Szyfrowanie hybrydowe I funkcje skrótu

Korzystając ze schematów z poprzednich laboratoriów realizujących protokół Diffie-Hellmana (dla parametrów podanych w pliku) i szyfr Trivium opracować model, który umożliwia uzgodnienie klucza w sposób asymetryczny i wykorzystanie uzgodnionego klucza i szyfrowania i deszyfrowania szyfrem symetrycznym. Korzystając z tego modelu uzgodnić tajny klucz i wykonać nim szyfrowanie i deszyfrowanie wiadomości utworzonej z własnego imienia i nazwiska

p = 816498706044804310413503820028516344479352881209

g = 991804914601628320830624946497142040596904847 38

Klucz: 7943382625300624585322209738523094270089223871 13

Trivium:

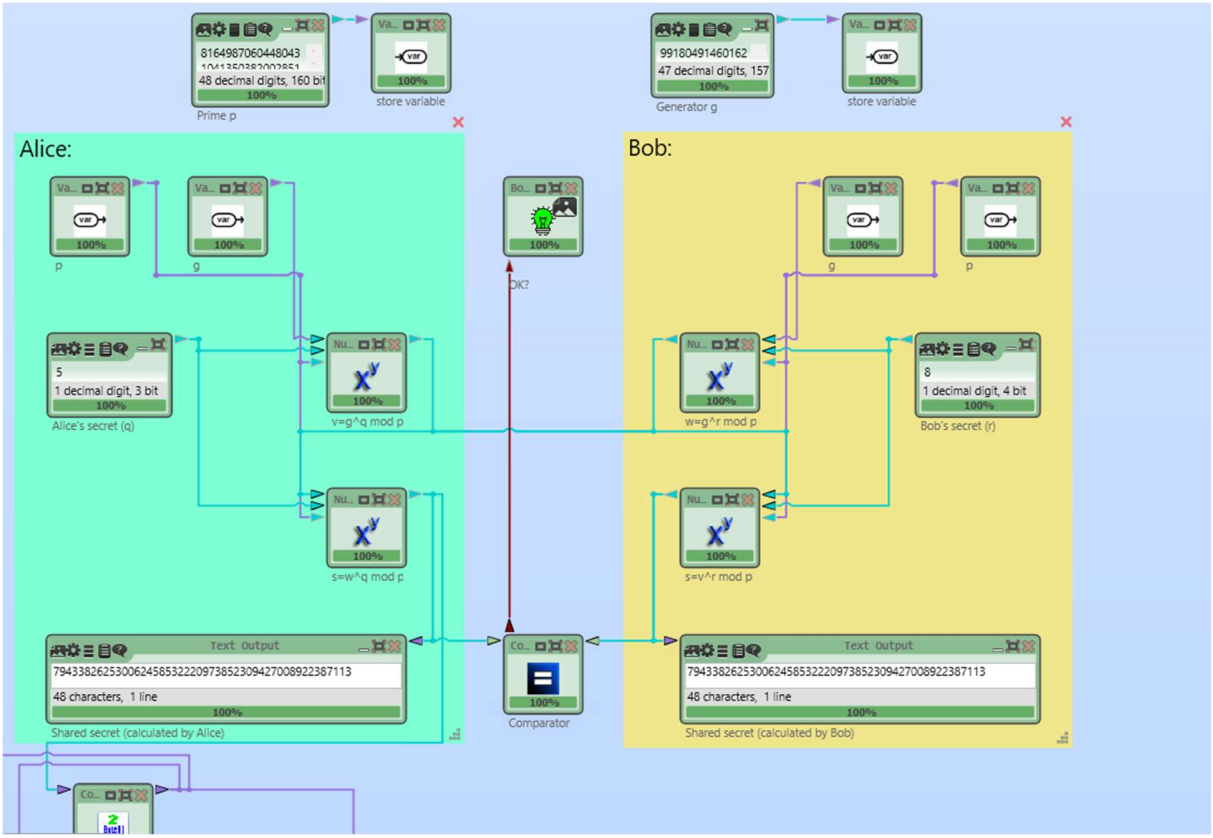
M: Wojtek Matras

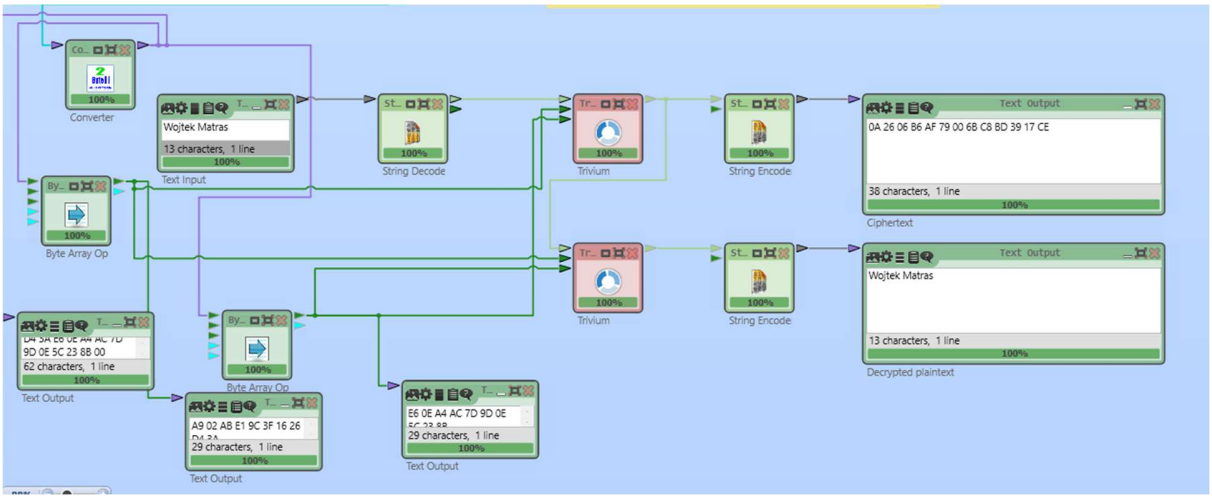
Crypted: 0A 26 06 B6 AF 79 00 6B C8 BD 39 17 CE

Decrypted: Wojtek Matras

Klucz trivium: A9 02 AB E1 9C 3F 16 26 D4 3A

Wektor: E6 0E A4 AC 7D 9D 0E 5C 23 8B





Korzystając ze schematów z poprzednich laboratoriów realizujących szyfry AES i RSA opracować model realizujący szyfrowanie i deszyfrowanie hybrydowe. Korzystając z tego modelu wykonać szyfrowanie i deszyfrowanie wiadomości utworzonej z własnego imienia i nazwiska.

