NMMB202 Zápočtový program - Šifrovací aplikace pro Android (Anigma)

Jan Oupický

2018

1 Zadání

Aplikace má umět šifrovat a i dešifrovat podle zadaných parametrů vstupní text a soubory. Použité šifry AES, 3DES apod.

2 Uživatelský manuál

Aplikace je dostupná ke stažení na Google Play pod jménem "Anigma". Odkaz ke stažení: `https://play.google.com/store/apps/details?id=xyz.honzaik.anigma`.

Po stažení stačí aplikaci zapnout. Aplikace si po spuštění vyžádá oprávnění ke čtení a zápisu souborů v telefonu, kvůli šifrování souborů viz 1. Pokud uživatel nedá aplikaci oprávnění, tak se aplikace vypne.

Jestliže aplikace dostala potřebné oprávnění tak se zobrází hlavní a jediné okno aplikace viz 2. Úplně nahoře jsou 2 tlačítka označení "TEXT MODE"a "FILE MODE". Pomocí těchto tlačítek si může uživatel vybírat zda-li chce šifrovat text 2 nebo soubory 3. Pod těmito tlačítky je další možnost výběru a to z dostupných šifer 4. V aktuální verzi (1.0) jsou v aplikaci pouze dostupné šifry AES-128, AES-256 a 3DES plánuje se podpora šifer Serpent a Twofish (finalisté AES).

Nyní si probereme samostatně "TEXT MODE"a "FILE MODE".

2.1 Textový mód

Následující dvojicí tlačítek po výběru šifry jsou tlačítka s označením "ENCRYPTION"a "DECRYPTION". Pomocí nich si uživatel může vybrat, zda chce text šifrovat nebo dešifrovat.

Pokud si vybere šifrování. Tak se mu zobrazí toto rozhraní 2. Do políčka "Plaintext"stačí vyplnit požadovaný text, jenž chce uživatel zašifrovat. Dále do políčka "Password (key)"uživatel vyplní heslo, pomocí kterého se odvodí klíč k zašifrování textu. Posledním políčkem je políčko pro inicializační vektor (IV), uživatel si může vyplnit vlastní inicializační vektor, ale musí mít správou délku pro vybranou šifru a být zakódován v Base64. Toto se nedoporučuje, a proto je hned vedle tlačítko "GENERATE RANDOM", které vygeneruje správně náhodný inicializační vektor.

Dále má uživatel možnost si inicializační vektor zkopírovat do schránky, ale to obvykle není potřeba, jelikož nemusí být tajný narozdíl od hesla a automaticky se přidává do šifrového textu.

Nakonec stačí stisknout tlačítko "ENCRYPT STRING", která zahájí šifrování. Zobrazí se načítací kolečko, které informuje, že šifrování právě probíhá. Obvykle šifrování ale proběhne tak rychle, že ho uživatel nespatří. Pokud vše proběhlo v pořádku, tak by se měl výsledek zobrazit v okénku pod tlačítkem "COPY RESULT TO CLIPBOARD", který zašifrovaný text zkopíruje do schránky 6. Jesliže nastala chyba, bude na to uživatel upozorněn viz 7.

Dešifrování probíhá obdobně. Nyní již není potřeba vyplňovat IV, jelikož je součástí zašifrovaného textu 8.

2.2 Souborový mód

V tomto módu si uživatel podobně může vybrat mezi šifrováním a dešifrováním jako v textovém módu, ale předtím má na výběr z daných souborů 3. Aplikace uživateli napoví, kde se nachazí složka aplikace, kde se se soubory pracuje. V tomto případě to je `/storage/emulated/0/Anigma`.

Následně uživatel vidí seznam dostupných souborů v této složce a může si z nich vybírat. Vybraný soubor je označen sytě nažloutlou barvou 9.

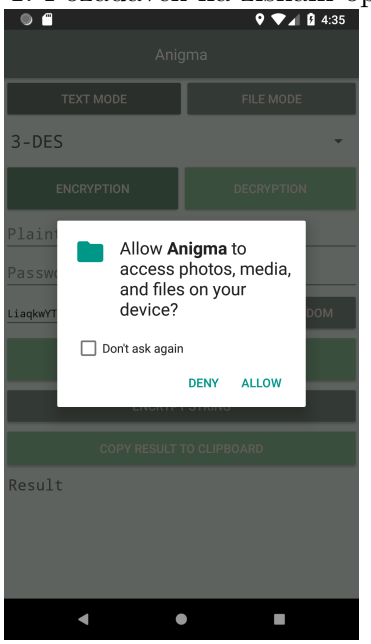
Nyní již stačí postupovat obdobně jako v textovém módu. Po zahájení šifrování a dešifrování se objeví "progress bar", která označuje kolik je již zašifrováno dat ze souboru 10. Jestliže zašifrování proběhlo úspěšně, tak se v dolním okně zobrazí hláška "Succesffully encrypted file"a v seznamu souborů, by se měl objevit soubor s sufixem "encrypted.0"(nebo jiné číslo v závilosti na duplicitě) 11.

Dešifrování probíhá obdobně. Po úspěšném dešifrování se vytvoří nový soubor s dalším sufixem "decrypted.0"12.

