**Sprawozdanie nr 5**

**z przedmiotu Wybrane Elementy Kryptologii**

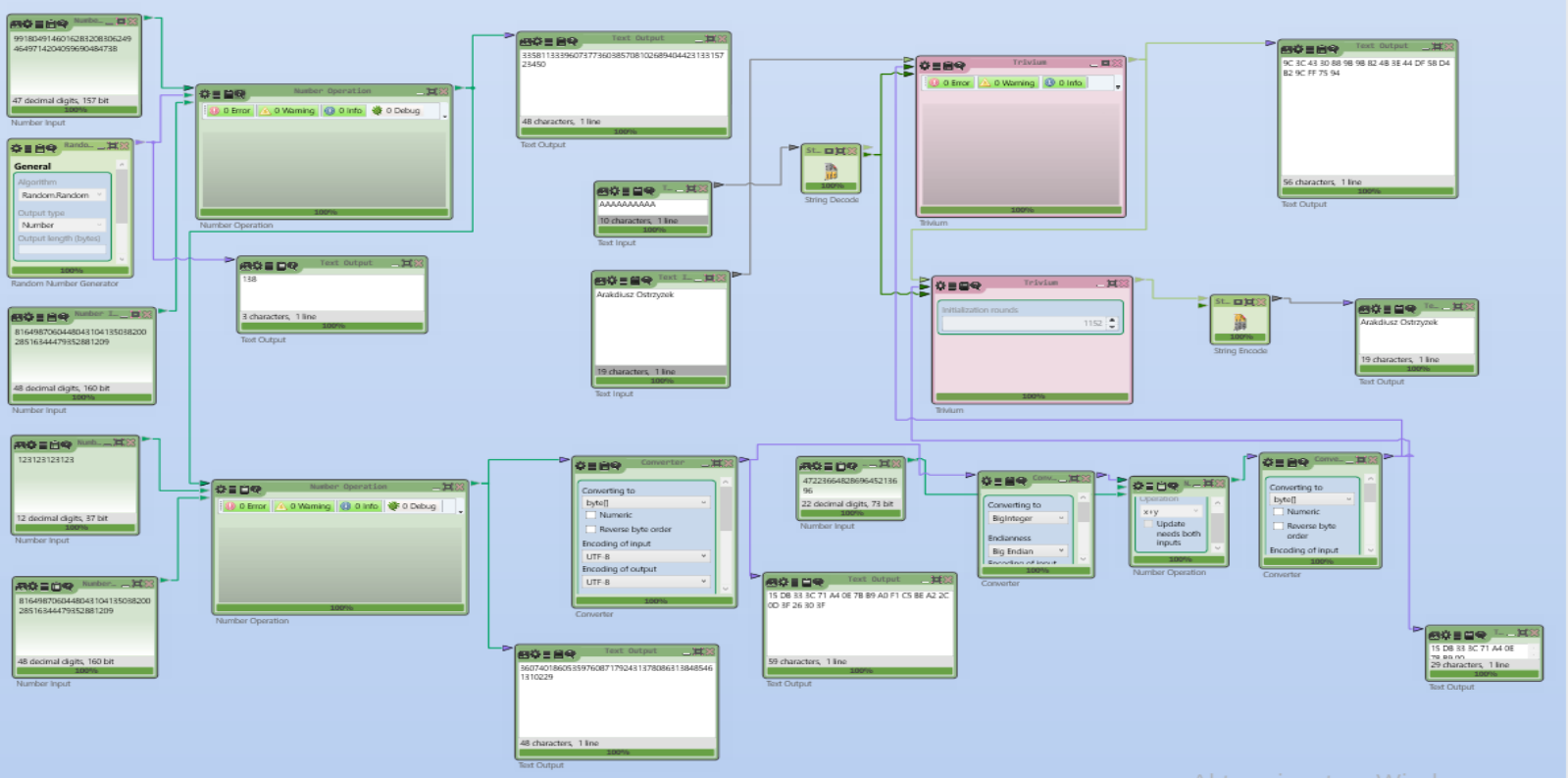
1. **Zagadnienie**

Szyfrowanie hybrydowe. Funkcje skrótu.