p=998813955049467801133

e=5802877

n= 10375947615867177312285893485139582597927 59

d= 385575739756394350812934958203384724843 89

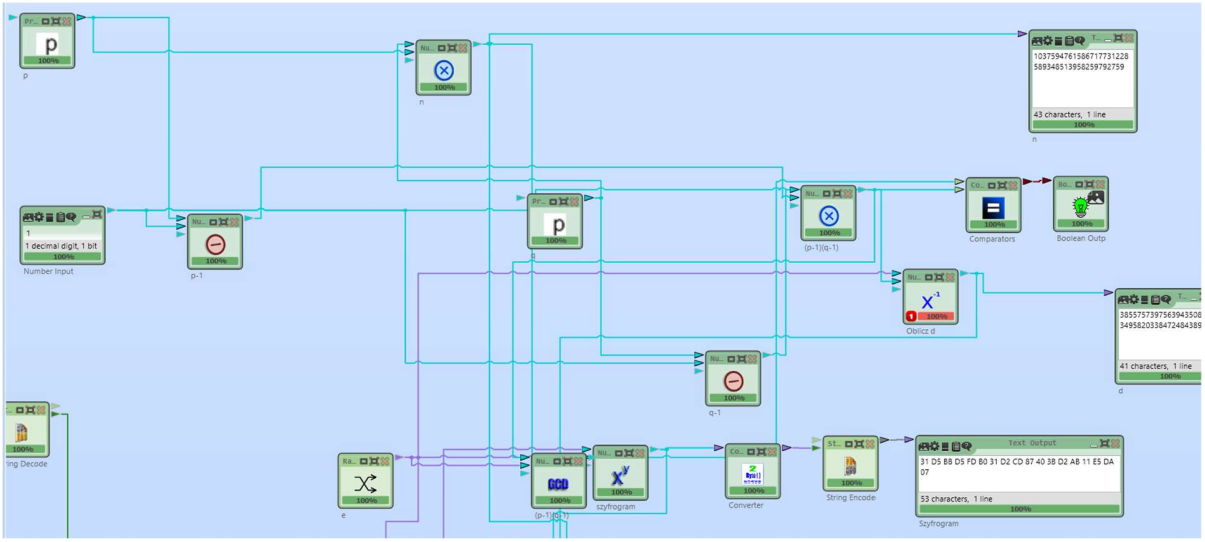
szyfrogram: 31 D5 BB D5 FD B0 31 D2 CD 87 40 3B D2 AB 11 E5 DA 07

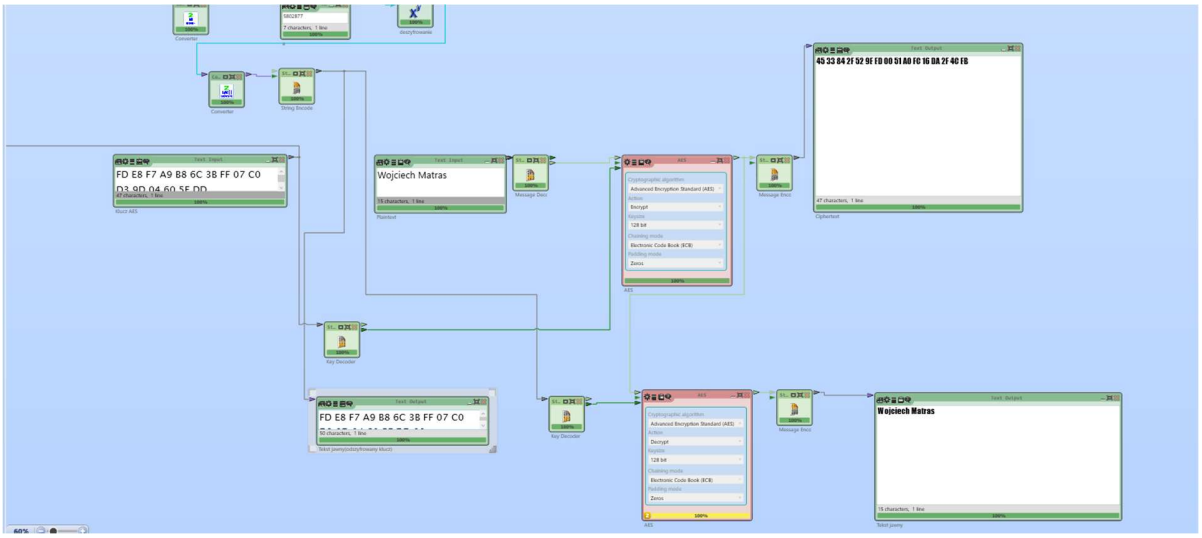
AES klucz: FD E8 F7 A9 B8 6C 3B FF 07 C0 D3 9D 04 60 5E DD

Messange: Wojciech Matras

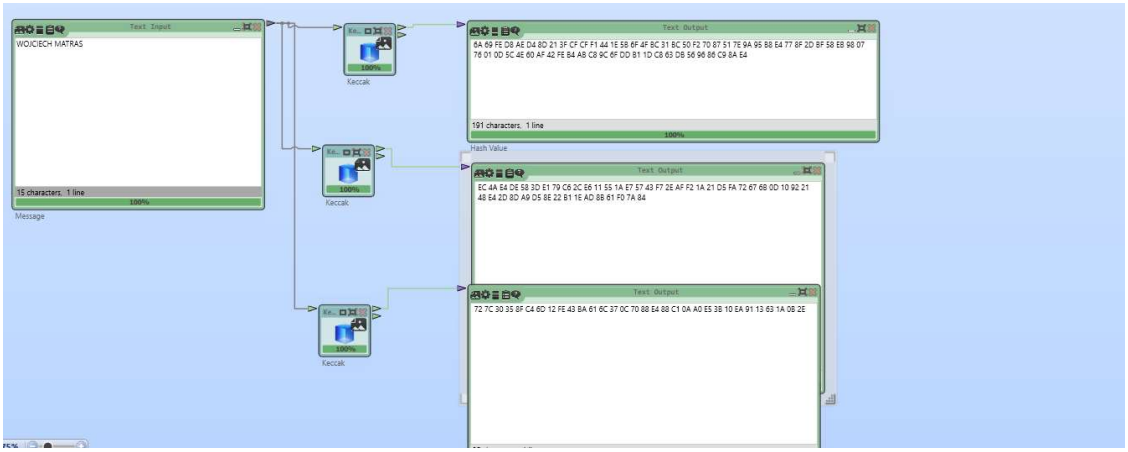
Zaszyfrowany tekst: 45 33 84 2F 52 9E ED 00 51 A0 FC 16 DA 2F 4C EB

