A. Používateľská príručka internetovej prezentácie IDEA

A.1 Príručka šifrovacieho java appletu

A.1.1 Inštalácia

Inštalácia appletu na počítač spočíva v nakopírovaní adresára IDEA, ktorý obsahuje všetky skompilované triedy (s príponou *.class*) : Applet1.class, Applet1&1.class, Applet1&2.class, .. až Applet1&47.class a súboru Applet1.html. Applet spustíme otvorením súboru Applet1.html v internetovom prehliadači. Nutnou podmienkou je, aby na danom počítači bola nainštalovaná java verzie j2sdk1.3.0_02 alebo vyššia prípadne prehliadač Internet Explorer verzie 6.0.2800, ktorý je súčasťou Windows XP SP1.

A.1.2 Tlačidlá

Prechádzanie medzi jednotlivými stránkami appletu je možné kliknutím myši na jednotlivé tlačidlá. Ich význam je nasledovný (kliknutím na ne sa vykoná nasledovná akcia):

- prechod na predchádzajúcu stránku

- prechod na ďalšiu stránku

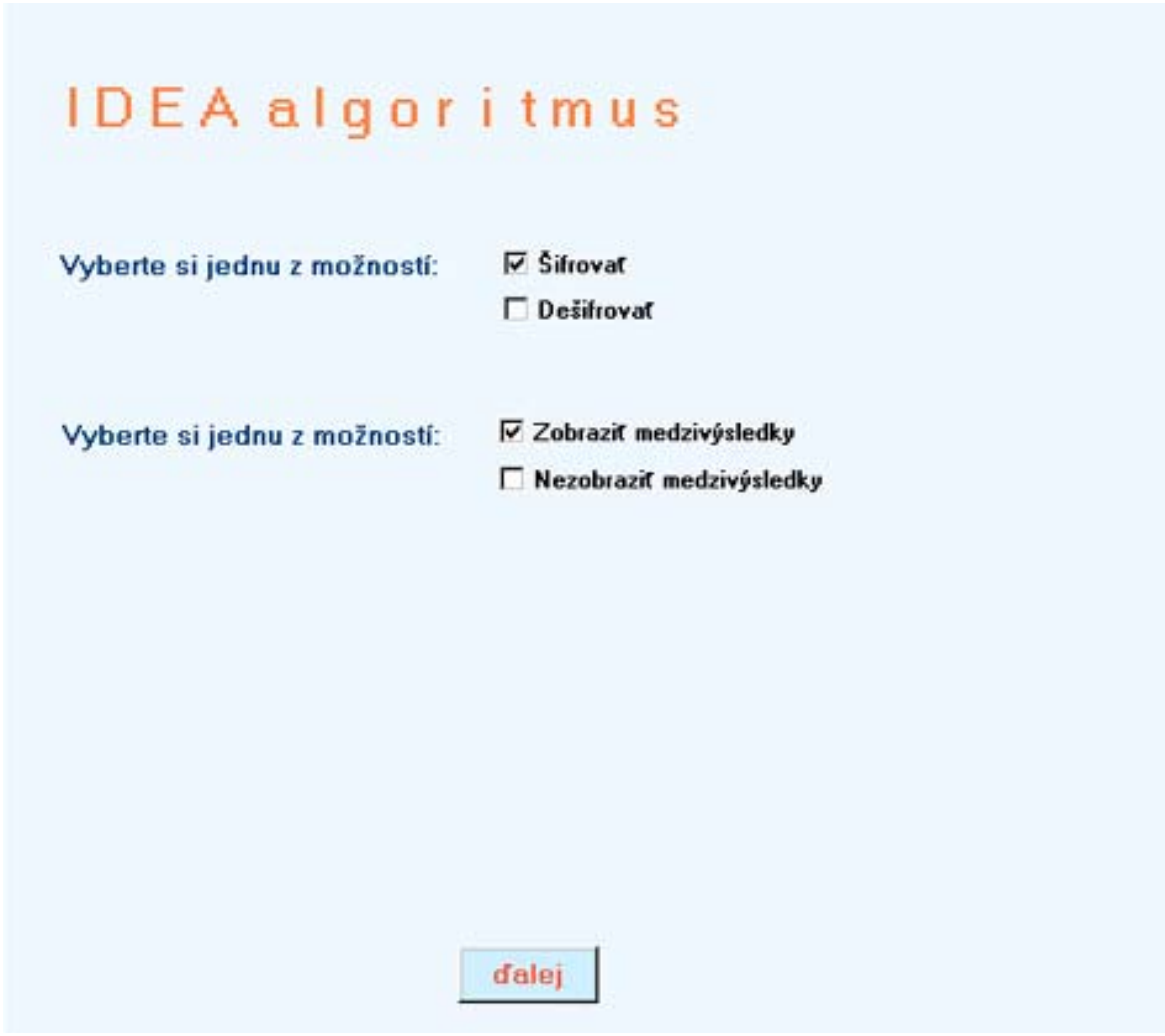
- vymaže všetky formuláre (okienka) na danej stránke