1. **Cel**

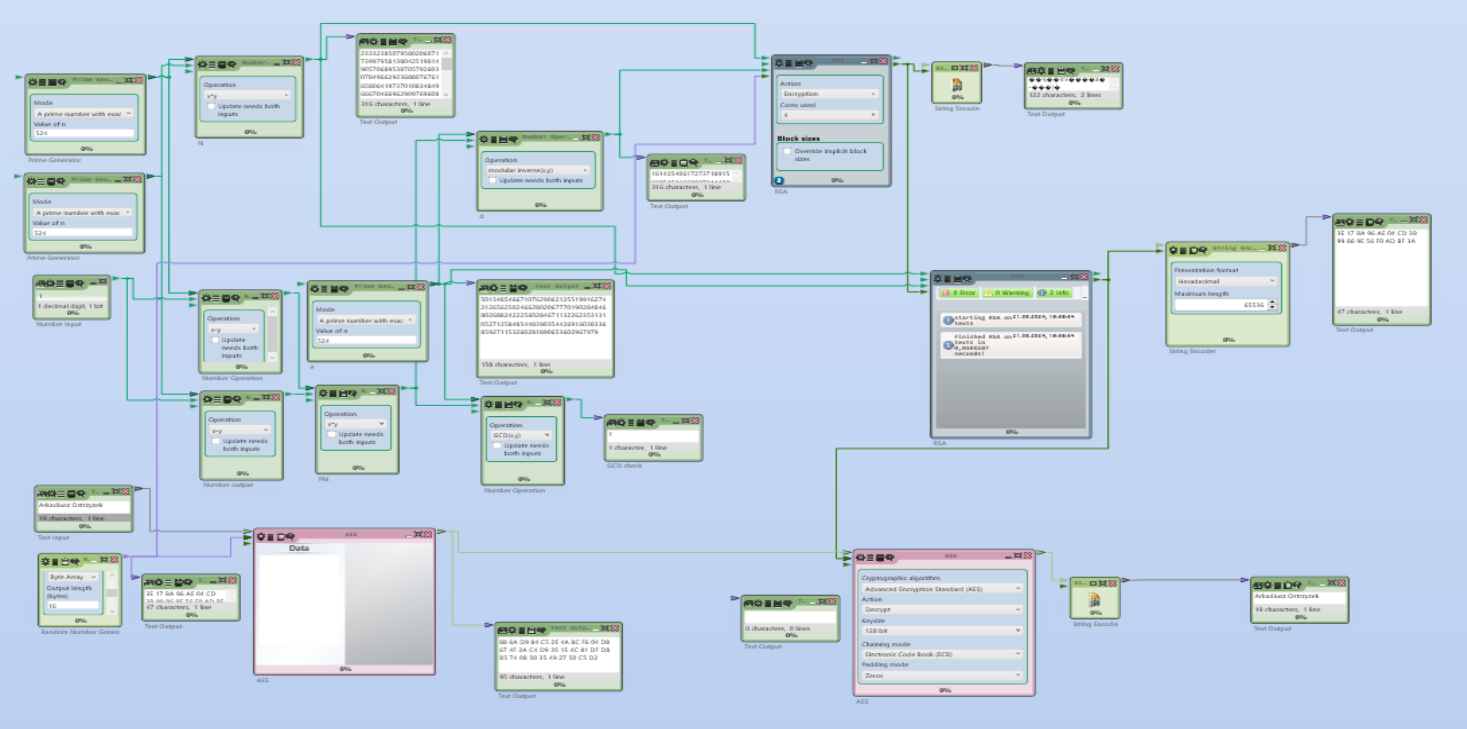
Zajęcia laboratoryjne realizowane z wykorzystaniem programu CryptTool 2.1 mające na celu zapoznanie się z sposobem realizacji szyfrowania hybrydowego oraz z własnościami funkcji skrótu, w tym standardami SHA-2 i SHA-3.