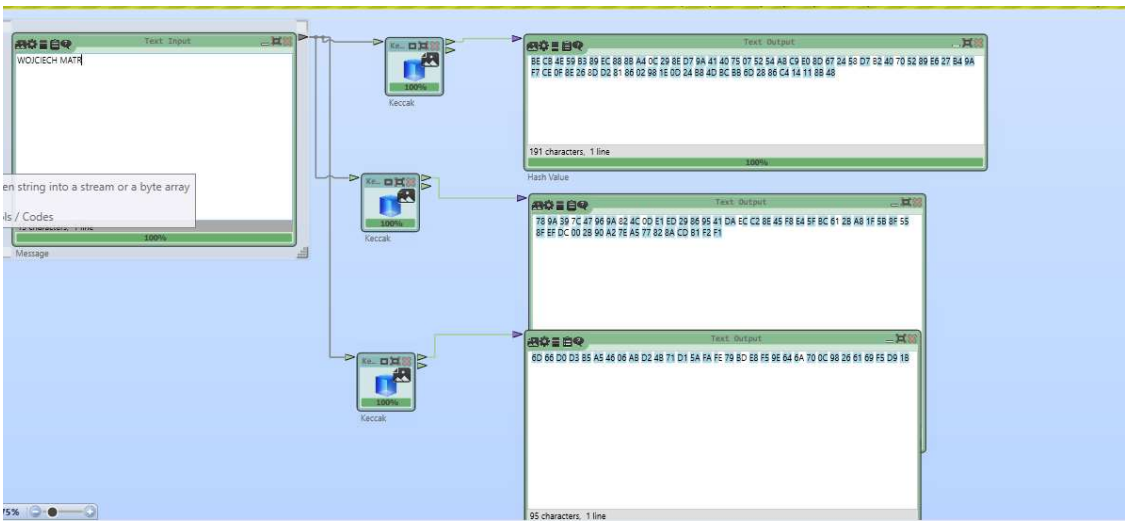
Odszyfrowany messange: Wojciech Matras





Standardowe funkcje skrótu SHA-2 i SHA-3 (Keccak) Korzystając z dostępnych bloków opracować model wyznaczający skrót dowolnej wiadomości funkcją skrótu SHA-2 i SHA-3 (Keccak) o tej samej długości skrótu (użyć trzech długości: 256, 384 i 512 bitów). Korzystając z obu funkcji skrótu wyznaczyć skrót wiadomości utworzonej z własnego imienia i nazwiska. Następnie wyznaczyć skróty wiadomości utworzonej przez modyfikację poprzedniej (zamianę, dopisanie lub usunięcie jednego lub kilku znaków) i porównać ze skrótami otrzymanymi wcześniej.





text input: WOJCIECH MATRAS

zmieniony na: WOJCIECH MATR

SHA3-512

6A 69 FE D8 AE D4 8D 21 3F CF CF F1 44 1E 5B 6F 4F BC 31 BC 50 F2 70 87 51 7E 9A 95 B8 E4 77 8F 2D BF 58 EB 98 07
76 01 0D 5C 4E 60 AF 42 FE B4 AB C8 9C 6F DD B1 1D C8 63 DB 56 96 86 C9 8A E4

zmiana:

BE CB 4E 59 B3 89 EC 88 8B A4 0C 29 8E D7 9A 41 40 75 07 52 54 A8 C9 E0 8D 67 24 58 D7 B2 40 70 52 89 E6 27 B4 9A F7 CE 0F 8E 26 8D D2 81 86 02 98 1E 0D 24 B8 4D BC BB 6D 28 86 C4 14 11 8B 48

Sha-512

3B 9C DC CF A5 2E 0B F6 6B 28 B9 DA 67 12 17 FD 7C 81 2C 96 E2 A5 B7 F2 3A 23 E0 D1 14 29 D8 3A 21 BB 13 18 1A 4A 60 AE FA B9 61 7B FB 9D 4F 0C EE 12 89 36 63 63 C8 4E D5 08 30 23 1D CC F8 01

Zmiana

40 37 47 E0 1D D4 88 10 27 62 55 55 87 43 98 7D 88 81 01 B5 EC DD 83 4B B0 84 86 C9 DC 0B 6D 4E 38 F4 70 8E 84 29 6D F0 4C 71 11 80 02 C7 88 2E B4 40 F6 E0 91 4B 0B 6C 67 E3 E2 73 52 96 9B 7F

SHA3-384

EC 4A E4 DE 58 3D E1 79 C6 2C E6 11 55 1A E7 57 43 F7 2E AF F2 1A 21 D5 FA 72 67 6B 0D 10 92 21 48 E4 2D 8D A9 D5 8E 22 B1 1E AD 8B 61 F0 7A 84

zmiana:

78 9A 39 7C 47 96 9A 82 4C 0D E1 ED 29 86 95 41 DA EC C2 8E 45 F8 E4 5F BC 61 2B A8 1F 5B 8F 55 8F EF DC 00 2B 90 A2 7E A5 77 82 8A CD B1 F2 F1

SHA-384

D5 60 FF 58 E6 BE C7 13 0B 40 CE 42 41 B2 77 7F 65 C3 35 11 40 D6 D0 03 C7 09 A8 9C F0 A8 0F 4B B8 88 AE 8E FD 80 25 4F 35 3C AC 27 31 4A CB 2D

zmiana:

72 ED 70 55 A3 AF 33 5B 08 CA 3D 6A 1C 5C 68 42 8D E2 B2 2A F1 FC 65 0A D1 B1 EF EE 45 CF E0 77 E9 D4 40 07 B0 B1 4B E8 86 D3 69 5F 0A B5 07 2E

SHA3-256

72 7C 30 35 8F C4 6D 12 FE 43 BA 61 6C 37 0C 70 88 E4 88 C1 0A A0 E5 3B 10 EA 91 13 63 1A 0B 2E

zmiana:

6D 66 D0 D3 B5 A5 46 06 AB D2 4B 71 D1 5A FA FE 79 BD E8 F5 9E 64 6A 70 0C 98 26 61 69 F5 D9 1B

SHA-256

3C 0A 85 1C C9 DD 81 5C 2B 9B 44 A4 E7 A3 60 AD 72 5D FD 60 BB 63 95 62 2E 67 A5 9F 65 66 9A 63

zmiana:

BD 11 0C CD 50 89 E3 77 88 BF 6E C4 0F D4 E0 0C CC 30 B8 71 6B 20 D7 74 2C B7 AB 12 0A 93 E9 18

Wnioski: NAWET DROBNE MODYFIKACJE W TEKŚCIE WEJŚCIOWYM POCZYNIONEJ ZMIAENIAJĄ WIELE ELEMENTÓW (BITÓW I BAJTÓW) W OTRZYMYWANYCH SKRÓTACH (TAK WYGENEROWANYCH PRZEZ

FUNKCJĘ SHA, JAK I PRZEZ FUNKCJĘ KECCAK). CHOĆ WIADOMOŚCI SĄ BLIŹNIACZO PODOBNE, SKUTKUJE TO W KONCOWYCH SKRÓTACH ODRĘBNE OD SIEBIE.

3. Ataki na funkcje skrótu

Korzystając z szablonów „MD5 Collision Finder" i „SHA-1 Collision" wyznaczyć dla funkcji skrótu MD5 i SHA-1 pary różnych wiadomości, które mają jednakowe skróty. W opracowanym modelu, korzystając z bloku porównywania pokazać, że wiadomości są różne, a skróty jednakowe

