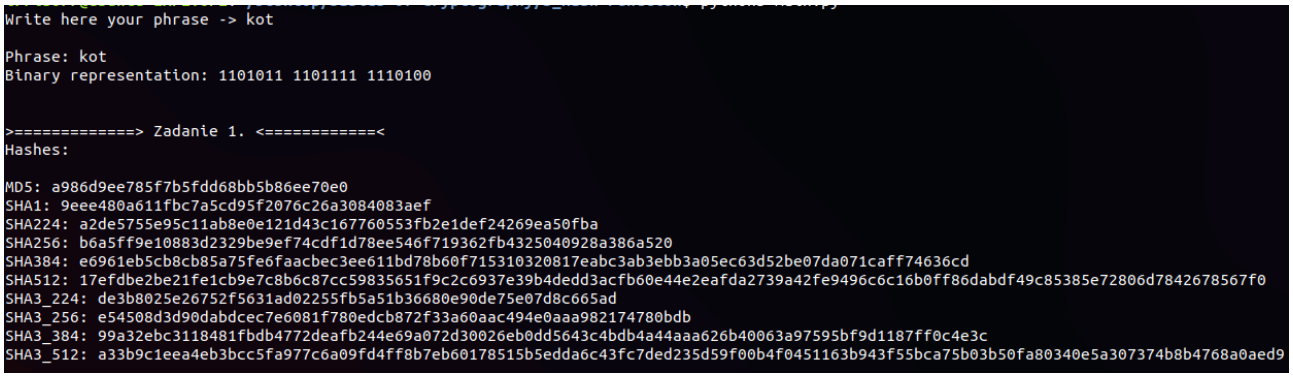
Funkcje skrótu - Hash functions

Heorhi Zakharkevich
153992

1. Screenshot z aplikacji

To jest tylko 1st zadanie, pozostałe można znaleść po uruchomeniu samej applikacji (plik main.py)



2. Omówienie sposobu implementacji

Kod zawiera kilka funkcji:

- **inputText()** - prosi user'a o wprowadzeniu frazy i zwraca ją
- **textToBin()** - konwertuje tekst na reprezentację binarną
- **getAllHashes()** - wyświetla wartości hash'ów dla każdej funkcji ktorą przyjmuje
- **generateHash()** - generuje wartość hash'a dla danego zakodowanego tekstu i funkcji hashującej za pomocą biblioteji hashlib
- **compareHashFunctions()** - porównuje (wyświetla) szybkość działania i długość wyjścia róznych funkcji hashujących
- **findHashMD5()** - przyjmuje słowo i ścieżkę do pliku, a następnie wyszukuje to słowo w pliku, porównując jego wartość hasha MD5 (nie wykorzystałem w aplikacji)
- **checkHashCollisions()** - sprawdza kolizje na pierwszych 12 bitach hasha dla danej funkcji hashującej i wyświetla znalezione kolizji
- **checkSAC()** - sprawdza spełnienie Ścisłego Kryterium Przepływu (Strict Avalanche Criteria - SAC) dla danej funkcji hashującej i słowa.
- **main()** - służy jako punkt wejścia, wywołując pozostałe funkcje i demonstrując ich użycie.

3. Określenie roli soli w tworzeniu skrótów

W swojej applikacji nie wykorzystałem koncepcje dodawania soli. W prostych słowach sól w kryptografii to dodatkowy losowy ciąg znaków dodawany do danych wejściowych przed zhashowaniem. Jej celem jest utrudnienie ataków słownikowych i ataków z wykorzystaniem preobliczonych tabel hashów, poprzez wprowadzenie unikalnych soli dla każdego hasła lub danych wejściowych.

4. Odpowiedź oraz jej uzasadnienie na pytanie postawione w pkt. 4

W ciągu ostatnich kilkunastu lat opublikowano wiele efektywnych ataków na MD5, umożliwiających znalezienie kolizji, czyli różnych plików dających ten sam skrót MD5. Ze względu na te podatności, MD5 nie jest już rekomendowana do zastosowań wymagających wysokiego poziomu bezpieczeństwa.

5. Zestawienie uzyskanych wyników

Wszystko można odnaleźć po uruchomeniu aplikacji