

# Sprawozdanie z przedmiotu "Podstawy Kryptografii"

## Szyfry blokowe

*Ivan Kaliadzich 153936*

1. Kod jest zrealizowany w pliku "main.py".
2. Obliczanie szybkości jest zrealizowane za pomocą biblioteki time.

Przykład obliczania czasu:

- a. Fraza wejściowa: "Kot"

Kod binarny: 1001011 1101111 1110100

MD5:

c0d03d2d3e717da54ffdfc8a76c0f089

**Czas: 0.023399999999895726 ms**

SHA-1:

a0e5cd812455e04d6e33646cd8dc17e05b674231

**Czas: 0.01180000000000625 ms**

SHA-256:

aedaac3e798149ebaec99435ea67f2ff1fc8b5cd2f3b039b885bdf8c04678c03

**Czas: 0.0123000000000076139 ms**

SHA3-256:

16c6f78ba37ae968b2602249278aad82aea653662b3e9583d598030f0fef5c4d

**Czas: 0.011399999999994748 ms**

SHA3-512:

4e8c7f92a8e50c690ebfc01aca3e91d29fae439427aa979271d159f4a0bc4f741

b3bab6144ecf36cacf21e23aa1720ce952fba1b8836dd7c819e4c6d73604b4a

**Czas: 0.0062000000000067263 ms**

- b. Fraza wejściowa: "Good Morning!"

Kod binarny: 1000111 1101111 1101111 1100100 100000 1001101 1101111

1110010 1101110 1101001 1101110 1100111 100001

MD5:

74e04112ff98f7de780eaf66a8cdaf21

**Czas: 0.018899999999710815 ms**

SHA-1:

f1f58acda74c0b342659582bc7d6792ef9b87aee

**Czas: 0.008399999999575414 ms**

SHA-256:

b8cf3a317a262435749cdd0d7de090bf0a3639be1f161266c2678414b010ce3  
2

**Czas: 0.007399999999435636 ms**

SHA3-256:

f62b3466b8c903430dddcc6a6b57e56faf58631fa8aca9c994497370c6f96caf

**Czas: 0.005999999999950489 ms**

SHA3-512:

9b998ca163f25c6605cd95cae9d5293ea6978d73f399b20e308f68de90ec1372  
05ce1550df110742d5e2517c77e0e16b9b95dca2d15de8c750d663ff5d2ecba6

**Czas: 0.003699999999717818 ms**

- c. Fraza wejściowa: "Secure encryption safeguards data privacy effectively."

Kod binarny: 1010011 1100101 1100011 1110101 1110010 1100101 100000  
1100101 1101110 1100011 1110010 1111001 1110000 1110100 1101001  
1101111 1101110 100000 1110011 1100001 1100110 1100101 1100111  
1110101 1100001 1110010 1100100 1110011 100000 1100100 1100001  
1110100 1100001 100000 1110000 1110010 1101001 1110110 1100001  
1100011 1111001 100000 1100101 1100110 1100110 1100101 1100011  
1110100 1101001 1110110 1100101 1101100 1111001 101110

MD5:

f65498211e4c017d505c96c3582c15b3

**Czas: 0.0177999999994849713 ms**

SHA-1:

316559916eebc6e87acb9f61a0b8dfb76b8bfe22

**Czas: 0.0081999999996350016 ms**

SHA-256:

f108aa6c58480b396ee249f573eb066c44ca384f1c976a86c899b803bf4fe728

**Czas: 0.00769999999976123945 ms**

SHA3-256:

dd69690dbe33c0e6704d7a0b875d0b14689d5c7d3818e29cf1ac78d946f5f4a  
1

**Czas: 0.00539999999915608 ms**

SHA3-512:

879266fc52567daad7fd4f4f34bd6ae726b093776bb48bf117bdc6cfad12fd001  
26eaf36625fc039c17f988a7923d09d39bef9f8d0f50ff52de022da2cc13b24

**Czas: 0.0035999999994373866 ms**

3. Wpisałem dwa krótkich słowa w języku angielskim - "cat" i "home", poszukałem ich w internecie i hasła MD5 były znane:



The George Washington University

<https://www2.gwu.edu/~8cf...> · [Перевести эту страницу](#)

### 1. Home ✓

Home page for LoggerPro manual. There is a navigation menu on the right that will take you to a short description of the various capabilities of LoggerPro that ...

Skróty MD5 krótkich haseł, szczególnie tych składających się z powszechnie używanych słów lub prostych kombinacji, mogą być łatwo odnalezione w tzw. rainbow tables lub za pomocą ataków brute force. Oznacza to, że nawet jeśli hasło jest hashowane, jego bezpieczeństwo jest niewielkie, jeśli oryginalne hasło jest zbyt proste lub krótkie.

4. Funkcja MD5 nie jest uważana za bezpieczną z kilku powodów. Pierwszym i najważniejszym problemem są kolizje: zostało udowodnione, że możliwe jest znalezienie dwóch różnych wejść, które generują taki sam skrót MD5. Oznacza to, że funkcja MD5 jest podatna na ataki, w których atakujący może zastąpić bezpieczne dane szkodliwymi, które mają taki sam skrót MD5.

Z powodu tych słabości, MD5 nie jest już zalecane do zastosowań, które wymagają silnych gwarancji kryptograficznych, takich jak przechowywanie haseł, podpisy cyfrowe czy zabezpieczenie integralności danych. Zamiast tego zaleca się stosowanie nowszych i bezpieczniejszych funkcji skrótu, takich jak SHA-256 lub SHA-3.

Na pytanie, czy funkcja MD5 może być uznana za bezpieczną, odpowiedź brzmi: nie. Znane są dla niej kolizje, co czyni ją niewłaściwą do większości zastosowań kryptograficznych, gdzie bezpieczeństwo jest kluczowe.

- 5.
- ```
Liczba kolizji na pierwszych 12 bitach skrótu: 129
Przykłady kolizji:
2c6: ['8', '511']
4ec: ['18', '710']
9f1: ['35', '114']
734: ['42', '170']
44c: ['43', '84']
```

6. Przykładowa odpowiedź:  
Średnia liczba zmienionych bitów: 128.04296875  
Prawdopodobieństwo: 0.5001678466796875

### Screenshot z aplikacji:

```
Wpisz frazę wejściową: gopfsagjsrf
Kod binarny: 1100111 1101111 1110000 1100110 1110011 1110011 1100111 1101010 1110011 1110000 1100110

MD5: 85d628281fb30049a5ab1fabb5827324
Czas: 0.0181000000001319 ms

SHA-1: a1fa73bbd257c1f6aab132131c1824f6d77317ba
Czas: 0.008699999999972619 ms

SHA-256: c43484e4cf7fcd500df4f5fb4e4f60b874398532f9a8706364a769fa819b3a12
Czas: 0.0087000000000416708 ms

SHA3-256: af8cceed670146c3d28e31c333f0b7f5c231e05c0101b8939f430afdf0b5e92b
Czas: 0.0070000000000090267 ms

SHA3-512: d9666e96adf293c888600f85458422b499d18786a92a87bcc732dce616adc24fff4d7477f30c162c9cff0f7095fba50605a70b66ad0db99290f9c2d8a1475796
Czas: 0.0032000000000092018 ms

Liczba kolizji na pierwszych 12 bitach skrótu: 129
Przykłady kolizji:
2c6: ['8', '511']
4ec: ['18', '710']
9f1: ['35', '114']
734: ['42', '170']
44c: ['43', '84']

Średnia liczba zmienionych bitów: 128.04296875
Prawdopodobieństwo: 0.5001678466796875
```