především z Knihy kódů a šifer. (3)

5.2.3 CVIČENÍ: SUBSTITUČNÍ ŠIFRA

Při vytváření podpůrných a doplňujících cvičení bylo zajímavé si zkusit jak roli autora šifry, který vymyslí kryptografický postup, tak odesilatele, který zprávu zašifruje a samozřejmě i post adresáta, který přijatou šifru musí dešifrovat, pokud chce získat otevřený text.

U této jednoduché šifry bylo cvičení navíc vymyšleno a zrealizováno velmi rychle, oproti jiným cvičením, které následují dále v kurzu.

5.2.4 CVIČENÍ: POLYBIŮV ČTVEREC

Polybiův čtverec přináší odlišný způsob od předchozího. Byl vybrán jako zástupce tabulkové šifry a student opět může zkusit dešifrovat text, protože správný klíč má k dispozici.

5.2.5 CVIČENÍ: CARDANOVA MŘÍŽKA

Cardanova mřížka je zajímavým příkladem transpoziční šifry. Ve studijním textu se ale většinou setkáváme s problémem, že student si nedokáže princip dostatečně dobře

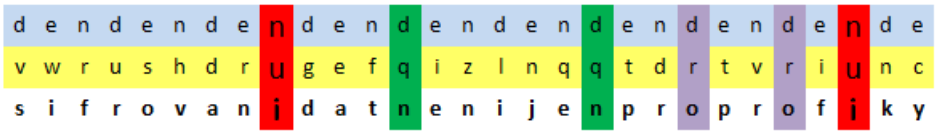
představit. Stejně tak by se tomu mohlo stát i u tohoto způsobu šifrování zvláště v případě, kdy se použije otočná Cardanova mřížka. Proto je ve cvičení ukázán postup a následně vypsáno zadání, které by student měl být schopen splnit.

5.2.6 CVIČENÍ: VIGENÉROVA ŠIFRA

Všechna cvičení až doposud byla založena na monoalfabetických šifrách. Vigenérova šifra je založená na odlišném principu, a proto je vloženo doprovodné cvičení. Polyalfabetické šifry jsou zajímavé použitím více abeced. Toto první cvičení, týkající se Vigenérovy šifry, je zaměřeno na vysvětlení postupu.

5.2.7 CVIČENÍ: VIGENÉROVA ŠIFRA – BEZPEČNOST

Druhé cvičení, které se týká Vigenérovy šifry, je naopak založeno na ukázce problémů, které tato šifra s sebou přináší. Při použití krátkého klíče dochází ke stejnému zašifrování shodných písmen. Problematické bylo vyznačit jednotlivé kolize tak, aby student pochopil, proč je tato šifra někdy prolomitelná. Opakování písmen bylo tedy vyznačeno barevně, mnohdy ne moc vhodně kontrastní barvou, nicméně pro pochopení problematiky se zdá být i tento příklad dostačující.



Obrázek 12 – Ukázka zvýraznění opakujícího se šifrování při použití krátkého klíče

5.2.8 STUDIJNÍ ČLÁNEK: ENIGMA A JAZYK KMENE NAVAJO

Při hledání materiálů pro tvorbu bakalářské práce byla vybrána i publikace, jejímž autorem je Simon Singh a nazývá se Kniha kódů a šifer; tato publikace již byla zmíněna i výše. V této publikaci bylo nalezeno spoustu poutavých a zajímavých informací, ale hlavně přehledné a srozumitelné nákresy šifrovacího stroje Enigma. Vedle těchto nákresů, které jsou samozřejmě přiloženy ke studijnímu článku v kurzu, zde byly uvedeny i některá „šifrovaná“ jména pro bojová letadla. Tato jména byla „šifrovaná“ jazykem kmene Navajo. Dobově spolu tyto dvě události souvisejí a rovněž tento studijní článek uzavírá kapitolu

historie, neboť s těmito šiframi se člověk setká už jen z vyprávění, či při návštěvě některých vojenských muzeí či památečních míst.

5.2.9 AUTOTEST: HISTORIE

Autotest je vložen jako prověřovací prostředek znalostí. Tentokrát je zaměřen na znalosti z kapitoly Historie.