1. **Zadania do realizacji w sprawozdaniu**
2. Szyfrowanie hybrydowe
3. Korzystając ze schematów z poprzednich laboratoriów realizujących protokół Diffie-Hellmana (dla parametrów podanych w pliku) i szyfru Trivium opracować model, który umożliwia uzgodnienie klucza w sposób asymetryczny i wykorzystanie uzgodnionego klucza do szyfrowania i deszyfrowania szyfrem symetrycznym (strumieniowym). Korzystając z tego modelu uzgodnić tajny klucz i wykonać nim szyfrowanie i deszyfrowanie wiadomości utworzonej z własnego imienia i nazwiska.



|  |  |
| --- | --- |
| P | 816498706044804310413503820028516344479352881209 |
| Q | 99180491460162832083062494649714204059690484738 |
| a | 138 |
| b | 123123123123 |
| klucz | 15 DB 33 3C 71 A4 0E 7B B9 00 |
| Wiadomość | Arkadiusz Ostrzyżek |
| szyfrogram | 9C 3C 43 30 88 9B 9B 82 4B 3E 44 DF 58 D4 B2 9C FF 75 94 |

1. 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.



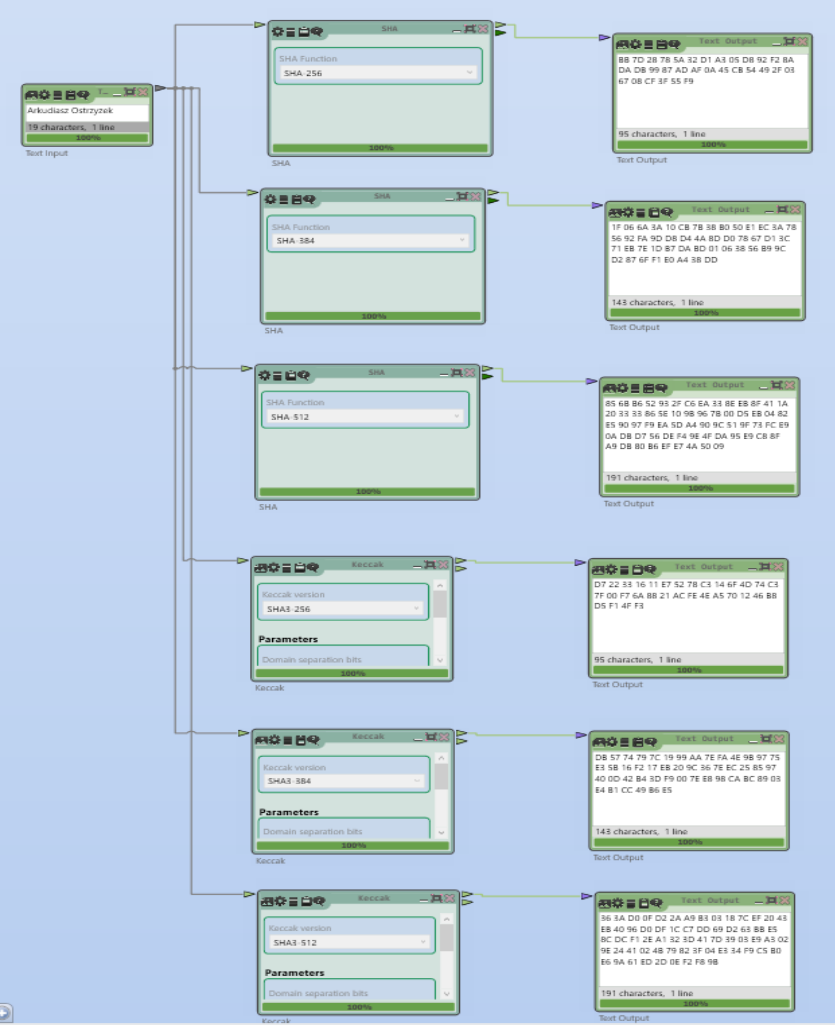
|  |  |
| --- | --- |
| P | 28050842437086530921206033705823526841851911701567340160991802835345986599877299584012458725933782906697535957894842507660125979613216930610663349224579851587 |
| q | 39245235960947604066749967399292166033291532327447994933634887238639639181032375236837824676322227993122117249134173691532863387110291619510095135705781613991 |
| N | 1860306233084495606110239035205046136175377314347922922801752692073858142643542633524950575556793937309106640322489391401293491890169570138328732847769158566919065548662718214893144360689320626090215315507804723535168802006535051783373893977980414901049544411165872069630739567662920705828646149683001723252129519087 |
| Phi |  |
| e | 35793581037569205791540107840261062306753195053973981039192750573647742323415899092023692716055267936412977739787172999286553451694787373332653527731011221413 |
| d | 161539051082239091864803047744152468916753866978375699879905436547319026873207657574186809686720091390716134297129017611570744439922582998165450861682762636552160127657905655234307756356853422618398746520810649268151751191256326515853673153086970291395286536847938564092596802322603196469252857191287933575257826717 |