- prechod na úvodnú stránku

Význam ďalších dvoch tlačidiel bude vysvetlený neskôr.

A.1.3 Návod na použitie

Tento návod opisuje postup práce so šifrovacím appletom. Po spustení appletu v prehliadači sa zobrazí úvodná stránka v podobe ako je na obrázku (obr. č. 1). Kliknutím na jednu z možností si môžete vybrať, či zadané vstupné údaje budete šifrovať alebo dešifrovať. Druhá voľba slúži na určenie, či sa budú zobrazovať medzivýsledky po každom z ôsmich kôl šifrovania resp. dešifrovania. Kliknutím na tlačidlo ďalej sa zobrazí nasledovná stránka, ktorá je na obrázku (obr. č. 2).



Obr. č. 1: Úvodná stránka appletu

Do príslušného textového poľa treba zadať kľúč, ktorý sa použije na šifrovanie resp. dešifrovanie. Zadáva sa v hexa znakoch (povolené sú znaky 0,1,2,3,4,5,6,7,8,9,a,b,c,d,e,f ako aj A,B,C,D,E,F) a jeho dĺžka musí byť 32 znakov - 128 bitov. Na obrazovke sa zobrazuje počet zatiaľ zadaných znakov. Ak ich je 32, zobrazí sa hlásenie: „Dĺžka kľúča je v poriadku“. Ak zadáte väčší počet znakov (napr. 33), zobrazí sa varovné hlásenie: „Dĺžka kľúča musí byť 32 hexa znakov a nie 33“. Ak zadáte znak, ktorý nepatrí do hexa abecedy (napr. „Z“), zobrazí sa varovné hlásenie: „Znak Z nepatrí do hexa sústavy“. Význam dvoch tlačidiel je nasledovný:

- doplní nuly pred zadaný kľúč tak, aby jeho dĺžka bola 32 hexa znakov

- doplní nuly pred zadaný kľúč tak, aby jeho dĺžka bola 32 hexa znakov

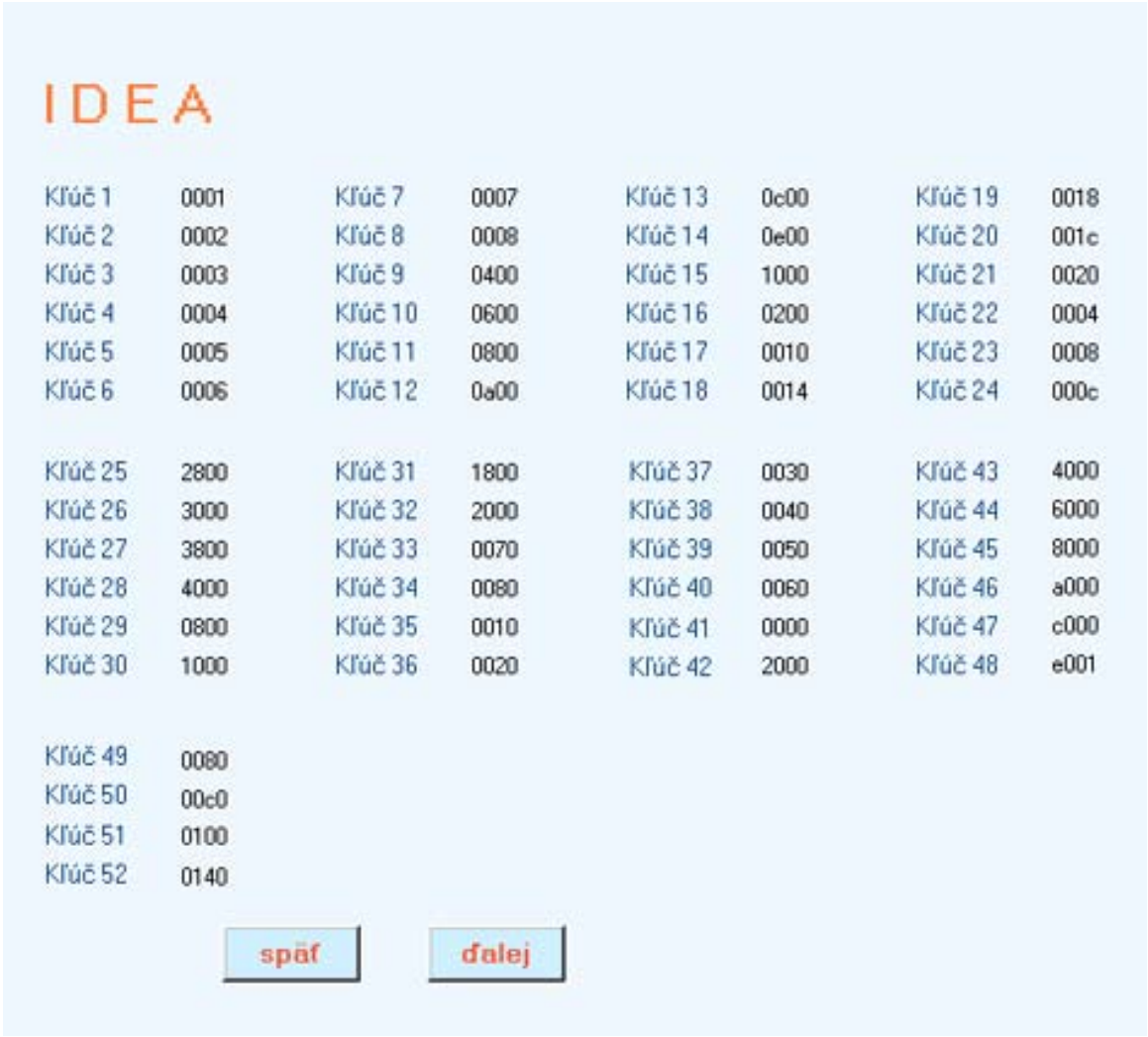
Obr. č. 2: Zadanie kľúča

To, ako budú vyzerať ďalšie stránky appletu záleží od zvolených možností v úvodnom menu. Preto je ďaľej návod rozdelený na štyri kapitoly, ktoré opisujú jednotlivé kombinácie zvolených možností. Na nasledujúcu stránku sa dostanete kliknutím na tlačidlo „ďalej“ (je to možné len po zadaní kľúča správnej dĺžky, ktorý obsahuje len znaky hexa abecedy). Nasledujúce príklady budú pracovať s kľúčom 00010002000300040005000600070008.

A.1.3.1 Šifrovanie so zobrazením medzivýsledkov

Po zadaní šifrovacieho kľúča a stlačení tlačidla „ďalej“ sa zobrazí stránka z obrázka (obr. č. 3). Obsahuje 52 podkľúčov vytvorených zo zadaného šifrovacieho kľúča, všetky sú zobrazené v hexa sústave a ich dĺžka je 4 znaky - 16 bitov. Prvých 48 podkľúčov je rozdelených do ôsmich stĺpcov po šesť. Podkľúče 1 až 6 sa použijú v prvom

kole transformácie, podkľúče 7 – 12 v druhom kole atď. Podkľúče 49 – 52 sa použijú v záverečnej výstupnej transformácii. Kliknutím na tlačidlo „ďalej“ sa zobrazí nasledujúca stránka appletu, ktorá je na obrázku (obr. č. 4).



Obr. č. 3: Podkľúče pre šifrovanie

Do príslušného textového poľa treba zadať údaje, ktoré sa budú šifrovať. Tiež sú zadávané v hexa sústave a ich dĺžka musí byť 16 znakov, teda 64 bitov. Podobne ako pri zadávaní kľúča aj tu je zobrazovaný počet zadaných znakov a po zadaní viac ako 16 znakov (napr. 20) vás applet upozorní nasledujúcim hlásením: „Dĺžka údajov musí byť 16 hexa znakov a nie 20“. Údaje sú rozdelené do štyroch blokov, z ktorých každý má dĺžku 4 hexa znaky t.j. 16 bitov.