Zde je třeba vložena otázka typu chyták – S jakou frekvencí se měnily denní klíče, které používal šifrovací stroj Enigma?

5.3 KAPITOLA: SYMETRICKÉ ŠIFROVÁNÍ

Symetrické šifrování bylo vyčleněno jako samostatná kapitola, která volně navazuje na kapitolu Historie; tam se skončilo v době 2. světové války. Návaznost je tedy dodržena, avšak členění zde je poněkud odlišné. Kapitola přináší ucelení představy o symetrickém šifrování, jednotlivých principech a postupech. Bylo nutné osvěžit některé ze základních pojmů a připojit na ně pojmy rozšiřující (například blok dat, či bloková šifra). Základním kamenem potom jsou dva algoritmy, DES a jeho nástupce AES, jejichž principy jsou postupně rozebrány ve cvičeních.

Důležité při koncepci kurzu také bylo rozhodnout se, pro koho je kurz určen. Jaké předpoklady a znalosti by měl student mít, pokud by chtěl studovat tento kurz. Byla položena otázka, zdali vysvětlovat většinu principů, či na ně jen odkázat do patřičného oboru. Nakonec byl zvolen kompromis. Je zabíháno i do oblastí jako matematika či logika a jsou vysvětleny i dílčí probíhající operace (například studijní články Matice či Matematika pro kryptology).

U symetrického šifrování jsou vedle studijních článků důležitá i cvičení, která již nemají pouhý doplňující charakter, ale spíše výukový. Kolikrát je postup vysvětlen přímo až u cvičení a poté formulováno přesné zadání, které by student měl být schopen splnit.

5.3.1 STUDIJNÍ ČLÁNEK: FEISTELOVA ŠIFRA A ALGORITMUS LUCIFER

Při vysvětlování algoritmu DES se vyskytl problém. Algoritmus DES není zcela tak úplně DES, ale upravený algoritmus Lucifer, který je založen principu Feistelovy šifry. Tímto byl další studijní článek na světě. Znovu může vyvstat otázka, proč není tento historicky zaměřený článek v kapitole Historie. Odpověď je celkem pochopitelná a zřejmá.

Kapitola Symetrické šifrování byla od sekce Historie oddělena, tudíž všechny informace týkající se vzniku či dalších úprav symetrických algoritmů, jsou umístěny pod příslušným studijním článkem v kapitole Symetrické šifrování. Informace o vzniku a různých soutěžích jsou zde umístěny i z důvodu návaznosti a lepší přehlednosti.

5.3.2 STUDIJNÍ ČLÁNEK: PRINCIP ALGORITMU DES

Princip algoritmu DES byl zpočátku tvrdým oříškem. Nejdříve nebylo dostatečně porozuměno rozdílu mezi generováním klíčů a samotnými iteracemi v algoritmu. Nastoupila tedy osvědčená metoda tužka a papír, kdy se formou pokus omyl, zkoušením permutací či jednotlivých dílčích operací, došlo ke kýženému výsledku a pochopení principu algoritmu. Poté se vyskytl problém – *„jak vyřešit ukázku principu tak, aby tomu rozuměl i někdo jiný než já*“ – studijní článek je tedy doplněn o velké množství tabulek a přiřazení (přiřazením zde rozumíme bit – hodnoty 1,0; a pozice bitů – obvykle 56, či 32 podle toho v jaké části iterace se bity nacházejí).

5.3.3 CVIČENÍ: ODVOZENÍ PODKLÍČE

Odvození podklíče byla již záležitost spíše zábavná, ovšem zdlouhavá. Byl vymyšlen vlastní příklad hlavního klíče, z něhož formou cvičení, jsou generovány podklíče.

5.3.4 STUDIJNÍ ČLÁNEK: DEŠIFROVÁNÍ, KRYPTOANALÝZA, PROLOMENÍ A MODIFIKACE DES

Vedle šifrování a postupu jak šifrovat je důležité vědět i jak dešifrovat, či jak provést kryptoanalýzu bez znalosti klíče.

Naopak je zde stěžejní informace o prolomení algoritmu. Věnován je tomu samostatný studijní článek i z důvodu bližšího zkoumání modifikací algoritmu DES.