| Szyfrogram rsa | 13 27 7C 60 55 17 D2 67 67 CA C4 8F 41 74 6D F8 0D B6 E1 3A D8 AF AD 5C 1D 32 71 E1 72 6B 7B B5 51 40 34 F7 EB 72 18 8B AB 6F 15 66 EA 8A 5E 64 90 71 5A 11 84 BC 69 2F C2 AE 97 B9 5A 3C 10 D1 69 A5 B4 97 F8 0D 35 CD DD 68 AD 46 D3 C8 5F BF 9C DA 9A AE 93 44 BD 6E A6 73 AC 1F C5 34 1A 4B 8B 99 8E F6 F2 BF C7 53 50 0B E8 AA E9 4C 1D 8F 6E 93 C9 3F 5E 55 72 2B 55 40 EE 45 A2 85 B7 97 27 15 25 |
| Wiadomość | Arkadiusz Ostrzyzek |
| Aes key | 3E 17 BA 96 AE 04 CD 3B 99 86 9E 56 F0 AD BF 3A |
| Szyfrogram aes | 88 6A D9 84 C5 2E 4A 8C F6 04 DB 67 4F 2A C4 D9 35 1E 4C 81 DF D8 B5 74 0B 50 35 49 27 50 C5 D2 |
| Szyfrogram RSA | 13 27 7C 60 55 17 D2 67 67 CA C4 8F 41 74 6D F8 0D B6 E1 3A D8 AF AD 5C 1D 32 71 E1 72 6B 7B B5 51 40 34 F7 EB 72 18 8B AB 6F 15 66 EA 8A 5E 64 90 71 5A 11 84 BC 69 2F C2 AE 97 B9 5A 3C 10 D1 69 A5 B4 97 F8 0D 35 CD DD 68 AD 46 D3 C8 5F BF 9C DA 9A AE 93 44 BD 6E A6 73 AC 1F C5 34 1A 4B 8B 99 8E F6 F2 BF C7 53 50 0B E8 AA E9 4C 1D 8F 6E 93 C9 3F 5E 55 72 2B 55 40 EE 45 A2 85 B7 97 27 15 25 |

1. Korzystając z modelu z poprzedniego podpunktu odczytaj wiadomość zaszyfrowaną hybrydowo szyfrem RSA i AES, której szyfrogramy zamieszczono w pliku do tego zadania.

|  |  |
| --- | --- |
| Moduł n | 644134708246853276396028587119792896257182745964948457011481049178310337255118407738388839 |
| Klucz jawny odbiorcy e | 108054456883440680435118185435842336553483494197784264002515198563504813886035083060546337 |
| Szyfrogram aes | 55 92 44 DD A8 9B C4 8C 95 68 89 09 28 C7 E0 D7 8A AE 9C BB 21 58 C1 AB 52 89 27 84 03 05 F4 4D 30 32 22 41 24 03 6A C6 6C C9 24 11 ED 41 46 22 9B 50 54 06 BE 59 8B 39 D9 A7 6F 3A CB 1B EE 8E |
| Szyfrogram rsa | 475978677907588718062828445241133687577241688938246767269026388530308830239034756594241933 |
| p | 191345727257741441518254159472328312311114061 |
| q | 830825649662879377561783488176232788397942403 |
| d | 55114238743750392654464094396889169525116514512898373332911168324739550958425762249201547 |
| Klucz aes |  |
| Tekst jawny |  |

