Lab3  
Zadanie1

Zaimplementuj skrypt generujący skróty MD5, SHA-256, md5deep, ssdeep. Jako dane wejściowe skrypt ma przyjmować dowolny plik/zbiór plików.

Następnie porównaj wyniki wszystkich funkcji dla:

* 2 różnych plików
* 2 plików o podobnej zawartości (np. pliki tekstowe ze zmienionym jednym zdaniem)

Wnioski z porównania umieść na swoim repozytorium.

**Info:**  Do implementacji funkcji skrótu możesz użyć istniejących bibliotek w wersjach nieposiadających publicznie znanych podatności.

Skrypt napisany przeze mnie dla dwóch różnych plików każdy ze skryptów generuje inny skrót,

Zaś dla dwóch podobnych plików skrypt Sha-256 oraz MD5 generują zupełnie inny skrót a MD5deep ssdeep generują skrót różniący się tylko częściowo.

**Zadanie 2**

Zaimplementuj funkcję generowania kluczy, szyfrowania i deszyfrowania algorytmu RSA. Korzystając ze swojej implementacji wygeneruj klucze (publiczny oraz prywatny). Klucz publiczny zakodowany w formacie Base64 umieść na swoim repozytorium.

~~Na maila otrzymasz plik tekstowy zaszyfrowany wygenerowanym przez Ciebie kluczem publicznym. Twoim zadaniem będzie odszyfrowanie pliku i umieszczenie go w repozytorium. Zawartość pliku po zaszyfrowaniu zakodowana została w formacie HEX.~~

Zaszyfruj dowolny plik swoim skryptem korzystając z klucza publicznego umieszczonego poniżej (zakodowany w Base64) i umieść zaszyfrowany plik zakodowany w formacie HEX w swoim repozytorium.

**Info:**  Do implementacji RSA użyj bibliotek w wersjach nieposiadających publicznie znanych podatności. Jeśli Twoje klucze zostaną wygenerowane niepoprawnie i nie będzie można ich użyć do szyfrowania/odszyfrowania, zadanie w części wymagającej użycia kluczy nie będzie zaliczone.

**Dodatkowo odpowiedz na pytania** (odpowiedzi umieść w repo):

|  |
| --- |
| MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAjv6/p0FXuUR+G8cp1eKkWe6Ijofcftdk  tHPlE+26dpapV4cf96SUHtNg0bQql4i9xSqLZZNX3I8lLmzF9bv1xlnMnpg330ym7uHEeImwVaw4  AruUkeiEg0kbCN/56UctmTQRNLz8Ts84kVVTvaCPlDCJN3qVxxGP687yhBKIrtsbi6IuIR2iq1J9  Jteszy4FQhJgoj8GzysT4P/VHo9AG8ETdoAnrSnDcVZNF5yCY5BhJy5PlAv1C6ZJCTP3iHFfjCaN  0shaRh6Jm6QWpRVX/seppPHtPflc9b0Uu1Kd0zG5p5goNmqVid6zLnMDac1iNS73/dkpfhGT9KM+  ASiabwIDAQAB |

* Jakiej funkcji użyłeś do wczytania pliku? Dlaczego? Czy istnieje inna metoda?

W moim programie użyłem funkcji open oraz read. Użyłem tej funkcji ponieważ jest ona prezentowana w większości kursów dla początkujących niestety nie znam na razie innej metody na wczytanie danych z pliku.

* Jaki rozmiar klucza RSA wybrałeś? Dlaczego?

Uzyłem klucza o rozmiarze 1024 bity ponieważ jest to klucz który do wygenerowania nie potrzebuje dużej mocy obliczeniowej oraz nie obciąza procesora przy szufrowaniu plików jak robią to klucze o większym rozmiarze. Do tego zadania był on jak najbardziej wystarczający jednak gdy miał bym szyfrować pliki o większej wadze wybrał bym zdecydowanie klucz o większym rozmiarze.

* Czym model PGP różni się od od hierarchii certyfikatów X.509?