5.3.5 STUDIJNÍ ČLÁNEK: MATICOVÝ POČET

Zde se právě setkáváme se třemi studijními prvky (jeden studijní článek a dvě cvičení), které mohou být pro některého studenta zbytečné, ale pro jiného potřebné. Jedná se o maticový počet a vybrané základní operace, které jsou implementovány v následujících algoritmech.

Bylo čerpáno ze skript Lineární algebra (5). Příklady jsou rovněž vymyšlené.

Velice časově náročné zde byly především obecné matice a jejich jednotlivé ukázky u daných příkladů ve cvičeních.

5.3.6 CVIČENÍ: SČÍTÁME, ODČÍTÁME…

Cvičení je určené pro představu o sčítání a odčítání dvou matic. Pro studenta je vložen příklad i obecné znázornění.

5.3.7 CVIČENÍ: NÁSOBÍME, TRANSPONUJEME….

Cvičení je určené pro představu o transponování a násobení dvou matic. Pro studenta je vložen příklad i obecné znázornění.

5.3.8 STUDIJNÍ ČLÁNEK: VYBÍRÁME NOVÝ STANDARD

Jak jinak uvést algoritmus AES než soutěží o nový šifrovací standard. Vzhledem k faktu, že šifrovací standard AES, který představuje algoritmus Rijndael, je používán a je platným šifrovacím standardem i dnes, byla by škoda neuvést soutěž poněkud podrobněji.

Bylo zajímavé hledat informace o jednotlivých kandidátech a předložených návrzích zvláště v závislosti na požadavcích, které byly stanoveny organizátorem soutěže, institutem NIST.

5.3.9 STUDIJNÍ ČLÁNEK: ALGORITMUS AES

Pro pochopení algoritmu AES bylo zapotřebí vysvětlení některých dílčích pojmů. V tomto studijním článku je snaha popsat jednotlivé operace i s příklady a uvést studenta do nového šifrovacího standardu, který je založen na odlišném principu.

Rovněž je důležité procvičit operace sčítání modulo a XOR, které jsou dále hojně využívány.

5.3.10 CVIČENÍ: OPERACE MODULO A XOR

Operace sčítání modulo je zajímavá sama o sobě, zvláště pak, když je implementována jako součást operací v algoritmu AES. Cvičení je zde zařazeno společně s logickou operací XOR.

Je zde tedy snaha o pochopitelné vysvětlení, co je to logická operace, jak probíhá sčítání modulo a co se stane s jedničkou, která o řád přeteče.

V programu SmartDraw bylo vytvořeno již několik schémat. I zde bylo vytvořeno podobné, kde za pomoci šipek a návodných komentářů, je studentovi vysvětleno, co se kdy s čím děje a proč je tomu tak.

5.3.11 STUDIJNÍ ČLÁNEK: PRINCIP ALGORITMU AES

Až zde je poté srozumitelně vysvětlen celý princip algoritmu. Bylo zapotřebí hlavně oddělit od sebe postup generování klíčů a princip samotného algoritmu. Generování klíčů je otázka pochopení spíše u cvičení, avšak postup všech čtyř operací, které probíhají v jedné rundě je vysvětlen již zde.

5.3.12 CVIČENÍ: ODVOZUJEME PODKLÍČE

Problémem při vysvětlování se zde stalo, jak vysvětlit odlišné generování sousedních sloupců. U matice klíče probíhá generování podle sloupců. Sloupce, jež jsou násobky čísla čtyři, mají odlišný výpočet než sloupce ostatní. Bylo tedy zapotřebí vymyslet vysvětlení pro oba typy generování a současně vymyslet, jak vygenerovat nejdříve čtvrtý sloupec, podle první metody a následně skočit na pátý sloupec, který se vytvoří metodou druhou. Toto cvičení může zezačátku působit chaoticky, ovšem nebyl nalezen efektivnější způsob pro vysvětlení.

Toto cvičení tedy klade nároky na studenta, i co se týče pozornosti a důslednosti při výpočtu jednotlivých sloupců.