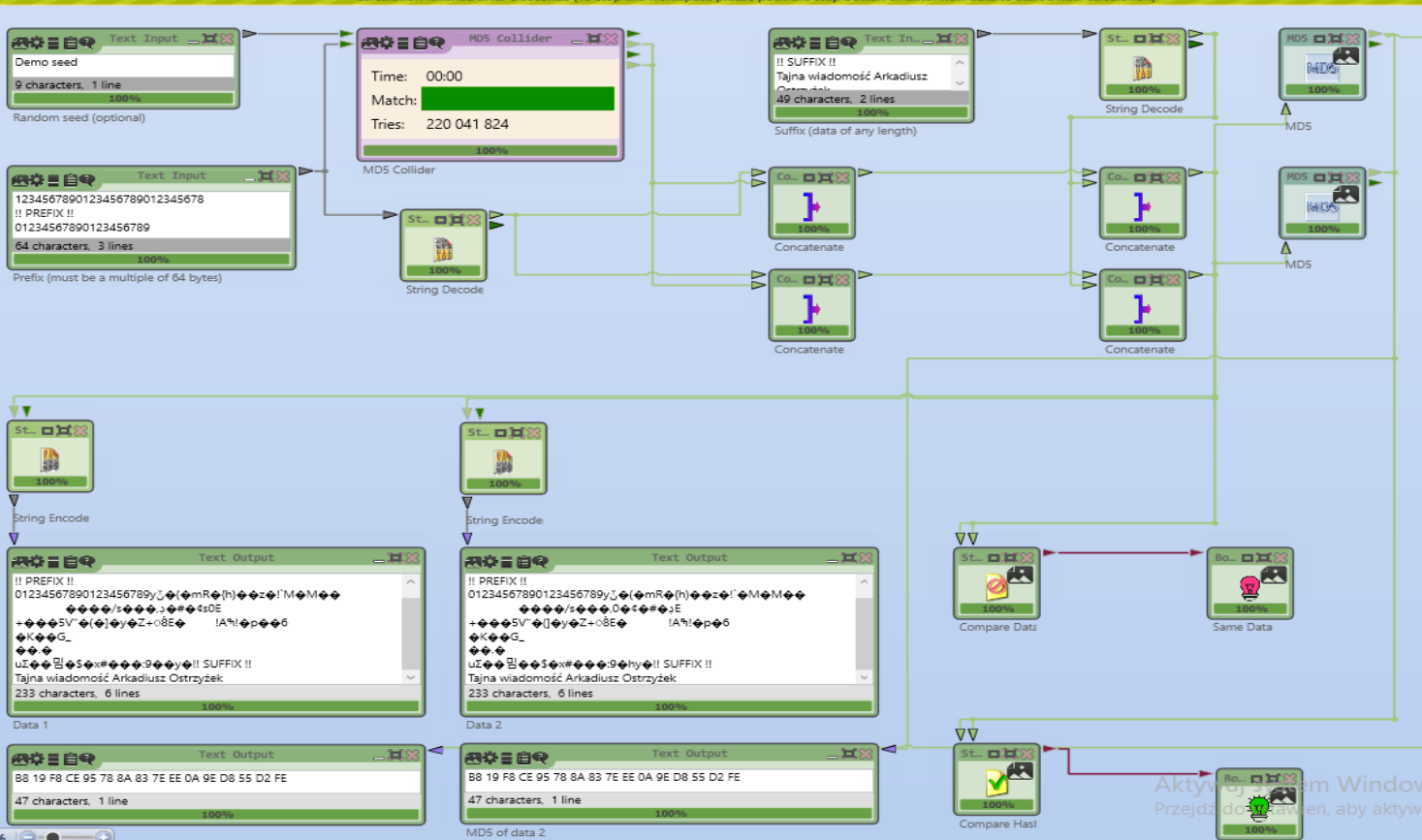
1. Standardowe funkcje skrótu SHA-2 i SHA-3 (Keccak)

