Zadanie 2
I-UPB: Úvod do počítačovej bezpečnosti

October 11, 2021

1 Úvod

Zadanie popisuje vytvorenú aplikáciu pre šifrovanie a rozšifrovanie súborov pomocou zvolenej symetrickej šifry.

2 Popis aplikácie

2.1 Použité technológie

Pre vytvorenie aplikácie bol zvolený programovací jazyk Java spolu s knižnicami JavaFX pre vytvorenie krásneho GUI a JCE framerwork obsiahnutý v štandardných knižniciach jazyka Java pre implementáciu šifrovacej funkcionality aplikácie.

2.2 Funkcionalita aplikacie

Aplikácia pozostáva z dvoch obrazoviek. Jedna pre Vytváranie nového kľúča + šifrovanie súboru a druhá pre dešifrovanie súboru. Pri prvom spustení aplikácie bude automaticky vytvorený náhodný kľúč spolu s náhodým inicializačným vektorom. Tieto informácie sú serializované v súbore generated.key. Pri každom ďalšom spustení si aplikácia prečíta tento súbor a jeho obsah zoserializuje do objektu. Pokiaľ bude súbor vymazaný tak aplikácia si ho znova pri ďalšom štarte vygeneruje.

2.3 Popis použitia šifrovacieho algoritmu

Pre šifrovanie je použitá symetrická šifra AES v CBC móde so zarovnaním blokov. CBC mód sa považuje za bezpečný pretože rovnaké blok dát neprodukujú rovnaký zašifrovaný výsledok. Na každý ďalší blok je aplikovaná operácia XOR so zašifrovaným textom s predchádzajúceho bloku. Pre prvý blok je nutné použiť spomínaný inicializačný vektor. Veľkosť kľúča je 128b.
$C_i = E_K(P_i \oplus C_{i-1})$,
$C_0 = IV$,$C_0 = IV$,

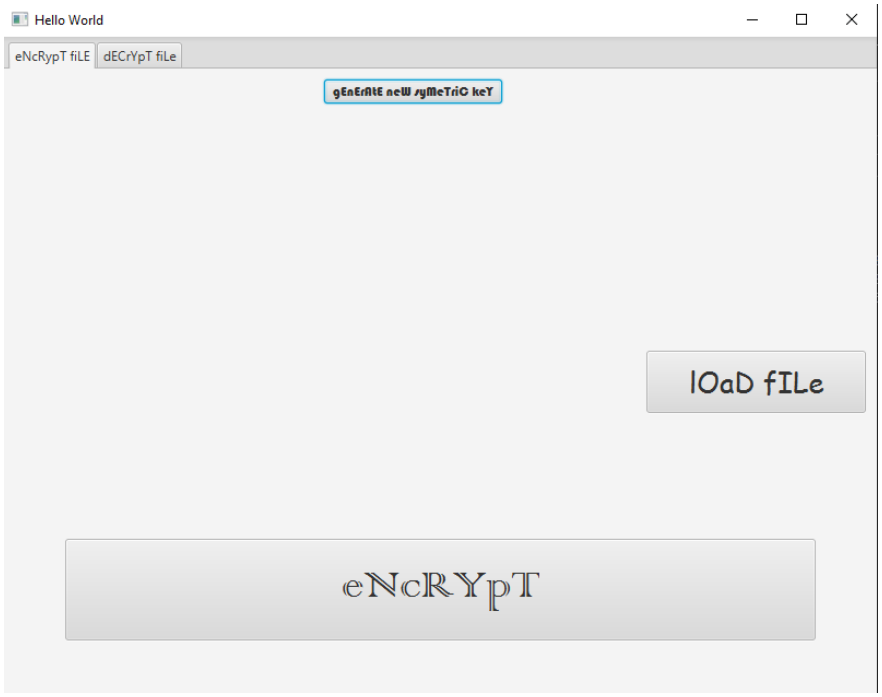
3 Použitie aplikácie

3.1 Spustenie

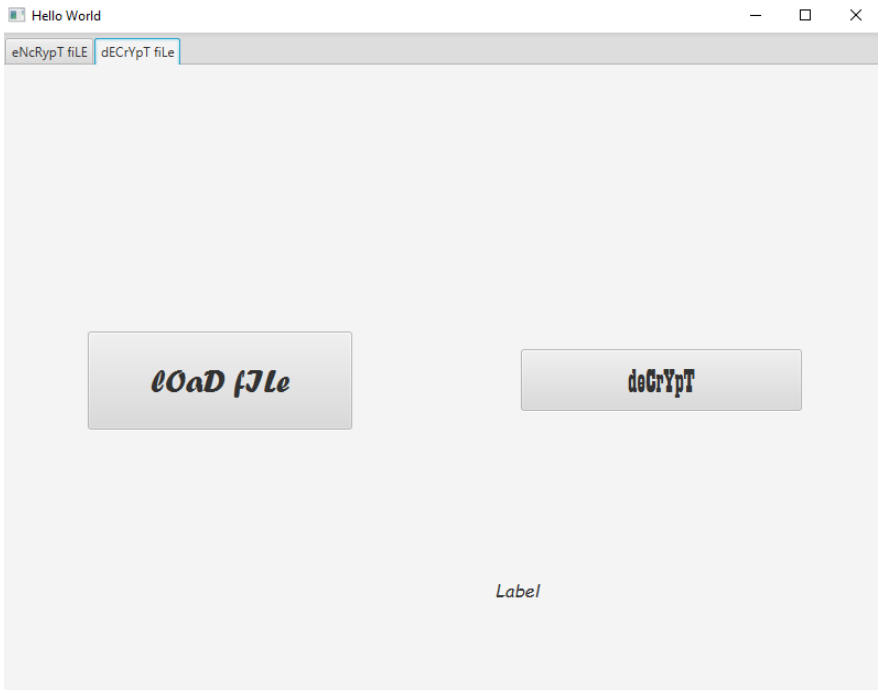
Pre spustenie aplikácie je nutné mať nainštalované JRE s min. verziou 1.7.0. Ak používateľ tento balíček nemá nainštalovaný tak aplikácia ho na to upozorní a odkáže na stránku kde si ho môže stiahnut. Aplikácia sa spušta pomocou súboru sonic.exe (ospravedlňujem sa ľuďom čo majú OS lepší ako Windows).

3.2 Hlavná a jediná funkcionalita

Pre zašifrovanie súboru je najskôr nutné súbor vybrať súbor stlačením tlačítka lOaD fILe. Po vybraní súboru je možné súbor zašifrovať stlačením tlačítka eNcRYpT. Táto akcia vytvorí súbor s názvom pôvodného súboru s postfixom _ec. Na tejto obrazovke je možné vygenerovať nový kľúč pomocou tlačítka gEnERatE neW syMeTriC keY.



Pre rozšifrovanie súboru je nutné sa prekliknúť na tab dECrYoT fiLe.



Na tejto obrazovke je znova nutné vybrať teraz už zašifrovaný súbor. Po vybraní súboru kliknúť na tlačítko deCrYpT ktoré rozšifruje súbor a vytvorí súbor decrypted s pôvodným formátom súboru.

4 Test rýchlosti

Na screenshotoch môžeme vidieť rýchlosť šifrovania a rozšifrovanie. Je nutné poznamenať že veľkým faktorom je SSD na počítači na ktorom program beží.