5.3.13 CVIČENÍ: OPERACE MIXCOLUMNS

Cvičení představující snad nejtěžší operaci v algoritmu AES. Zde bylo zapotřebí hledání informací i jinde než v doporučených zdrojích, protože i při několikerém čtení stále nedocházelo k pochopení, kde se jen tak objeví mixovací matice, či co to je Galoisovo číslo, ale jako velmi kvalitním dílčím zdrojem se zde stala německá wikipedie. Nastoupila tedy obvyklá metoda náčrtků a počítání na papír a po nalezení konečně správného postupu bylo zapotřebí vymyslet, jak to vysvětlit jednoduše, srozumitelně a logicky studujícím kurzu.

Bylo zvoleno rozdělení již při násobení (násobení probíhá jedničkou, dvěma a třemi), následně bylo zapotřebí vysvětlit, kdy se používá aplikace Galoisova čísla a kde se vezme mixovací matice.

Rovněž zde na místě vysvětlit podstatu polynomiálního násobení. Protože násobení matic zde probíhá klasicky jako násobení matice maticí (řádek x sloupec), a toto si mohli studující vyzkoušet na některém z předchozích cvičení. Avšak prvky, které do operace násobení vstupují, se násobí mezi sebou polynomiálně.

Dále bylo nutné studujícím přesně a přehledně vyznačit, kde probíhá jaká operace. Většinou modré kolečko s černým plusem představuje sčítání modulo a nápis XOR operaci XOR. Jednotlivé kroky jsou doplněny i o komentáře, takže v případě potřeby je zřejmé, kdy je nutné aplikovat Galoisovo číslo, a kdy naopak je tento krok zbytečný.

Přínos vymýšlení tohoto cvičení spočívá v zopakování si polynomiálního násobení a rovněž i po delší době zopakování násobení matice maticí.

5.3.14 CVIČENÍ: RUNDA V ALGORITMU AES

Zobrazení a ukázka celého průběhu jedné rundy i s aplikací dílčího podklíče.

Tady se řešil problém, jestli použít dílčích výsledků z dřívějších cvičení, nebo vymyslet nový příklad. Protože ale byla snaha vytvořit ještě podpůrný soubor v MS Excel, kde si studující následně mohou vymyslet své příklady, bylo rozhodnuto využít dílčích výsledků, ke kterým by měli studující dojít při plnění jednotlivých cvičení. Je tedy definováno stejné zadání, a doporučeno využít některých dílčích výsledků, které by studenti měli mít již vyzkoušené a spočítané.

Vymýšlení tohoto cvičení bylo takové vysvobozující, protože bylo poslední u tohoto algoritmu a zároveň propojilo většinu již vypočítaných výsledků a získaných znalostí.

5.3.15 STUDIJNÍ ČLÁNEK: IDEA, BLOWFISH, TWOFISH

Studijní článek doplňuje informace o dalších symetrických algoritmech. Upozaděny jsou Blowfish a Twofish, neboť o Twofish již byla zmínka při soutěži o nový šifrovací standard. Hlavní součástí je zde algoritmus IDEA.

IDEA je zařazená z důvodu, že v principu je velmi jednoduchá a lehká na pochopení. Po složitostech s algoritmy DES a AES bylo zapotřebí vložit nějaký lehčí algoritmus, ale neméně účinný. Pochopení algoritmu IDEA je snadné a doplňující cvičení je spíše bráno jako věc navíc, či zajímavost.

5.3.16 CVIČENÍ: RUNDA V ALGORITMU IDEA

Cvičení je přidáno spíše pro zpestření a jako věc navíc. Obrázek, kterým je toto cvičení doplněno, byl navíc jedním z prvních, který byl v programu SmartDraw vytvořen.

5.3.17 STUDIJNÍ ČLÁNEK: RC4, RC5, RC6…

Rodina algoritmů RCx ukončuje a doplňuje přehlídku symetrických šifer.

Celkově je tato kapitola stěžejní v celém kurzu, neboť ukazuje principy a postupy algoritmů DES a AES. Je zde také snaha o neustálé opakování toho, že hlavním úskalím symetrického šifrování, je transport klíče.

5.3.18 AUTOTEST: SYMETRICKÉ ŠIFROVÁNÍ

Autotest je vložen jako prověřovací prostředek pro studenta, nyní je tematicky zaměřen na symetrické šifrování.