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.



|  |  |  |
| --- | --- | --- |
| Wiadomość hashowana | Arkadiusz Ostrzyzek | Arkudiasz Ostrzyzek |
| SHA-256 | 8B 57 1B AD 04 D6 49 FA 99 AE 4F 03 38 98 72 CD 54 65 9F 84 53 68 0B 55 7D A4 D0 FE 91 D5 22 E9 | BB 7D 28 78 5A 32 D1 A3 05 D8 92 F2 8A DA DB 99 87 AD AF 0A 45 CB 54 49 2F 03 67 08 CF 3F 55 F9 |
| SHA-384 | C7 4D 6C 2F 17 D3 90 87 03 E4 34 1F 8C 03 A4 70 78 F0 09 48 4E A2 FD 4F 6F 77 B3 9A E0 99 67 4F AF DD 63 2B E0 DB 52 C4 E8 28 8E 3B 5B 79 EF A1 | 1F 06 6A 3A 10 CB 7B 38 B0 50 E1 EC 3A 78 56 92 FA 9D D8 D4 4A 8D D0 78 67 D1 3C 71 EB 7E 1D B7 DA BD 01 06 38 56 B9 9C D2 87 6F F1 E0 A4 38 DD |
| SHA-512 | D1 DD D1 AA 4A 0D 19 59 B1 49 B3 AF 0A 3E C8 45 9F B7 83 A6 2C 77 98 72 3B F7 E4 4B 9C BC 60 7C C5 2E CA F4 A1 CA D8 40 59 D2 5B 0F 4F 7B DC DA 10 62 C2 8E 7F 7D F9 70 67 18 D0 A7 7C 25 67 AF | 85 6B B6 52 93 2F C6 EA 33 8E EB 8F 41 1A 20 33 33 86 5E 10 9B 96 7B 00 D5 EB 04 82 E5 90 97 F9 EA 5D A4 90 9C 51 9F 73 FC E9 0A DB D7 56 DE F4 9E 4F DA 95 E9 C8 8F A9 DB 80 B6 EF E7 4A 50 09 |
| SHA3-256 | BB A5 77 A9 5B E9 A5 B9 6E 64 4E 3F 0C 03 03 C4 12 F4 46 4F D0 EA E8 9E B6 76 19 05 D2 89 77 61 | D7 22 33 16 11 E7 52 78 C3 14 6F 4D 74 C3 7F 00 F7 6A 88 21 AC FE 4E A5 70 12 46 B8 D5 F1 4F F3 |
| SHA3-384 | A8 4F 19 2E 2D 91 03 E0 EA 3E 3C 8F 2E 73 7C 11 6D DE 66 C6 EE D5 E2 19 BF B0 25 F7 23 D2 67 36 E8 F0 D3 64 91 E8 66 DE CE CC C1 B6 E9 00 DE 86 | DB 57 74 79 7C 19 99 AA 7E FA 4E 9B 97 75 E3 5B 16 F2 17 EB 20 9C 36 7E EC 25 85 97 40 0D 42 B4 3D F9 00 7E E8 98 CA BC 89 03 E4 B1 CC 49 B6 E5 |
| SHA3-512 | 08 0E F8 97 C3 09 F9 39 D4 0B 36 87 62 07 3A 45 58 F3 43 A7 66 38 18 F9 55 BA 7A 5E A1 3A 2F E6 48 A1 F3 CA 7C B7 ED C8 E9 A4 2C 22 A7 27 38 93 D2 38 79 61 D3 FE 4B 4F EA 59 7C EA C0 27 5B 0B | 36 3A D0 0F D2 2A A9 B3 03 18 7C EF 20 43 EB 40 96 D0 DF 1C C7 DD 69 D2 63 BB E5 8C DC F1 2E A1 32 3D 41 7D 39 03 E9 A3 02 9E 24 41 02 4B 79 82 3F 04 E3 34 F9 C5 B0 E6 9A 61 ED 2D 0E F2 F8 9B |