Obr. č. 4: Zadanie údajov

Nasledujúca stránka, ktorá sa objaví po kliknutí na tlačidlo „ďalej“, je zobrazená na obrázku (obr. č. 5). Obsahuje medzivýsledky po prvom kole šifrovania. X1, X2, X3 a X4 sú vstupné bloky údajov a SK*i* je *i*-ty kľúč i je z intervalu 1 až 6. Ostatné skratky sú len označenia pre jednotlivé pomocné premenné na uchovanie medzivýsledkov. Posledné štyri riadky sú zvýraznené a predstavujú hodnoty, ktoré budú použité ako vstup nasledujúceho kola šifrovania. Význam jednotlivých znakov vyjadrujúcich matematické operácie je nasledovný:

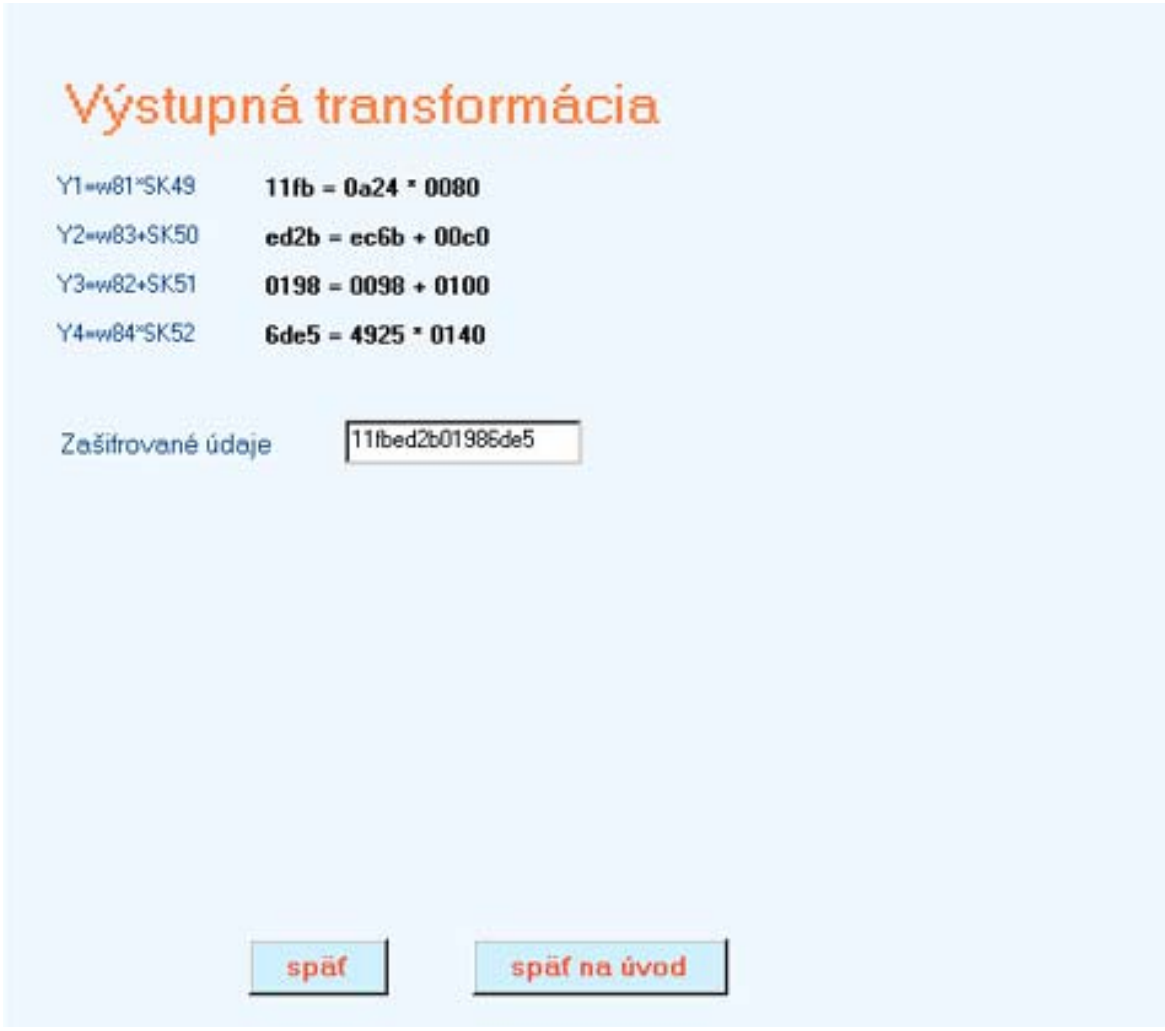
* – operácia súčin modulo $2^{16}+1$

+ – operácia súčet modulo 2^{16}

xor – operácia XOR

Obr. č. 5: Kolo 1

Počet kôl pri šifrovaní je osem a prepínať sa medzi nimi možno klikaním na tlačidlá „ďalej“ a „späť“. Kliknutím na tlačidlo „ďalej“ na stránke zobrazujúcej ôsme kolo šifrovania sa zobrazí výstupná transformácia - obrázok (obr. č. 6). Zašifrované údaje sú zobrazené v textovom poli a môžu byť označené a následne skopírované. To sa dá využiť napríklad pri overovaní výsledku šifrovania, kedy zašifrované dáta zadáme ako vstup pre dešifrovanie (kľúč musí ostať nezmenený) a výsledkom by mali byť pôvodné údaje. Dĺžka zašifrovaných údajov je 16 hexa znakov – 64 bitov.



Obr. č. 6: Výstupná transformácia

A.1.3.2 Šifrovanie bez zobrazenia medzivýsledkov

