Zadanie 3
I-UPB: Úvod do počítačovej bezpečnosti

October 17, 2021

1 Úvod

Zadanie popisuje vytvorenú aplikáciu pre šifrovanie a rozšifrovanie súborov pomocou asymetrického šifrovania.

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 RSA keypair kľúč spolu s náhodým inicializačným vektorom. Tieto informácie sú serializované v súbore keys.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

S dôvodu výpočtovej náročnosti pri použití asymetrického šifrovania pomocou algoritmu RSA bol zvolený následovný postup.
Pre zašifrovanie:

1. Aplikácia vygeneruje RSA keypair
2. Aplikácie vygeneruje symetrický AES kľúč

3. symetrický kľúč je zašifrovaný verejným RSA kľúčom
4. vykoná sa kontrola integrity
5. plaintext súboru sa zašifruje symetricky, AES kľúčom za použitia GCM módu
6. zašifrovaný symetrický kľúč sa pripojí do zašifrovaného súboru ako hlavička.

Pre rozšifrovanie:

1. zo zašifrovaného súboru je extrahovaný symetrický kľúč a ciphertext
2. vykoná sa kontrola integrity
3. zašifrovaný symetrický kľúč je odšifrovaný pomocou súkromného RSA kľúča
4. ciphertext je rozšifrovaný rozšifrovaným symetrickým kľúčom.

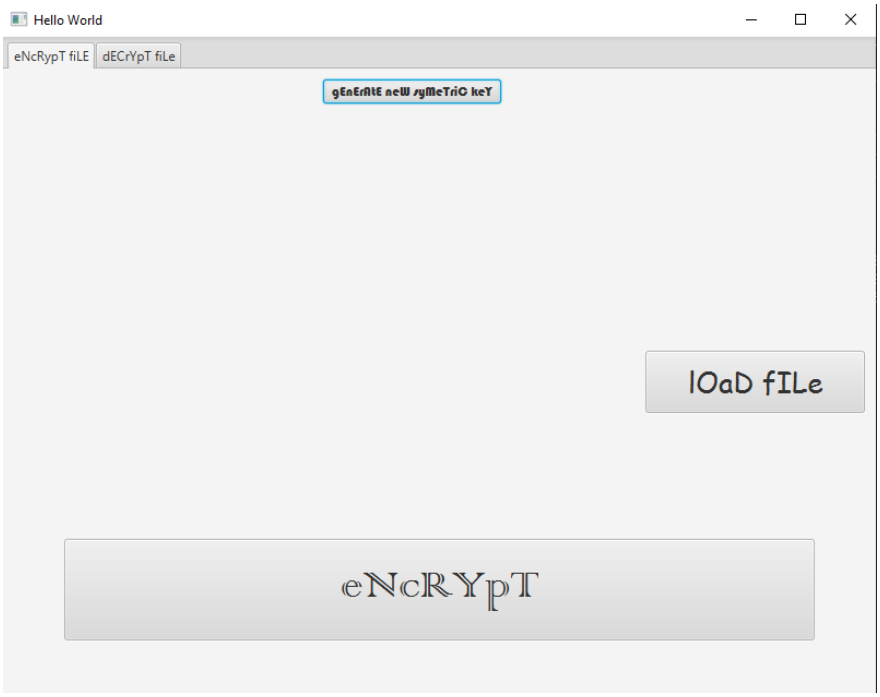
3 Použitie aplikácie

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).

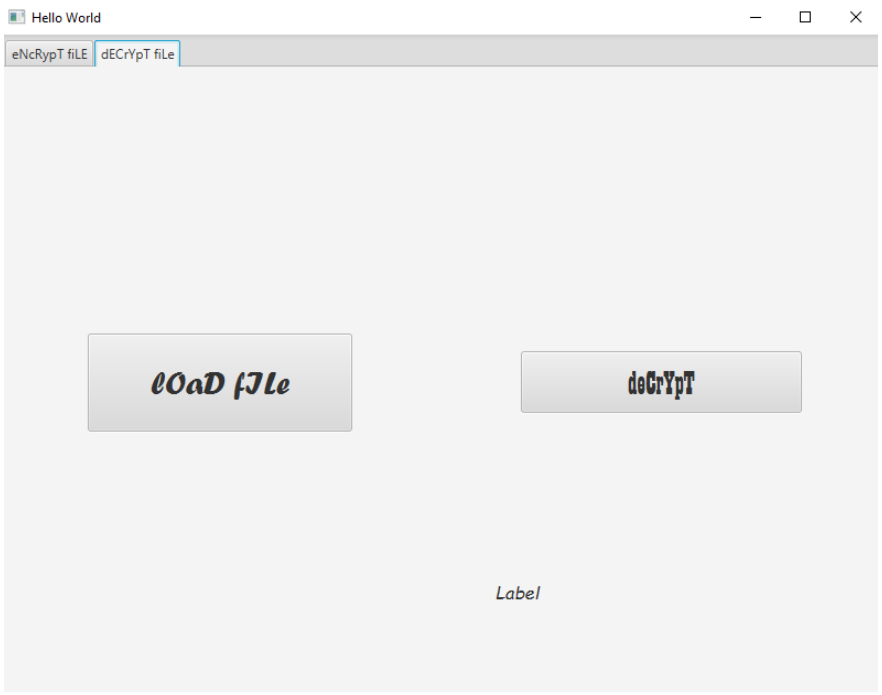
3.2 Hlavná a jediná funkcionalita

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.



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.


Hello World
eNcRypT fiLE
dECrYpT fiLe
lOaD fJle
deCrYpT
Label