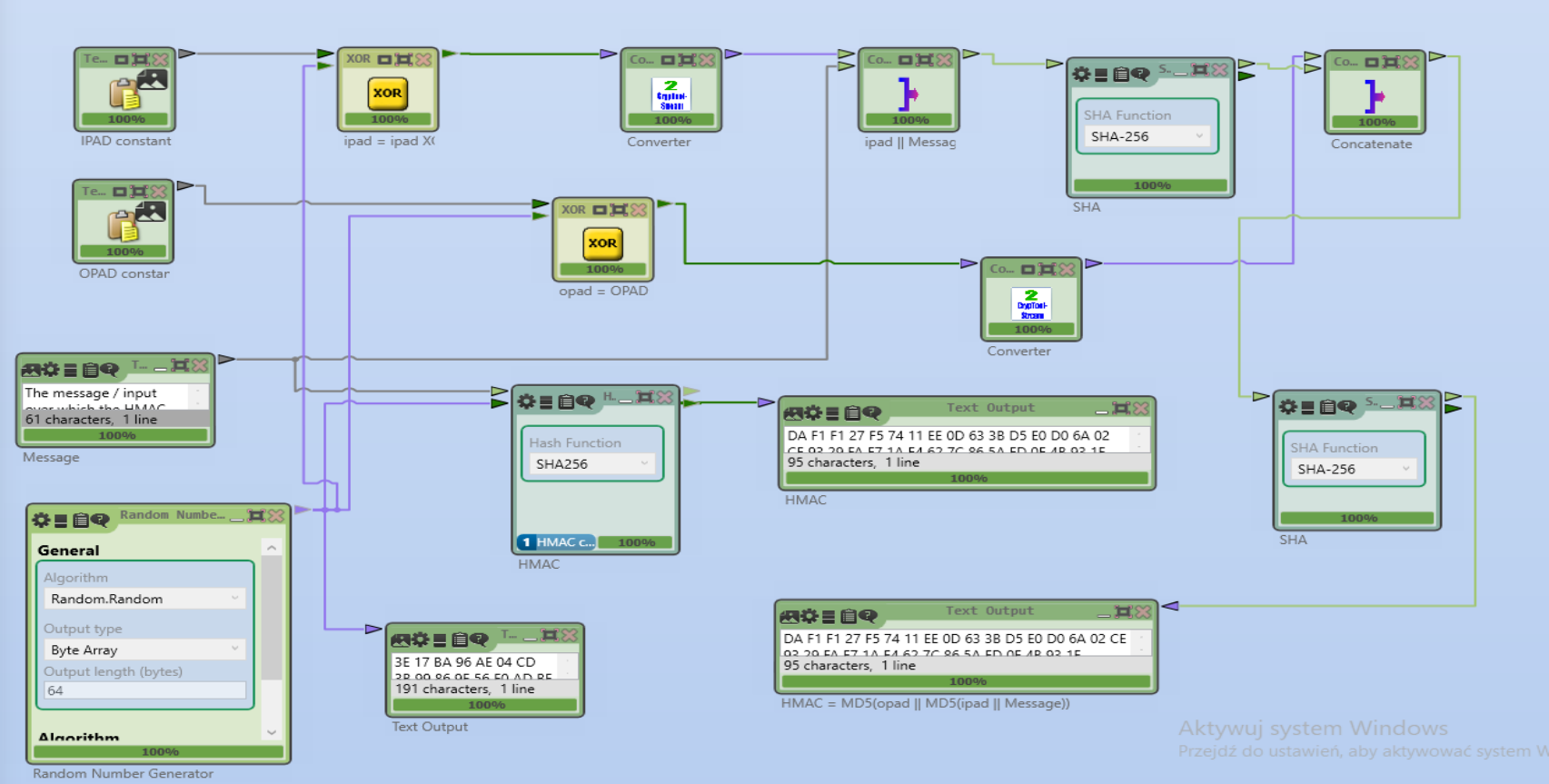
1. Ataki na funkcje skrótu
2. Korzystając z szablonów „MD5 Collision Finder” i „SHA-1 Collision” wyznaczyć dla funkcji skrótu MD5 i SHA-1 pary różnych wiadomości, które mają jednakowe skróty. W opracowanym modelu, korzystając z bloku porównywania pokazać, że wiadomości są różne, a skróty jednakowe.