Po zadaní šifrovacieho kľúča a stlačení tlačidla „ďalej“ sa zobrazí stránka z obrázka (obr. č. 4). Tzn. že sa nezobrazia jednotlivé podkľúče, čo je rozdiel oproti predchádzajúcej kapitole. Po zadaní vstupných údajov a kliknutí na tlačidlo „ďalej“ sa v spodnej časti obrazovky zobrazia zašifrované údaje - obrázku (obr. č. 7). O vstupných aj dešifrovaných údajoch platí všetko, čo bolo spomenuté v predchádzajúcej kapitole. Pokiaľ používateľ chce zašifrovať ďalší (iný) blok údajov tým istým kľúčom, stačí tieto údaje zadať do príslušného okienka a po stlačení tlačidla „ďalej“ sa zobrazia príslušné zašifrované údaje. Môže taktiež kliknutím na tlačidlo „vymazať“ vymazať všetky údaje nachádzajúce sa na tejto stránke a až potom zadať nové údaje na šifrovanie (tento postup je prehľadnejší).

Obr. č. 7: Dešifrovanie bez zobrazenia medzivýsledkov

A.1.3.3 Dešifrovanie so zobrazením medzivýsledkov

Po zadaní dešifrovacieho kľúča a stlačení tlačidla „ďalej“ sa zobrazí stránka na obrázku (obr. č. 8). Opäť sú rozdelené podobným spôsobom ako bolo spomenuté v kapitole 1.3.1. Nasledujúci postup je zhodný so šifrovaním, ktorý je uvedený v kapitole 1.3.1. Rozdiel je len vo výsledku, ktorý predstavuje dešifrované údaje.

Obr. č. 8: Podkľúče pre dešifrovanie

A.1.3.4 Dešifrovanie bez zobrazenia medzivýsledkov

Postup zobrazovaných stránok je zhodný s postupom v kapitole 1.3.2. Zadáva sa kľúč, ktorý je použitý na dešifrovanie. Jeho rozdelenie na podkľúče nie je zobrazené. Po zadaní údajov sú tieto dešifrované a výsledok sú dešifrované údaje dĺžky 16 hexa znakov – 64 bitov.

A.2 Príručka interaktívnej prezentácie pomocou Flash

A.2.1 Požiadavky

Na korektné prehrávanie interaktívnej prezentácie odporúčame nasledujúcu zostavu:

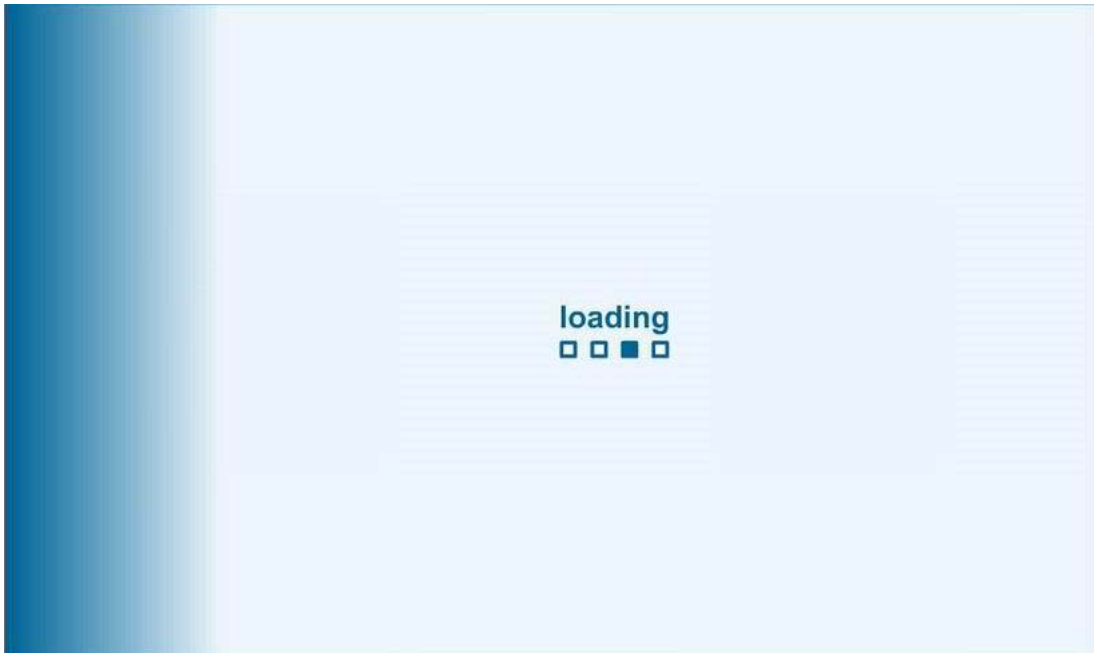
- procesor s taktovacou frekvenciou 233 MHz
- operačná pamäť 64 MB
- monitor 15” (rozlíšenie 1024 x 768)
- myš
- operačný systém Microsoft ® Windows (95/98/NT/Me/2k/XP)
- prehliadač Internet Explorer 5, s nainštalovaným modulom podpory Flash animácií (od firmy Macromedia®)

A.2.2 Spustenie animácie

Animáciu je možné spustiť zo stránky:

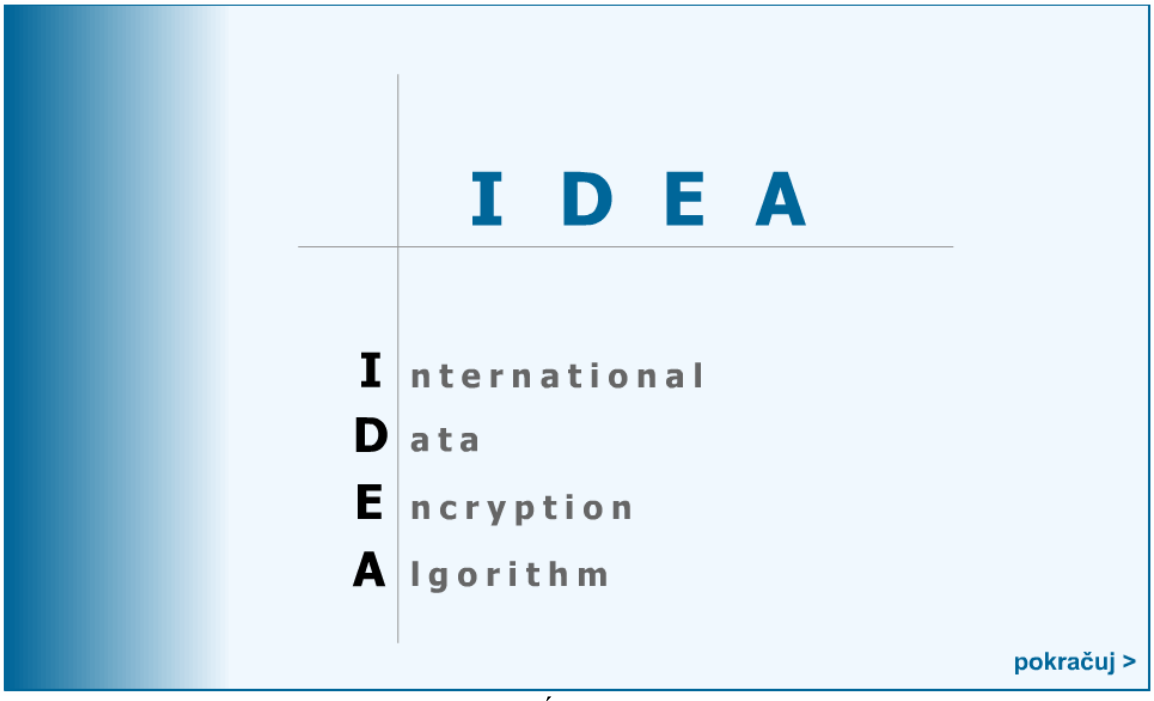
www2.dcs.elf.stuba.sk/~team11/prezentacia.htm