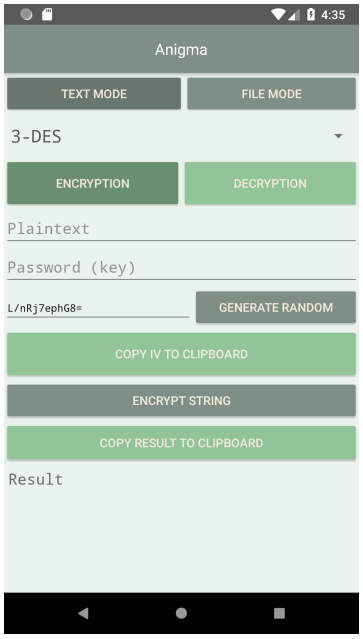
3 Závěr

Aplikace je plně funkční, i když v aktuální verzi nepodporuje mnoho šifer. Naštěstí přidání podpory dalších šifer je snadné. Dalším vylepšením této aplikace by mohlo být integrování samostatného prohlížeče souboru, aby nebylo potřeba pořád kopírovat soubory do složky aplikace. Zdrojový kód je také k dispozici na `https://github.com/Honzaik/Anigma`.

Obrázek 1: Požadavek na získání oprávnění.

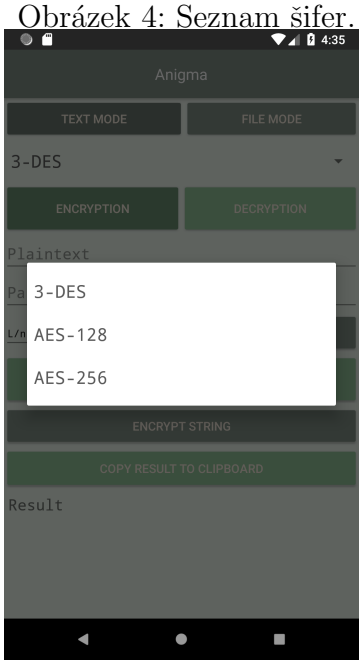


Obrázek 2: Hlavní okno - text mode (šifrování).

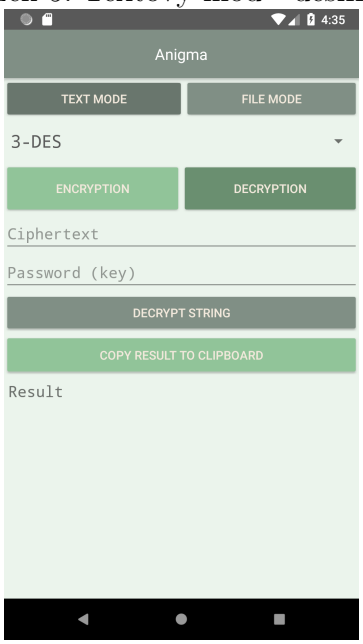


Obrázek 3: Hlavní okno - file mode.

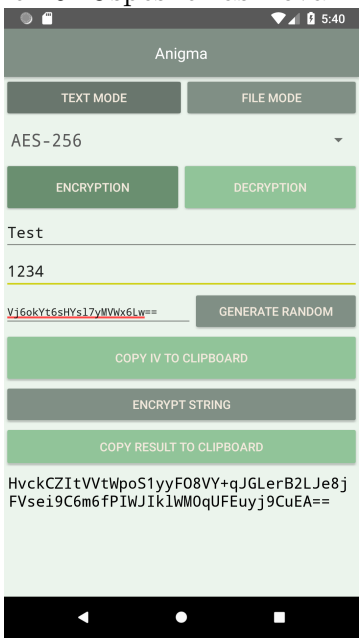
Obrázek 4: Seznam šifer.



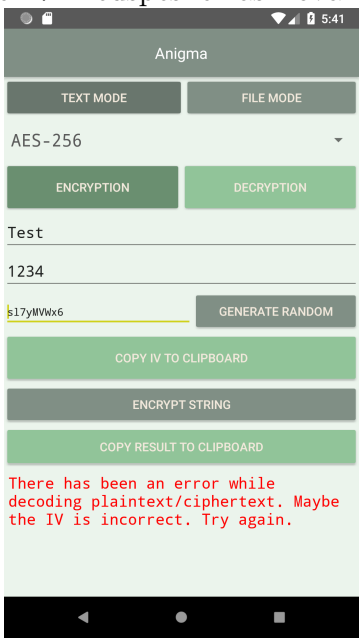
Obrázek 5: Textový mód - dešifrování.



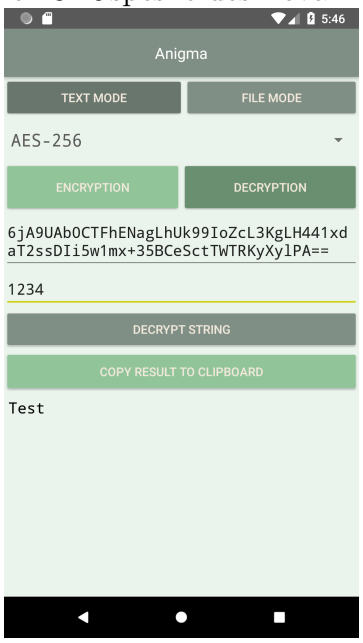
Obrázek 6: Úspěšné zašifrování textu.



Obrázek 7: Neúspěšné zašifrování textu.



Obrázek 8: Úspěšné dešifrování textu.



Obrázek 9: Vybrání souboru.

Obrázek 10: Progress bar.

Obrázek 11: Zašifrovaný soubor.

Obrázek 12: Dešifrovaný soubor.