5.4 KAPITOLA: ASYMETRICKÉ ŠIFROVÁNÍ

Asymetrické šifrování je druhou stěžejní kapitolou. Bylo zde ovšem rovněž nutné zakomponovat některé poznatky z jiných oborů, stejně tak jako tomu bylo v předchozí kapitole. Například se zde setkáte s vysvětlením operací div a mod, definuje se zde soudělnost a nesoudělnost čísel, nebo jako modrá aktivizační šipečka tu je otázka, zda je jednička prvočíslo.

Bylo především nutné sem zařadit stěžejní algoritmus, kterým se stal RSA. Protože ale ve skutečnosti se pracuje s mnohem více- cifernými čísly, bylo nutné tuto informaci na několika místech vyzdvihnout. Cvičení, která jsou zde k tomuto algoritmu připravena, jsou rovněž dvě – jedno méně výpočetně náročné, ovšem s nižšími čísly, druhé poněkud delší, ovšem ukazuje shodný postup při použití vyšších prvočísel.

5.4.1 STUDIJNÍ ČLÁNEK: MATEMATIKA PRO KRYPTOLOGY

Jak již bylo předesláno, bylo nutné vysvětlení některých dílčích operací, které spadají spíše do oblasti matematiky.

Pro patřičné pochopení soudělnosti a nesoudělnosti čísel byl například vložen příklad o největším společném děliteli dvou čísel, či naopak nejmenším společném násobku dvou čísel. Postupně návodnými otázkami se došlo k pojmu soudělnost a nesoudělnost, který byl dále definován.

Dále bylo záhodno vysvětlit operaci mod a div. Zde je aplikován odkaz na programování, kde se tato dvě klíčová slůvka potřebují a používají celkem často. Princip operací je pak rovněž vysvětlen formou příkladu.

5.4.2 STUDIJNÍ ČLÁNEK: ASYMETRICKÉ ŠIFROVÁNÍ

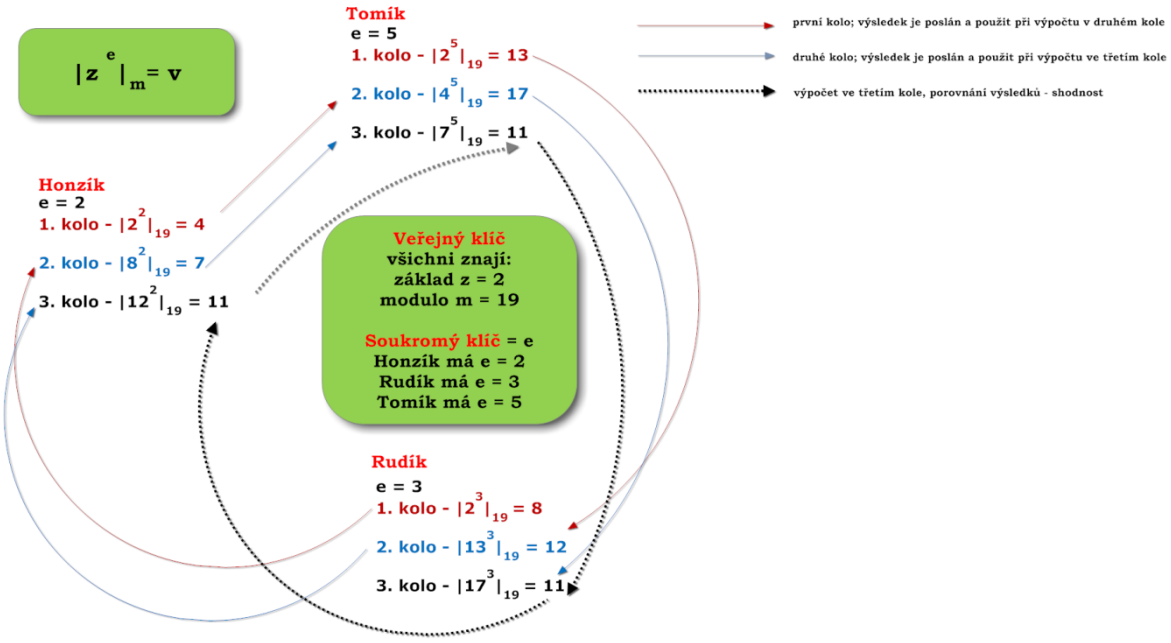
Studijní článek je spíše chápán jako opakovací prvek a než aby přinášel nové informace, tak je v něm spíše opakováno již zjištěné a získané učivo. Je chápán jako odrazový můstek pro vysvětlení algoritmu RSA a protokolu Diffie Hellman.