Po kliknutí na odkaz **Interaktívna prezentácia** sa začne nahrávať animácia do prehliadača. Tento proces môže trvať niekoľko sekúnd, až minút v závislosti od rýchlosti pripojenia. Proces nahrávania je sprevádzaný obrazovkou zobrazenou na obrázku (obr. č. 9)..



Obr. č. 9: Proces nahrávania

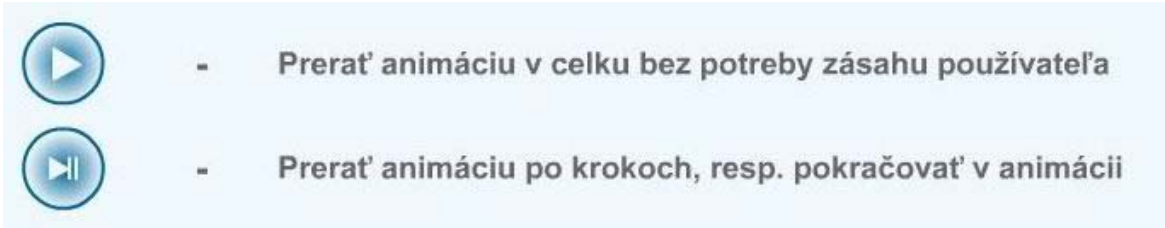
Po úspešnom načítaní celej prezentácia sa automaticky spustí a začne sa prehrávať úvodná animácia, ktorú je možné preskočiť stlačením tlačidla pokračuj >, ktoré je umiestnené v pravom dolnom rohu - obrázok (obr. č. 10).



Obr. č. 10: Úvodná animácia

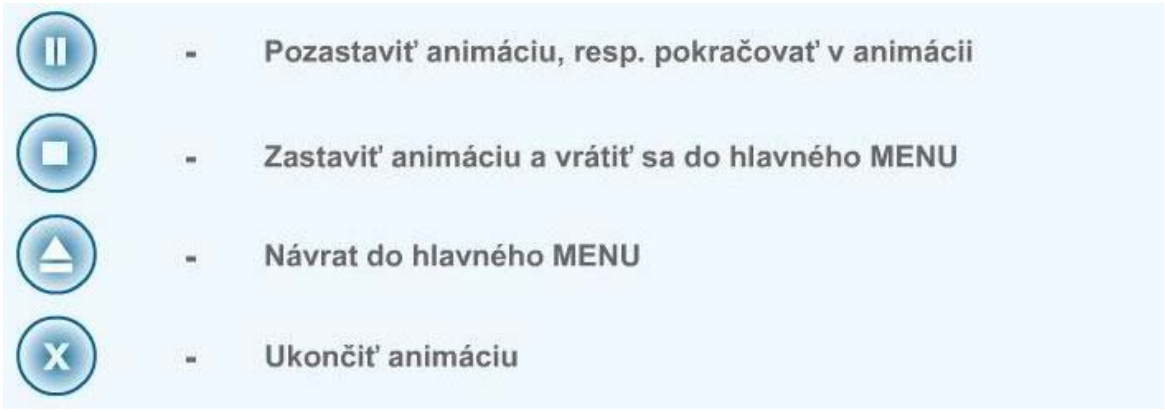
A.2.3 Prehrávanie animácie

Animáciu je možné spustiť v dvoch základných režimoch. Prvý z nich je prehrávanie animácie v celku (implicitný) a druhý je prehrávanie animácie po krokoch. Prepínanie medzi nimi je umožnené kedykoľvek počas animácie a realizuje sa potvrdením príslušných tlačidiel znázornených na obrázku (obr. č. 11).