MD5

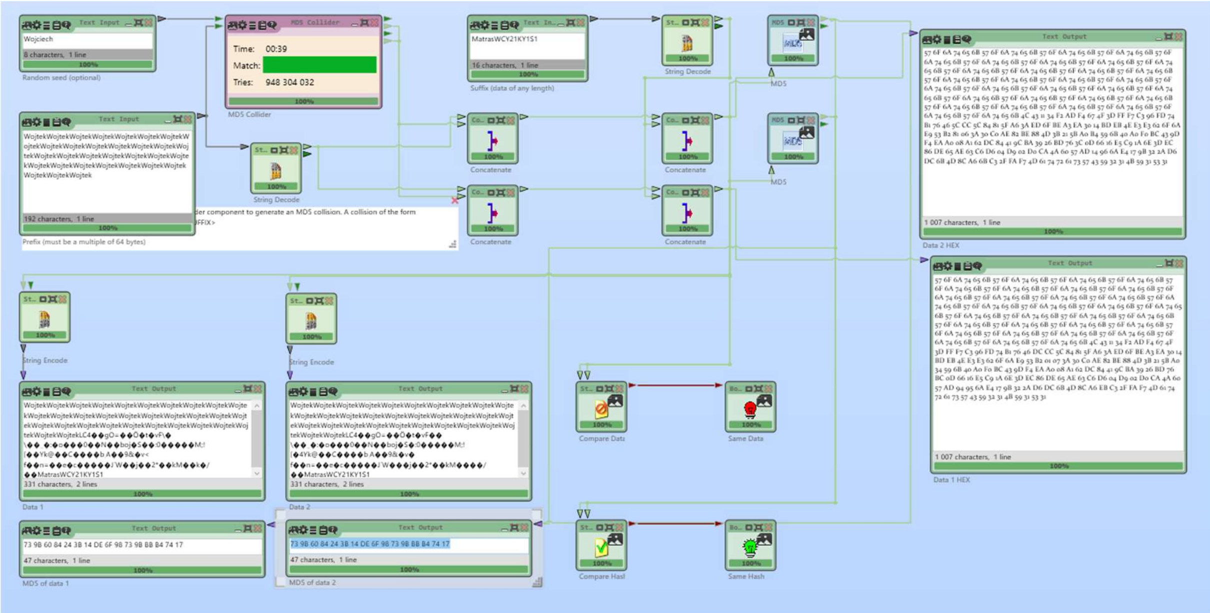
Wiadomosc 1

```
57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B
57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B
57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B
57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B
57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B
57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 4C 43 11 34 F2 AD F4 67 4F 3D FF F7 C3 96 FD 74 B1 76 46 5C CC 5C 84 81
5F A6 3A ED 6F BE A3 EA 30 14 BD EB 4E E3 E3 62 6F 6A E9 53 B2 81 06 3A 30 C0 AE 82 BE 88 4D 3B 21 5B A0
B4 59 6B 40 A0 F0 BC 43 9D F4 EA A0 08 A1 62 DC 84 41 9C BA 39 26 BD 76 3C 0D 66 16 E5 C9 1A 6E 3D EC 86
DE 65 AE 63 C6 D6 04 D9 02 D0 CA 4A 60 57 AD 14 96 6A E4 17 9B 32 2A D6 DC 6B 4D 8C A6 6B C3 2F FA F7 4D
61 74 72 61 73 57 43 59 32 31 4B 59 31 53 31
```

Wiadomosc 2

```
57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B
57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B
57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B
57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B
57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 57 6F 6A 74 65 6B
57 6F 6A 74 65 6B 57 6F 6A 74 65 6B 4C 43 11 34 F2 AD F4 67 4F 3D FF F7 C3 96 FD 74 B1 76 46 DC CC 5C 84
81 5F A6 3A ED 6F BE A3 EA 30 14 BD EB 4E E3 E3 62 6F 6A E9 53 B2 01 07 3A 30 C0 AE 82 BE 88 4D 3B 21 5B
A0 34 59 6B 40 A0 F0 BC 43 9D F4 EA A0 08 A1 62 DC 84 41 9C BA 39 26 BD 76 BC 0D 66 16 E5 C9 1A 6E 3D EC
86 DE 65 AE 63 C6 D6 04 D9 02 D0 CA 4A 60 57 AD 94 95 6A E4 17 9B 32 2A D6 DC 6B 4D 8C A6 EB C3 2F FA F7
4D 61 74 72 61 73 57 43 59 32 31 4B 59 31 53 31
```

Skrot 73 9B 60 84 24 3B 14 DE 6F 98 73 9B BB B4 74 17



SHA 1

wiadomość 1- 25 50 44 46 2D 31 2E 33 0A 25 E2 E3 CF D3 0A 0A 0A 31 20 30 20 6F 62 6A 0A 3C 3C 2F 57 69 64
74 68 20 32 20 30 20 52 2F 48 65 69 67 68 74 20 33 20 30 20 52 2F 54 79 70 65 20 34 20 30 20 52 2F 53 75 62 74
79 70 65 20 35 20 30 20 52 2F 46 69 6C 74 65 72 20 36 20 30 20 52 2F 43 6F 6C 6F 72 53 70 61 63 65 20 37 20 30
20 52 2F 4C 65 6E 67 74 68 20 38 20 30 20 52 2F 42 69 74 73 50 65 72 43 6F 6D 70 6F 6E 65 6E 74 20 38 3E 3E
0A 73 74 72 65 61 6D 0A FF D8 FF FE 00 24 53 48 41 2D 31 20 69 73 20 64 65 61 64 21 21 21 21 21 85 2F EC 09
23 39 75 9C 39 B1 A1 C6 3C 4C 97 E1 FF FE 01 7F 46 DC 93 A6 B6 7E 01 3B 02 9A AA 1D B2 56 0B 45 CA 67 D6
88 C7 F8 4B 8C 4C 79 1F E0 2B 3D F6 14 F8 6D B1 69 09 01 C5 6B 45 C1 53 0A FE DF B7 60 38 E9 72 72 2F E7
AD 72 8F 0E 49 04 E0 46 C2 30 57 0F E9 D4 13 98 AB E1 2E F5 BC 94 2B E3 35 42 A4 80 2D 98 B5 D7 0F 2A 33
2E C3 7F AC 35 14 E7 4D DC 0F 2C C1 A8 74 CD 0C 78 30 5A 21 56 64 61 30 97 89 60 6B D0 BF 3F 98 CD A8 04
46 29 A1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FE 00 FE 00 00 00 00 00 00 00 00 FF E0
00 10 4A 46 49 46 00 01 01 01 00 48 00 48 00 00 FF FE 00 13 43 72 65 61 74 65 64 20 77 69 74 68 20 47 49 4D 50
FF DB 00 43 00 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 FF DB 00 43 01
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 FF C2 00 11 08 00 08 00 08 03
01 11 00 02 11 01 03 11 01 FF C4 00 14 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 FF C4 00 14 01 01
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 FF FE 00 06 FF FE 00 2F FF DA 00 0C 03 01 00 02 10 03 10 00
00 01 53 9D C5 1F FF C4 00 15 10 01 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 16 26 FF FE 00 06 FF FE 00
33 FF DA 00 08 01 01 00 01 05 02 A9 53 FF C4 00 1F 11 00 00 03 09 00 00 00 00 00 00 00 00 00 00 00 00 14 15 17
00 13 16 27 45 63 65 86 95 FF FE 00 06 FF FE 00 41 FF DA 00 08 01 03 01 01 3F 01 9A 8A A5 6D 53 3B B2 38 73
9E 61 21 66 B9 0E 60 5B FF C4 00 1E 11 00 00 04 07 00 00 00 00 00 00 00 00 00 00 00 00 14 15 17 13 27 45 63
65 85 94 FF FE 00 06 FF FE 00 40 FF DA 00 08 01 02 01 01 3F 01 98 4E 15 55 C1 55 B6 6C DC 3E 04 A2 1A 44 4C
40 FF C4 00 1E 10 00 01 01 09 00 00 00 00 00 00 00 00 00 00 00 00 14 13 00 12 15 16 44 62 64 85 94 FF FE 00 06
FF FE 00 33 FF DA 00 08 01 01 00 06 3F 02 AD 9A 4D B1 75 DC E6 08 6D 74 3B 05 BF FF C4 00 14 10 01 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 FF FE 00 06 FF FE 00 12 FF DA 00 08 01 01 00 01 3F 21 60 01 FF FE 00
06 FF FE 00 2B FF DA 00 0C 03 01 00 02 00 03 00 00 00 10 1F FF C4 00 14 11 01 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 FF FE 00 06 FF FE 00 28 FF DA 00 08 01 03 01 01 3F 10 69 80 FF C4 00 14 11 01 00 00 00 00