Navíc po článku o matematické problematice bylo zapotřebí vložit „předěl“, neboť kdyby se hned navázalo pojmem Diffie & Hellman, či rovnou RSA, nebyla by dodržena struktura kurzu a mohlo by to pro studenta být matoucí.

5.4.3 STUDIJNÍ ČLÁNEK: DIFFIE & HELLMAN

Aby byly věci uvedeny na pravou míru i zde, tak algoritmus Diffie-Hellman, či také dále používaný jako DH Protokol, není tak zcela příklad asymetrického šifrování. Tento protokol představuje možnou cestu předání si informací mezi komunikujícími stranami po nezabezpečeném kanálu. Je to tedy metoda, která je implementována při transportu klíče, či výměně informací o klíči.

Proč je tedy DH Protokol mezi asymetrickým šifrováním? Protože jeho myšlenka je vložena v algoritmu RSA.



Obrázek 13 – Ukázka použití principu DH Protokolu

U obrázku, který tento algoritmus doplňuje, bylo problematické znázornit průběh všech tři operací najednou.

Je zde vložena pouze část vytvořeného schématu, z důvodu přehlednosti a především čitelnosti. Bylo zapotřebí ukázat, že komunikující strany si sdělí vždy pouze vypočítaný dílčí výsledek, a že toto sdělení probíhá naráz. Bylo tedy využito pomocných šipek, které jsou vyznačeny jinak barevně pro každé kolo.

5.4.4 STUDIJNÍ ČLÁNEK: RSA

Studijní článek uvádí do problematiky tohoto způsobu asymetrického šifrování. Byl zařazen před konkrétní cvičení, aby mohly být především vysvětleny používané vzorečky při šifrování a dešifrování.

5.4.5 CVIČENÍ: RSA S „MALÝMI" PRVOČÍSLY

Aplikuje znalosti z předchozích článků a především vzorečky ze studijního článku. Bylo zde nutné vymyslet příklad, který bude výpočetně jednoduchý, aby nedošlo k žádným problémům při pochopení, ale zároveň, aby na něm mohl být ukázán postup jak šifrování, tak dešifrování. Jsou použita malá prvočísla, která zajišťují hladký průběh výpočtu.

Ovšem je i zde zdůrazněno, že cvičení je pouhou ukázkou principu. V šifrovacím světě počítačů se používají několika násobně vyšší čísla, aby byl algoritmus RSA bezpečný.

5.4.6 CVIČENÍ: RSA S „VELKÝMI" PRVOČÍSLY

Analogie předchozího cvičení, ovšem zde je ukázán i postup, jakým je řešeno postupné „zmenšování" pro nás již vysokých čísel.

Cvičení je zde také zařazeno z důvodu uvědomění si, jak rychle dokáže počítač pracovat v porovnání s tím, jak dlouho trvá člověku spočítat daleko menší a jednodušší příklad, než je zadáván ke zpracování počítači.

5.4.7 AUTOTEST: ASYMETRICKÉ ŠIFROVÁNÍ

Autotest na konci kapitoly opět předesílá možnost ověření dosavadních znalostí studenta. Je zaměřený na problematiku asymetrického šifrování.

5.5 KAPITOLA: HASH, ELEKTRONICKÝ PODPIS A CERTIFIKÁTY

Poslední kapitola je chápána jako zastřešující a propojující všechny dosavadní postupy a principy. Je v ní vysvětleno hashování a postup při certifikaci dat, ovšem stěžejní a důležité jsou závěrečné studijní články, ve kterých dochází k vyjmenování a

představení protokolů a různých typů bezpečnostních ochran, které využívají dříve vysvětlené symetrické a asymetrické typy šifer.

5.5.1 STUDIJNÍ ČLÁNEK: HASH A HASHOVACÍ FUNKCE

Hashe a hashovací funkce jsou jednou z dalších zajímavých informací, které kurz přináší. Jsou zmíněny jen ve studijních článcích, tudíž pro ně nebyla vytvořena žádná cvičení, nicméně na přiložených obrázcích je alespoň částečně postup ukázán.