|  |  |
| --- | --- |
| Wartość 1 (base64) | MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3OA0KISEgUFJFRklYICEhDQowMTIzNDU2Nzg5MDEyMzQ1Njc4OXndqaMouW1SzBB7aCma7HqKIWABTbtN+PgJgoGOE7svcxj58PIs2orrI/LConMwRQ0rtK8R5DVWIvkogl3seRoOnFor3604ReC3CSFB35Ihx3D7gjYNoUuEFcRHXwztwRkuyQp1zqPf7aDrsIgG3SQH4Xgjt5/0Ojkfyeh5AP0dISEgU1VGRklYICEhDQpUYWpuYSB3aWFkb21vxZvEhyBBcmthZGl1c3ogT3N0cnp5xbxlaw== |
| Wartość 2 (base64) | MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3OA0KISEgUFJFRklYICEhDQowMTIzNDU2Nzg5MDEyMzQ1Njc4OXndqaMouW1SzBB7aCma7HqKIWCBTbtN+PgJgoGOE7svcxj58PIs2orrI/LCovMwRQ0rtK8R5DVWIvkoAl3seRoOnFor3604ReC3CSFB35Ihx3D7AjYNoUuEFcRHXwztwRkuyQp1zqPf7aDrsIiG3CQH4Xgjt5/0OjkfyWh5AP0dISEgU1VGRklYICEhDQpUYWpuYSB3aWFkb21vxZvEhyBBcmthZGl1c3ogT3N0cnp5xbxlaw== |
| hash | B8 19 F8 CE 95 78 8A 83 7E EE 0A 9E D8 55 D2 FE |

1. 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. Opisać krótko zastosowaną metodę oraz podać liczbę wykonanych prób do znalezienia tego przeciwobrazu.
2. 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. Opisać krótko zastosowaną metodę oraz podać liczbę wykonanych skrótów do znalezienia tej kolizji.
3. Funkcja HMAC

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. Porównaj otrzymany wynik z wynikiem działania wbudowanego bloku HMAC.



|  |  |
| --- | --- |
| Wiadomość | Arkadiusz Ostrzyzek |
| Seed | 3E 17 BA 96 AE 04 CD 3B 99 86 9E 56 F0 AD BF 3A 6F B7 4D 25 55 17 5D CC 6E 8B 09 14 57 9A B0 36 CF D6 28 0B B3 C7 07 DB AE F2 70 DC 95 05 09 6E 67 6B E7 F1 0D 46 D8 27 BA ED 27 22 FB B9 E4 FE |
| Szyfrogram | 9A 16 96 56 B3 B7 0F 78 B1 D3 8B 0D CE 30 7E 64 B4 23 CD EE 19 77 3B 66 D8 1D DB FA 32 EB 0D 71 |

1. **Wyniki**

W celu zaliczenia zagadnienia nr 5 należy oddać:

1. Pliki projektowe wykonane w CryptTool dla każdego punktu.
2. Sprawozdanie z opisem działania każdego opracowanego modelu wraz z zrzutami ekranu wykonanych modeli.
3. Dla każdej operacji szyfrowania hybrydowego w sprawozdaniu należy umieścić: wiadomość, klucz AES, klucz publiczny i prywatny RSA i uzyskany szyfrogram wiadomości i szyfrogram klucza.
4. Dla funkcji skrótu MD5 i SHA-1 w sprawozdaniu należy umieścić: różne wiadomości dające te same skróty i ich skróty.