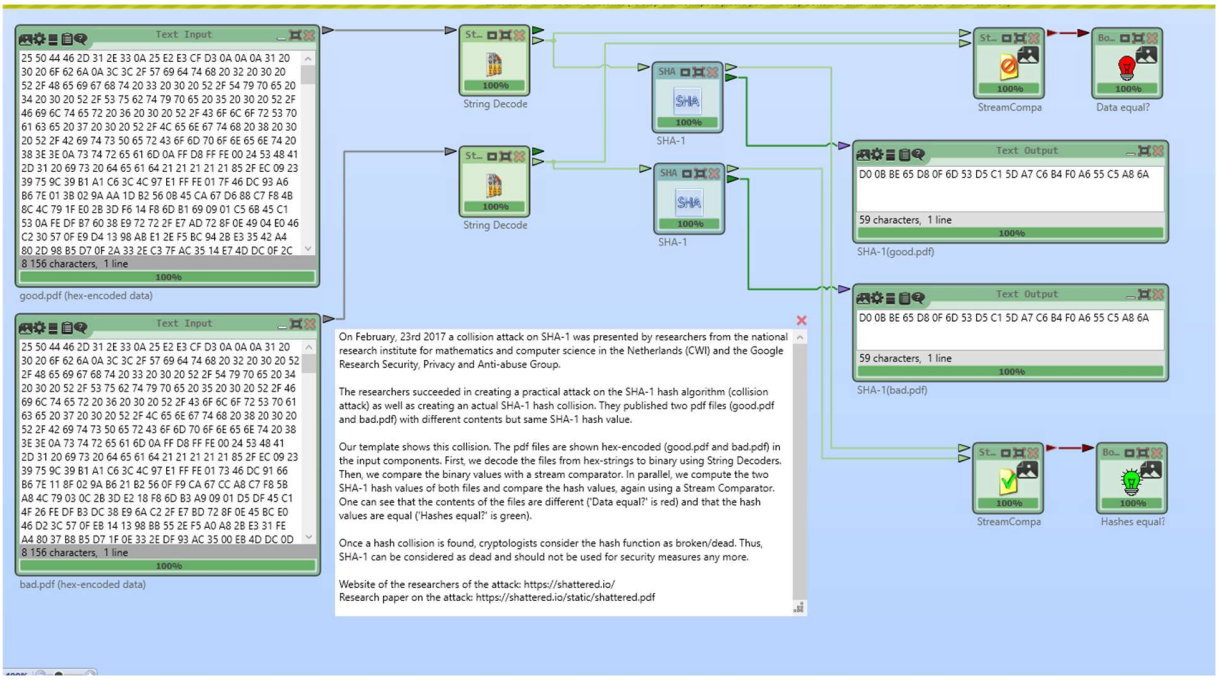
```
00 00 00 00 00 00 00 00 00 00 00 00 FF FE 00 06 FF FE 00 28 FF DA 00 08 01 02 01 01 3F 10 6B C7 FF C4 00 14
10 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FE 00 06 FF FE 00 14 FF DA 00 08 01 01 00 01 3F 10 15
3F FF D9 41 4E 47 45 FF E0 00 10 4A 46 49 46 00 01 01 01 00 48 00 48 00 00 FF FE 00 13 43 72 65 61 74 65 64 20
77 69 74 68 20 47 49 4D 50 FF DB 00 43 00 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
01 01 01 01 FF DB 00 43 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 FF
C2 00 11 08 00 08 00 08 03 01 11 00 02 11 01 03 11 01 FF C4 00 14 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 09 FF C4 00 15 01 01 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 06 07 FF DA 00 0C 03 01 00 02 10 03 10
00 00 01 52 4A 5F FF 00 FF C4 00 14 10 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF DA 00 08 01 01 00
01 05 02 7F FF C4 00 18 11 00 02 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F0 37 A7 B7 FF DA 00 08 01 03 01
01 3F 01 DF DB FD 9F CF FF C4 00 18 11 00 02 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F0 36 A6 B6 FF DA
00 08 01 02 01 01 3F 01 CA 35 46 28 7F FF C4 00 18 10 00 02 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F0 37
67 A7 FF DA 00 08 01 01 00 06 3F 02 A9 9C 99 89 8F FF C4 00 14 10 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 FF DA 00 08 01 01 00 01 3F 21 7F FF DA 00 0C 03 01 00 02 00 03 00 00 00 10 1F FF C4 00 14 11 01 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF DA 00 08 01 03 01 01 3F 10 0F FF C4 00 14 11 01 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 FF DA 00 08 01 02 01 01 3F 10 0F FF C4 00 14 10 01 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 FF DA 00 08 01 01 00 01 3F 10 0F FF D9 0A 65 6E 64 73 74 72 65 61 6D 0A 65 6E 64 6F 62 6A
0A 0A 32 20 30 20 6F 62 6A 0A 38 0A 65 6E 64 6F 62 6A 0A 0A 33 20 30 20 6F 62 6A 0A 38 0A 65 6E 64 6F 62 6A
0A 0A 34 20 30 20 6F 62 6A 0A 2F 58 4F 62 6A 65 63 74 0A 65 6E 64 6F 62 6A 0A 0A 35 20 30 20 6F 62 6A 0A 2F 49
6D 61 67 65 0A 65 6E 64 6F 62 6A 0A 0A 36 20 30 20 6F 62 6A 0A 2F 44 43 54 44 65 63 6F 64 65 0A 65 6E 64 6F 62
6A 0A 0A 37 20 30 20 6F 62 6A 0A 2F 44 65 76 69 63 65 52 47 42 0A 65 6E 64 6F 62 6A 0A 0A 38 20 30 20 6F 62 6A
0A 31 36 39 33 0A 65 6E 64 6F 62 6A 0A 0A 39 20 30 20 6F 62 6A 0A 3C 3C 0A 20 20 2F 54 79 70 65 20 2F 43 61
74 61 6C 6F 67 0A 20 20 2F 50 61 67 65 73 20 31 30 20 30 20 52 0A 3E 3E 0A 65 6E 64 6F 62 6A 0A 0A 0A 31 30 20
30 20 6F 62 6A 0A 3C 3C 0A 20 20 2F 54 79 70 65 20 2F 50 61 67 65 73 0A 20 20 2F 43 6F 75 6E 74 20 31 0A 20 20
2F 4B 69 64 73 20 5B 31 31 20 30 20 52 5D 0A 3E 3E 0A 65 6E 64 6F 62 6A 0A 0A 31 31 20 30 20 6F 62 6A 0A 3C
3C 0A 20 20 2F 54 79 70 65 20 2F 50 61 67 65 0A 20 20 2F 50 61 72 65 6E 74 20 31 30 20 30 20 52 0A 20 20 2F 4D
65 64 69 61 42 6F 78 20 5B 30 20 30 20 38 20 38 5D 0A 20 20 2F 43 72 6F 70 42 6F 78 20 5B 30 20 30 20 38 20 38
5D 0A 20 20 2F 43 6F 6E 74 65 6E 74 73 20 31 32 20 30 20 52 0A 20 20 2F 52 65 73 6F 75 72 63 65 73 0A 20 20 3C
3C 0A 20 20 20 20 2F 58 4F 62 6A 65 63 74 20 3C 3C 2F 49 6D 30 20 31 20 30 20 52 3E 3E 0A 20 20 3E 3E 0A 3E
3E 0A 65 6E 64 6F 62 6A 0A 0A 31 32 20 30 20 6F 62 6A 0A 3C 3C 2F 4C 65 6E 67 74 68 20 33 30 3E 3E 0A 73 74