Šlo zde spíše o vysvětlení rozdílu mezi šifrováním a podepisováním a důraz je kladen na rozdílné použití soukromého a veřejného klíče.

Díky hashům bylo také možné plynule navázat na problematiku elektronického a digitálního podpisu, protože soukromým klíčem zašifrovaná hash nám vytvoří digitální podpis daného dokumentu.

5.5.2 STUDIJNÍ ČLÁNEK: MD5

Příklad hashovacího algoritmu, jeho postup a důvody, proč již není bezpečný.

5.5.3 STUDIJNÍ ČLÁNEK: SHA

Další příklad hashovacího algoritmu – spíše celé rodiny algoritmů. U studijních článků MD5 či SHA jde spíše o povědomí o existenci některých hashovacích algoritmů, než o přesnou znalost principu. Důležitější je vědět, kde jsou tyto hashe implementovány a co to vlastně hash je.

5.5.4 STUDIJNÍ ČLÁNEK: ELEKTRONICKÝ, DIGITÁLNÍ A ZARUČENÝ PODPIS

Problematické se zde jevilo především vysvětlení rozdílu mezi jednotlivými pojmy. Rozdíly mezi zaručeným elektronickým podpisem a elektronickým podpisem, jsou totiž definovány v právních předpisem dané konkrétní země, která elektronický, či zaručený elektronický podpis k daným operacím používá. Proto jsou zde blíže vyobrazeny úryvky ze Směrnice EU a českého zákona č. 227, Sb. „O elektronickém podpisu“. Mnohdy je velmi zajímavé porovnat rozdíly a naopak shodnosti, které tyto dva dokumenty obsahují.

5.5.5 STUDIJNÍ ČLÁNEK: CERTIFIKÁTY

V návaznosti na elektronický podpis a jeho další specifikace byl představen útok na transport klíče, kterému se dá předcházet za pomoci certifikátu. Právě vytvoření pochopitelného návodu, jak vzniká certifikát, z čeho se skládá, či co předchází jeho vydání,

bylo předmětem přemýšlení. Nakonec vznikl jeden z posledních obrázků, který je rovněž vytvořen v programu SmartDraw, a ukazuje cestu vytvoření certifikátu, aby se zamezilo tomuto způsobu útoku. Certifikáty sami o sobě mají využití u protokolů a způsobů ochrany.

5.5.6 STUDIJNÍ ČLÁNEK: PKI

Studijní článek PKI úzce souvisí i s posledním článkem, protože v sobě implementuje většinu vysvětlených a vyzkoušených principů.

5.5.7 STUDIJNÍ ČLÁNEK: PGP, WEP, WPA, WPA 2, SSL/TSL

Implementace většiny vysvětlených algoritmů se zdála být dobrým zakončením celého kurzu. Tento studijní článek přináší přehled některých protokolů a způsobů ochrany, se kterými se běžný uživatel může setkat a setkává, aniž by věděl, jaké šifrovací či hashovací algoritmy vlastně používá.

Vybráno bylo PGP jako protipól PKI (PGP bylo zpočátku založeno na důvěře mezi komunikujícími na rozdíl od PKI, která užívala certifikační autority pro zjištění totožnosti).

Webové protokoly zajišťující bezpečnost bezdrátové sítě byly zařazeny z důvodu, že dnes si bez známé, používané, oblíbené a neustále se rozšiřující WI-FI sítě, neumíme připojení k internetu na některých místech ani představit.

A konečně protokol SSL/TSL jako bezpečnostní protokol používaný při platbách přes internet.

5.5.8 AUTOTEST: HASH, ELEKTRONICKÝ PODPIS A CERTIFIKÁTY

Závěrečná a poslední studijní aktivita kurzu. Autotest, který slouží pro ověření znalostí ze závěrečné kapitoly Hash, elektronický podpis a certifikáty.

