UPB Zadanie 2/3

Aplikácia na šifrovanie a dešifrovanie

Špecifikácia:

Aplikácia je pre kompatibilitu so serverom napísaná v jazyku python, verzia 3.9 .
Používateľovi sa odporúča použiť 2048 bitový RSA kľúč generovaný v systéme.

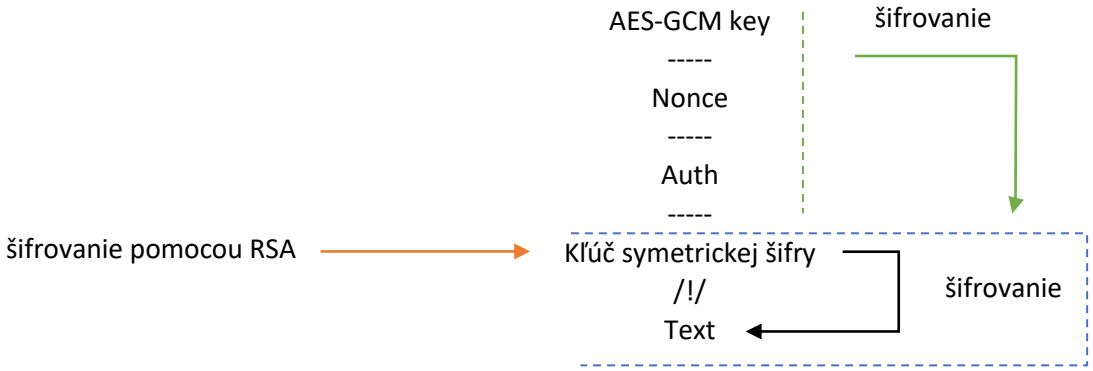
Šifrovanie:

- Vstupný text je zašifrovaný náhodným symetrickým kľúčom – kľúč má veľkosť 256 bitov a je generovaný pomocou knižnice Fernet.
- Vygenerovaný kľúč je následne zašifrovaný pomocou asymetrického šifrovania s využitím verejného RSA kľúča používateľa – zašifrovaný kľúč je vložený do hlavičky súboru.
- Celý súbor aj s hlavičkou je nakoniec šifrovaný blokovou šifrou AES-GCM, ktorá zároveň zabezpečí aj zachovanie integrity súboru – údaje potrebné na dešifrovanie sú priložené do hlavičky-kľúč má 256 bitov a je vygenerovaný náhodne pomocou os.urandom().
- Výsledný súbor je v base64 encodingu.

Dešifrovanie:

- Z hlavičky súboru sa vyberú potrebné metadáta na odšifrovanie pomocou AES-GCM
- Pri dešifrovaní zároveň prebehne kontrola integrity súboru, v prípade že súbor bol poškodený ďalej sa nedešifruje.
- Následne sa vyberie z hlavičky symetrický kľúč a odšifruje sa privátnym RSA kľúčom používateľa.
- Nakoniec je pomocou kľúča odšifrovaný súbor.
- Výstupom je pôvodný text.

Štruktúra súboru



Offline aplikácia

Aplikácia slúži na šifrovanie, dešifrovanie a generovanie nového rsa páru v offline verzii.

Knižnice: pycryptodome – pip install pycryptodome
Cryptography – pip install cryptography (from Crypto.Cipher / from Cryptodome.cipher)*
Fire – pip install fire
*Može nastať problém pri pomenovaní knižníc v závislosti od verzie python

Použitie:

enc_tool.py [options] <path?> <path?>

encrypt message public_key.pem/pub : encryption
decrypt message private_key.pem : decryption
-n : new rsa pair

Súbory, ktoré vygeneruje program budú uložené v koreňovom adresári programu

Použité knižnice:
pycryptodome
cryptography
os
fire

Pozn:
Veľkosti kľúčov a šifrovacích funkcií zodpovedá bezpečnostným odporúčaniam:
2048-bit rsa kľúč generovaný s najväčším dostupným exponentom
256-bit symetrický kľúč generovaný náhodným vektorom
256-bit kľúč použitý pre šifrovanie blokovou šifrou
Použitie AES-GCM pre aditívne šifrovanie a zabezpečenie integrity súboru