**Lab12**

**Paweł Górzyński 283815**

**Zad 1.**

**Obraz zawierający tekst, zrzut ekranu, oprogramowanie, System operacyjny

Zawartość wygenerowana przez AI może być niepoprawna.**

Wszystkie polecenia wykonałem, zaś zadanie 9 i 11 wykonałem w Kali Linux, zgodnie z wymaganym sposobem (rockyou, JohnTheRipper).

**Zad 2.**

**Obraz zawierający tekst, zrzut ekranu, oprogramowanie

Zawartość wygenerowana przez AI może być niepoprawna.**

**Komendy: input, with open, , import, len**

Na początku importujemy AES i get\_random\_bytes z odpowiednich bibliotek i wczytujemy dane od użytkownika. Potrzebujemy od niego nazwy pliku szyfrowanego, zaszyfrowanego i hasła. Następnie definiujemy funkcję, przyjmującą 3 zdefiniowane przed chwilą argumenty która będzie odpowiedzialna za wygenerowanie zakodowanego pliku. W tej funkcji generujemy klucz AES, szyfr oraz wektor inicjalizujący „iv”(potrzebny do zabezpieczenia szyfrów i rozpoczęcia procesu szyfrowania). Następnie otwieramy plik wejściowy i wyjściowy, odpowiednio w trybach do zapisu i czytania. Czytamy dane z pliku wejściowego, szyfrujemy i zapisujemy do pliku wyjściowego. Zmienna „padding” jest potrzebna do uzupełnienia pliku szyfrowanego, gdyż nasz algorytm wykorzystuje 128 bitowy blok (16 bajtów) i trzeba uzupełnić go jakimś znakiem. Na koniec plik szyfrujemy i wywołujemy funkcję.

Obraz zawierający tekst, zrzut ekranu, Czcionka, oprogramowanie

Zawartość wygenerowana przez AI może być niepoprawna.

**Zad 3.**

**Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Zawartość wygenerowana przez AI może być niepoprawna.**

**Komendy: input, open, print**

Na początku importujemy potrzebne moduły z biblioteki Crypto – algorytmu RSA, podpisu cyfrowego i funkcji haszującej SHA-256. Następnie wczytujemy od użytkownika plik który mamy podpisać i generujemy klucz publiczny i prywatny RSA. Klucze te oraz dane z podanego pliku zapisujuemy do plików dla kluczy kryptogtaficznych „.pem”. Na koniec program wczytuje te klucze i generuje plik z podpisem cyfrowym.

Obraz zawierający tekst, Czcionka, zrzut ekranu, typografia

Zawartość wygenerowana przez AI może być niepoprawna.