5.6 ZÁVĚREM O TVORBĚ ELEKTRONICKÉHO VÝUKOVÉHO MATERIÁLU

Kurz je ucelenou jednotkou, která může být v případě potřeby využita jako plnohodnotná náhrada klasické kontaktní výuky. Náplň kurzu je úzce zaměřena na problematiku šifrování v oblasti počítačů, stěžejními pojmy jsou symetrické a asymetrické šifrování a především poté vysvětlení principů algoritmů DES a AES. Doplňkovými informacemi jsou principy některých dalších algoritmů a k procvičení slouží připravená cvičení. Své znalosti může student otestovat v připravených autotestech.

6 ZÁVĚR

Tvorba elektronických materiálů s sebou přináší řadu nových zkušeností, nabytí či zdokonalení se v již stávajících dovednostech, ale především vymýšlení vlastních příkladů a cvičení jako podpůrného a názorného prvku. Pro autora je mnohdy těžké určit, co studující již bude znát, a co by se mělo v kurzu objevit jako možné neznámé. Autor může předpokládat a doporučit kurz přiměřené skupině studujících, ale plně už nedokáže odhadnout jejich dispozice ani například přesný čas, který budou na intenzivní studium kurzu potřebovat. Stejně tak mohou být některé informace brány jako opakující a jiné jako nové, které rozšiřují vědomostní obzory studujícího.

Zajímavé pro autora také je vyzkoušet si role všech zainteresovaných osob – nejdříve vymyslí koncept daného cvičení, jeho náplň, rozdělí dílčí úkoly či doplní cvičení obrázky. Poté se pomyslně stane studentem, který si dané cvičení chce vyzkoušet – tudíž své vymyšlené cvičení vlastně správně vyhotoví. Pro lepší znázornění a pochopení vytvoří obrázky či textovou dokumentaci.

Rovněž bylo velmi zajímavé a přínosné vytvořit podpůrný prográmek, který demonstruje průběh algoritmu AES.

Překážky, které bylo nutné překonávat a řešit, byly mnohdy přínosné, neboť se ukázala lepší a efektivnější cesta pro řešení daného problému. Bohužel někdy se nezadařilo dle představ, ovšem byla vynaložena maximální snaha o napravení a zdokonalení.

Celkově bakalářská práce stojí na tvorbě podpůrného elektronického materiálu, kterým je výukový kurz s tématem Šifrování v oblasti počítačů. Textová část slouží jako dokumentace této tvorby a zachycuje myšlenkové pochody při tvorbě a některé z komplikovanějších problémů. Nicméně přese všechny problémy byla práce úspěšně dokončena a může tedy sloužit jako výukový kurz pro zájemce z řad studentů.

7 SEZNAM OBRÁZKŮ

8 SEZNAM LITERATURY

1. **Dostálek, Libor a Vohnoutová, Marta.** *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu.* Brno : Computer Press, 2006. ISBN 80-251-0828-7.

2. **Jiroušek, Radim.** *Principy digitální komunikace.* Voznice : Leda, 2006. ISBN 80-733-5084-X.

3. **Singh, Simon.** *Kniha kódů a šifer: tajná komunikace od starého Egypta po kvantovou kryptografii.* Praha : Dokořán, 2009. ISBN 978-807-3632-687.

4. **Vybíral, Zdeněk.** *Psychologie komunikace.* Praha : Portál, 2009. ISBN 978-807-3673-871.

5. **Tesková, Libuše.** *Lineární algebra.* Plzeň : Západočeská univerzita, 2010. ISBN 978-80-7043-966-1.

9 RESUMÉ

Creating of software for a lecture gives new experiences and improves skills. The main purpose of that is creating of exercises and lessons as supportive object. For the author it is hard to specify student's knowledge and what could be unknown for students. Although the author can recommend it to group of chosen students, the author cannot estimate time for a session and student's abilities. In the same way an information included with course can be know or unknown for some of student's.

It is interesting for the author to try variety of position of concerned people. Firstly the author works out the exercises and after then gets role of student to realize one's own thoughts and requirements. The author composes a pictures and white papers for better understanding.

Also it was really interesting and helpful to create program to demonstrate AES algorithm. The author had to get over many problems and it gives him new experiences and possibilities of ways to result the problems.

Unfortunately it couldn't be solved everything but the author left no stone unturned.

The bachelor thesis is base on creating of software for a lecture of encryption in computers. The text of the work describes creating of the software and shows trains in complicated problems. For all that this work has been finished and it can be offer to student.