72 65 61 6D 0A 71 0A 20 20 38 20 30 20 30 20 38 20 30 20 30 20 63 6D 0A 20 20 2F 49 6D 30 20 44 6F 0A 51 0A 65
6E 64 73 74 72 65 61 6D 0A 65 6E 64 6F 62 6A 0A 0A 0A 0A 78 72 65 66 0A 30 20 31 33 20 0A 30 30 30 30 30 30 30
30 30 30 20 36 35 35 33 35 20 66 20 0A 30 30 30 30 30 30 30 30 31 37 20 30 30 30 30 30 20 6E 20 0A 30 30 30 30
30 30 31 38 36 31 20 30 30 30 30 30 20 6E 20 0A 30 30 30 30 30 30 31 38 37 39 20 30 30 30 30 30 20 6E 20 0A 30
30 30 30 30 30 31 38 39 37 20 30 30 30 30 30 20 6E 20 0A 30 30 30 30 30 30 31 39 32 32 20 30 30 30 30 30 20 6E
20 0A 30 30 30 30 30 30 31 39 34 35 20 30 30 30 30 30 20 6E 20 0A 30 30 30 30 30 30 31 39 37 32 20 30 30 30 30
30 20 6E 20 0A 30 30 30 30 30 30 31 39 39 39 20 30 30 30 30 30 20 6E 20 0A 30 30 30 30 30 30 32 30 32 30 20 30
30 30 30 30 20 6E 20 0A 30 30 30 30 30 30 32 30 37 36 20 30 30 30 30 30 20 6E 20 0A 30 30 30 30 30 30 32 31 34
32 20 30 30 30 30 30 20 6E 20 0A 30 30 30 30 30 30 32 33 30 39 20 30 30 30 30 30 20 6E 20 0A 0A 74 72 61 69 6C
65 72 20 3C 3C 20 2F 52 6F 6F 74 20 39 20 30 20 52 20 2F 53 69 7A 65 20 31 33 3E 3E 0A 0A 73 74 61 72 74 78 72
65 66 0A 32 33 39 31 0A 25 25 45 4F 46 0A
```

```
wiadomość 2- 25 50 44 46 2D 31 2E 33 0A 25 E2 E3 CF D3 0A 0A 0A 31 20 30 20 6F 62 6A 0A 3C 3C 2F 57 69 64
74 68 20 32 20 30 20 52 2F 48 65 69 67 68 74 20 33 20 30 20 52 2F 54 79 70 65 20 34 20 30 20 52 2F 53 75 62 74
79 70 65 20 35 20 30 20 52 2F 46 69 6C 74 65 72 20 36 20 30 20 52 2F 43 6F 6C 6F 72 53 70 61 63 65 20 37 20 30
20 52 2F 4C 65 6E 67 74 68 20 38 20 30 20 52 2F 42 69 74 73 50 65 72 43 6F 6D 70 6F 6E 65 6E 74 20 38 3E 3E
0A 73 74 72 65 61 6D 0A FF D8 FF FE 00 24 53 48 41 2D 31 20 69 73 20 64 65 61 64 21 21 21 21 21 85 2F EC 09
23 39 75 9C 39 B1 A1 C6 3C 4C 97 E1 FF FE 01 73 46 DC 91 66 B6 7E 11 8F 02 9A B6 21 B2 56 0F F9 CA 67 CC
A8 C7 F8 5B A8 4C 79 03 0C 2B 3D E2 18 F8 6D B3 A9 09 01 D5 DF 45 C1 4F 26 FE DF B3 DC 38 E9 6A C2 2F E7
BD 72 8F 0E 45 BC E0 46 D2 3C 57 0F EB 14 13 98 BB 55 2E F5 A0 A8 2B E3 31 FE A4 80 37 B8 B5 D7 1F 0E 33
2E DF 93 AC 35 00 EB 4D DC 0D EC C1 A8 64 79 0C 78 2C 76 21 56 60 DD 30 97 91 D0 6B D0 AF 3F 98 CD A4 BC
46 29 B1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FE 00 FE 00 00 00 00 00 00 00 00 FF E0
00 10 4A 46 49 46 00 01 01 01 00 48 00 48 00 00 FF FE 00 13 43 72 65 61 74 65 64 20 77 69 74 68 20 47 49 4D 50
FF DB 00 43 00 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 FF DB 00 43 01
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 FF C2 00 11 08 00 08 00 08 03
01 11 00 02 11 01 03 11 01 FF C4 00 14 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 FF C4 00 14 01 01
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 FF FE 00 06 FF FE 00 2F FF DA 00 0C 03 01 00 02 10 03 10 00
00 01 53 9D C5 1F FF C4 00 15 10 01 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 16 26 FF FE 00 06 FF FE 00
33 FF DA 00 08 01 01 00 01 05 02 A9 53 FF C4 00 1F 11 00 00 03 09 00 00 00 00 00 00 00 00 00 00 00 00 14 15 17
00 13 16 27 45 63 65 86 95 FF FE 00 06 FF FE 00 41 FF DA 00 08 01 03 01 01 3F 01 9A 8A A5 6D 53 3B B2 38 73
9E 61 21 66 B9 0E 60 5B FF C4 00 1E 11 00 00 04 07 00 00 00 00 00 00 00 00 00 00 00 00 00 14 15 17 13 27 45 63
65 85 94 FF FE 00 06 FF FE 00 40 FF DA 00 08 01 02 01 01 3F 01 98 4E 15 55 C1 55 B6 6C DC 3E 04 A2 1A 44 4C