Obr. č. 11: Režimy prehrávania animácie

Animáciu je možné počas prehrávania pozastaviť stlačením tlačidla **pauza**. Úplné zastavenie animácie a návrat do hlavného menu sa realizuje tlačidlom **stop**. Ukončenie animácie a návrat na predchádzajúcu WEB stránku ponúka tlačidlo **koniec**. Všetky tlačidlá je možné použiť kedykoľvek počas prehrávania - obrázok (obr. č. 12).



Obr. č. 12: Tlačidlá Pauza, Stop, Menu a Koniec

A.2.4 Prvky navigácie

Prvky navigácie, obrázok (obr. č. 13), slúžia na pohodlný prechod na požadovanú časť animácie kedykoľvek počas jej prehrávania. Tieto prvky sú implementované na dvoch úrovniach, a to:

- Prechod medzi Fázami šifrovania
- Prechod medzi jednotlivými krokmi (v rámci konkrétnej fázy)

Obr. č. 13: Prvky navigácie

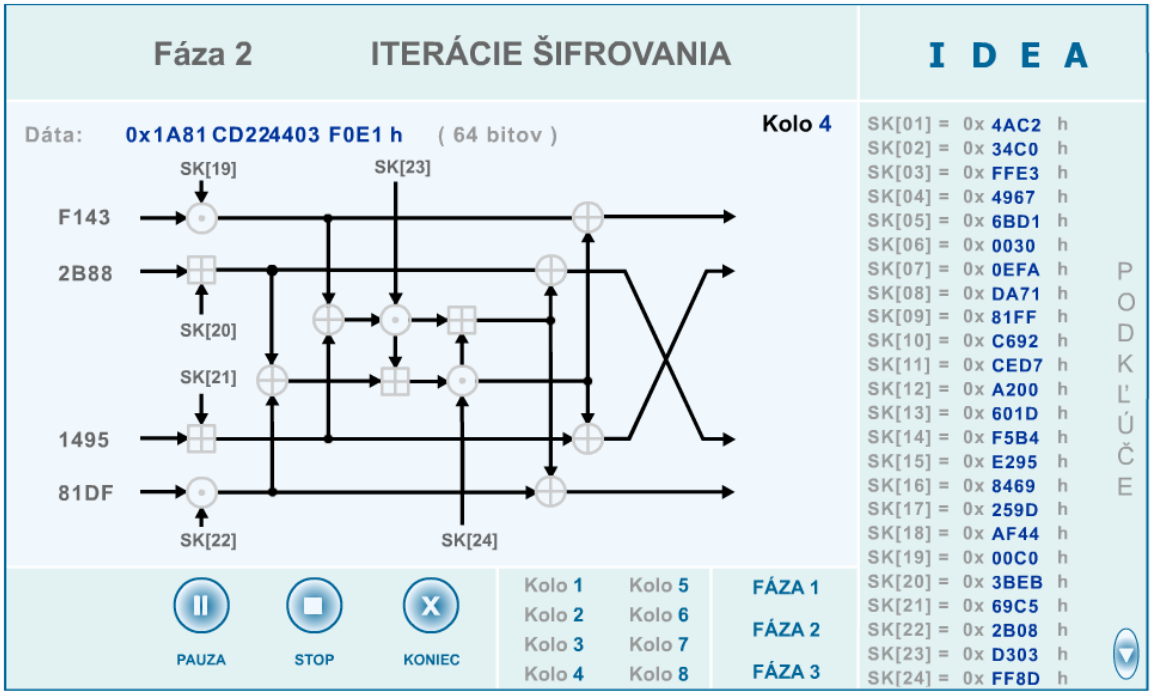
A.2.5 Nápoveda

Informácie o funkcionalite jednotlivých tlačidiel je možné získať stlačením tlačidla POMOC  , umiestneného v hlavnom menu animácie, obrázok (obr. č. 14).

Obr. č. 14: Hlavné menu

A.2.6 Identifikácia matematických symbolov

Matematické symboly použité vo fáze 2, obrázok (obr. č. 15), je možné identifikovať umiestnením kurzora na daný symbol. Následne sa zobrazí v priestore shématickej značky okno so stručným popisom funkcie.



Obr. č. 15: Fáza 2