40 FF C4 00 1E 10 00 01 01 09 00 00 00 00 00 00 00 00 00 00 00 00 14 13 00 12 15 16 44 62 64 85 94 FF FE 00 06
FF FE 00 33 FF DA 00 08 01 01 00 06 3F 02 AD 9A 4D B1 75 DC E6 08 6D 74 3B 05 BF FF C4 00 14 10 01 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 FF FE 00 06 FF FE 00 12 FF DA 00 08 01 01 00 01 3F 21 60 01 FF FE 00
06 FF FE 00 2B FF DA 00 0C 03 01 00 02 00 03 00 00 00 10 1F FF C4 00 14 11 01 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 FF FE 00 06 FF FE 00 28 FF DA 00 08 01 03 01 01 3F 10 69 80 FF C4 00 14 11 01 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 FF FE 00 06 FF FE 00 28 FF DA 00 08 01 02 01 01 3F 10 6B C7 FF C4 00 14
10 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FE 00 06 FF FE 00 14 FF DA 00 08 01 01 00 01 3F 10 15
3F FF D9 41 4E 47 45 FF E0 00 10 4A 46 49 46 00 01 01 01 00 48 00 48 00 00 FF FE 00 13 43 72 65 61 74 65 64 20
77 69 74 68 20 47 49 4D 50 FF DB 00 43 00 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
01 01 01 01 FF DB 00 43 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 FF
C2 00 11 08 00 08 00 08 03 01 11 00 02 11 01 03 11 01 FF C4 00 14 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 09 FF C4 00 15 01 01 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 06 07 FF DA 00 0C 03 01 00 02 10 03 10
00 00 01 52 4A 5F FF 00 FF C4 00 14 10 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF DA 00 08 01 01 00
01 05 02 7F FF C4 00 18 11 00 02 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F0 37 A7 B7 FF DA 00 08 01 03 01
01 3F 01 DF DB FD 9F CF FF C4 00 18 11 00 02 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F0 36 A6 B6 FF DA
00 08 01 02 01 01 3F 01 CA 35 46 28 7F FF C4 00 18 10 00 02 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F0 37
67 A7 FF DA 00 08 01 01 00 06 3F 02 A9 9C 99 89 8F FF C4 00 14 10 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 FF DA 00 08 01 01 00 01 3F 21 7F FF DA 00 0C 03 01 00 02 00 03 00 00 00 10 1F FF C4 00 14 11 01 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF DA 00 08 01 03 01 01 3F 10 0F FF C4 00 14 11 01 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 FF DA 00 08 01 02 01 01 3F 10 0F FF C4 00 14 10 01 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 FF DA 00 08 01 01 00 01 3F 10 0F FF D9 0A 65 6E 64 73 74 72 65 61 6D 0A 65 6E 64 6F 62 6A
0A 0A 32 20 30 20 6F 62 6A 0A 38 0A 65 6E 64 6F 62 6A 0A 0A 33 20 30 20 6F 62 6A 0A 38 0A 65 6E 64 6F 62 6A
0A 0A 34 20 30 20 6F 62 6A 0A 2F 58 4F 62 6A 65 63 74 0A 65 6E 64 6F 62 6A 0A 0A 35 20 30 20 6F 62 6A 0A 2F 49
6D 61 67 65 0A 65 6E 64 6F 62 6A 0A 0A 36 20 30 20 6F 62 6A 0A 2F 44 43 54 44 65 63 6F 64 65 0A 65 6E 64 6F 62
6A 0A 0A 37 20 30 20 6F 62 6A 0A 2F 44 65 76 69 63 65 52 47 42 0A 65 6E 64 6F 62 6A 0A 0A 38 20 30 20 6F 62 6A
0A 31 36 39 33 0A 65 6E 64 6F 62 6A 0A 0A 39 20 30 20 6F 62 6A 0A 3C 3C 0A 20 20 2F 54 79 70 65 20 2F 43 61
74 61 6C 6F 67 0A 20 20 2F 50 61 67 65 73 20 31 30 20 30 20 52 0A 3E 3E 0A 65 6E 64 6F 62 6A 0A 0A 0A 31 30 20
30 20 6F 62 6A 0A 3C 3C 0A 20 20 2F 54 79 70 65 20 2F 50 61 67 65 73 0A 20 20 2F 43 6F 75 6E 74 20 31 0A 20 20
2F 4B 69 64 73 20 5B 31 31 20 30 20 52 5D 0A 3E 3E 0A 65 6E 64 6F 62 6A 0A 0A 31 31 20 30 20 6F 62 6A 0A 3C
3C 0A 20 20 2F 54 79 70 65 20 2F 50 61 67 65 0A 20 20 2F 50 61 72 65 6E 74 20 31 30 20 30 20 52 0A 20 20 2F 4D
65 64 69 61 42 6F 78 20 5B 30 20 30 20 38 20 38 5D 0A 20 20 2F 43 72 6F 70 42 6F 78 20 5B 30 20 30 20 38 20 38
5D 0A 20 20 2F 43 6F 6E 74 65 6E 74 73 20 31 32 20 30 20 52 0A 20 20 2F 52 65 73 6F 75 72 63 65 73 0A 20 20 3C
3C 0A 20 20 20 20 2F 58 4F 62 6A 65 63 74 20 3C 3C 2F 49 6D 30 20 31 20 30 20 52 3E 3E 0A 20 20 3E 3E 0A 3E
3E 0A 65 6E 64 6F 62 6A 0A 0A 31 32 20 30 20 6F 62 6A 0A 3C 3C 2F 4C 65 6E 67 74 68 20 33 30 3E 3E 0A 73 74
72 65 61 6D 0A 71 0A 20 20 38 20 30 20 30 20 38 20 30 20 30 20 63 6D 0A 20 20 2F 49 6D 30 20 44 6F 0A 51 0A 65
6E 64 73 74 72 65 61 6D 0A 65 6E 64 6F 62 6A 0A 0A 0A 0A 78 72 65 66 0A 30 20 31 33 20 0A 30 30 30 30 30 30 30
30 30 30 20 36 35 35 33 35 20 66 20 0A 30 30 30 30 30 30 30 30 31 37 20 30 30 30 30 30 20 6E 20 0A 30 30 30 30
30 30 31 38 36 31 20 30 30 30 30 30 20 6E 20 0A 30 30 30 30 30 30 31 38 37 39 20 30 30 30 30 30 20 6E 20 0A 30
30 30 30 30 30 31 38 39 37 20 30 30 30 30 30 20 6E 20 0A 30 30 30 30 30 30 31 39 32 32 20 30 30 30 30 30 20 6E
20 0A 30 30 30 30 30 30 31 39 34 35 20 30 30 30 30 30 20 6E 20 0A 30 30 30 30 30 30 31 39 37 32 20 30 30 30 30
30 20 6E 20 0A 30 30 30 30 30 30 31 39 39 39 20 30 30 30 30 30 20 6E 20 0A 30 30 30 30 30 30 32 30 32 30 20 30
30 30 30 30 20 6E 20 0A 30 30 30 30 30 30 32 30 37 36 20 30 30 30 30 30 20 6E 20 0A 30 30 30 30 30 30 32 31 34
32 20 30 30 30 30 30 20 6E 20 0A 30 30 30 30 30 30 32 33 30 39 20 30 30 30 30 30 20 6E 20 0A 0A 74 72 61 69 6C

65 72 20 3C 3C 20 2F 52 6F 6F 74 20 39 20 30 20 52 20 2F 53 69 7A 65 20 31 33 3E 3E 0A 0A 73 74 61 72 74 78 72 65 66 0A 32 33 39 31 0A 25 25 45 4F 46 0A

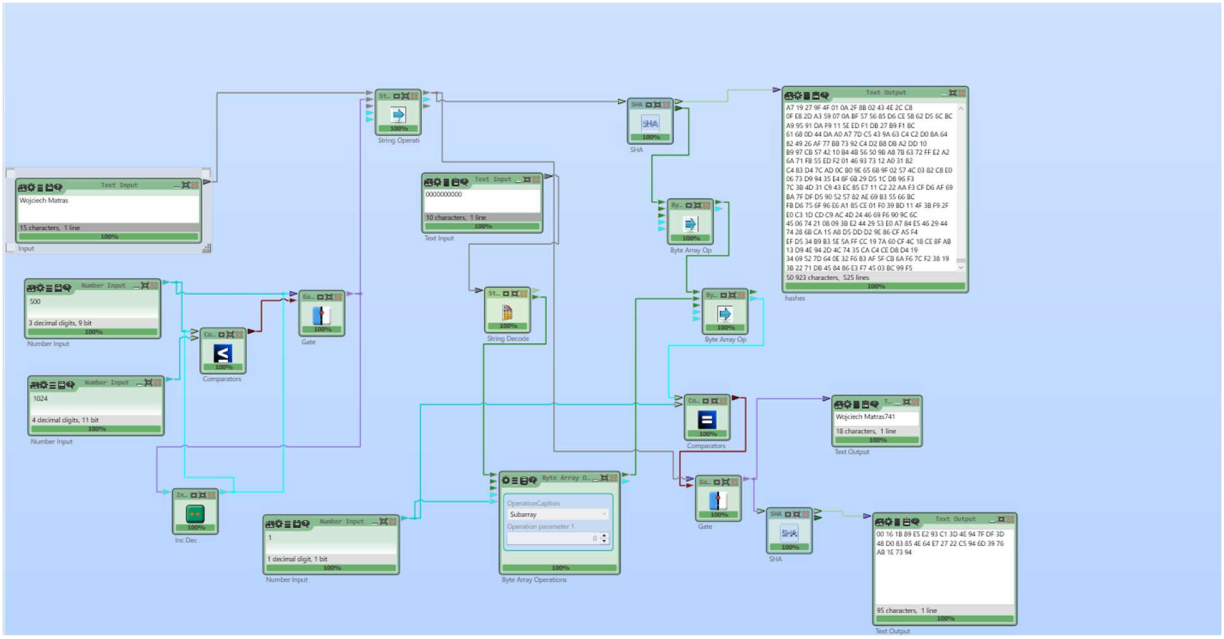
skrót D0 0B BE 65 D8 0F 6D 53 D5 C1 5D A7 C6 B4 F0 A6 55 C5 A8 6A



Dla wybranej standardowej funkcji skrótu (SHA-2 lub SHA-3) i dla dowolnej długości generowanego skrótu znaleźć wiadomość (przeciwobraz), której pierwszy bajt skrótu jest równy 00. Wypisać tę wiadomość i jej skrót.

wiadomość Wojciech Matras741

skrot SHA-256 00 16 1B 89 E5 E2 93 C1 3D 4E 94 7F DF 3D 48 D0 83 85 4E 64 E7 27 22 C5 94 6D 39 76 AB 1E 73 94



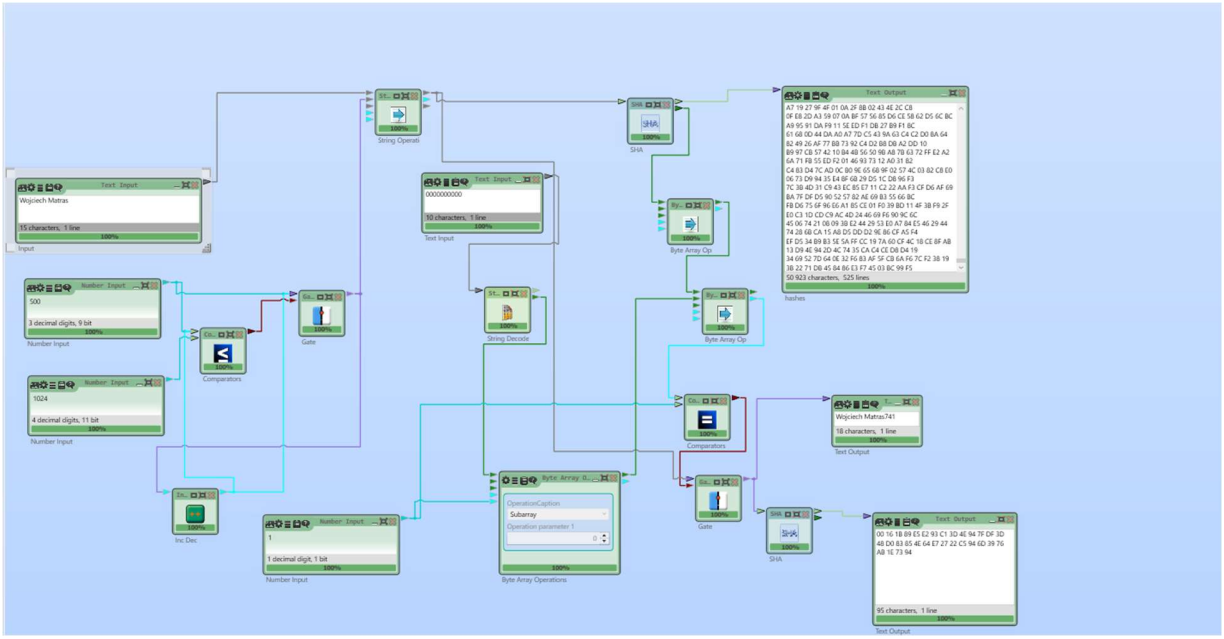
Dla wybranej standardowej funkcji skrótu (SHA-2 lub SHA-3) i dla dowolnej długości generowanego skrótu znaleźć dwie różne wiadomości, których pierwszy bajt skrótu jest taki sam (kolizja). Wypisać obie wiadomości i ich skróty.

Wiadomość 1- Wojciech Matras583

Skrot 1- 00 B8 41 AD 1C 61 B4 83 88 5A A7 B7 21 92 9D 8F C2 DB 80 0B FC 6C 4E CD 4D BD 56 2F 29 D2 22 4C

Wiadomosc 2- Wojciech Matras741

skrot SHA-256 00 16 1B 89 E5 E2 93 C1 3D 4E 94 7F DF 3D 48 D0 83 85 4E 64 E7 27 22 C5 94 6D 39 76 AB 1E 73 94



Korzystając z funkcji skrótu SHA-2 albo SHA-3 z dowolną długością skrótu opracować model funkcji skrótu z kluczem (MAC) na bazie funkcji skrótu (HMAC) zgodnie ze standardem FIPS 198-1. Przy użyciu tego modelu wyznaczyć skrót wiadomości utworzonej z własnego imienia i nazwiska stosując losowy klucz odpowiedniej długości.

Wiadmosc: Wojciech Matras

Klucz: “The top half of the workspace consists of an arrangement of other existing components to calculate an MD5-HMAC "manually". These”

HMAC: C4 6F 55 CD 05 31 2B 80 CF 4C D7 DD B9 FA D0 76 DC 08 48 35 2D B3 FC FE 86 D3 E2 01 BA 6A 4B 3D 58 88 E6 C1 AB B5 C1 96 40 2E 9C A3 89 99 9A 92 57 93 24 27 44 8A 10 9B 77 DE 31 B4 D8 06 BA A4