**Sprawozdanie nr 4**

**z przedmiotu Wybrane Elementy Kryptologii**

1. **Zagadnienie**

Kryptosystemy klucza publicznego.

1. **Cel**

Zajęcia laboratoryjne realizowane z wykorzystaniem programu CryptTool 2.1 mające na celu zapoznanie się z algorytmami asymetrycznymi, w tym z protokołem Diffie-Hellmana, algorytmami RSA i ElGamala, oraz bezpieczeństwem tych algorytmów.

1. **Zadania do realizacji w sprawozdaniu**
2. Protokół uzgadniania klucza Diffie-Hellmana

Protokół uzgadniania klucza Diffie-Hellmana służy do stworzenia klucza do szyfrowania wiadomości poprzez kanały publiczne. Jest on możliwy dzięki istniejącemu problemowi z rozwiązywaniem logarytmu dyskretnego. Operacja generowania klucza przez uczestników protokołu jest bardzo prosta, jednak praktycznie niemożliwa dla atakującego.

1. Korzystając z bloku Number Operation opracuj model realizujący potęgowanie modularne tj. obliczanie wartości X = gx mod p. Następnie korzystając z wartości p i g podanych w załączonym pliku oraz używając jako tajnej wartości x losowej liczby (<p) uzyskanej przy pomocy bloku „Random Number Generator” oblicz X = gx mod p. Uzyskaną wartość X przekaż kanałem jawnym (np. chat MSTeams) wybranej osobie z grupy, a uzyskaną od niej wartość oznacz przez Y. Korzystając ponownie z modelu realizującego potęgowanie oblicz k = Yx mod p. Potwierdź, że osoba, z którą wymieniałeś(aś) wartości X i Y uzyskała ten sam klucz k. W sprawozdaniu zamieść poprawnie opisane wszystkie wartości: p, g, x, X, Y i k.

P= 183333237870103747764160111956844034494632155429934262557252640441894316978700303556505764211,

g=28866939382179745657940698838054353433319336592503252131637024636761218014958897320844331561 ,

x = 130 ,

X=55315630105706625395554022640741439566399947138115030828158750255360971668305954869429534234 ,

Y=170612559486660163429698510416970072327357385514458088913052520045106567490231951257274298936 ,

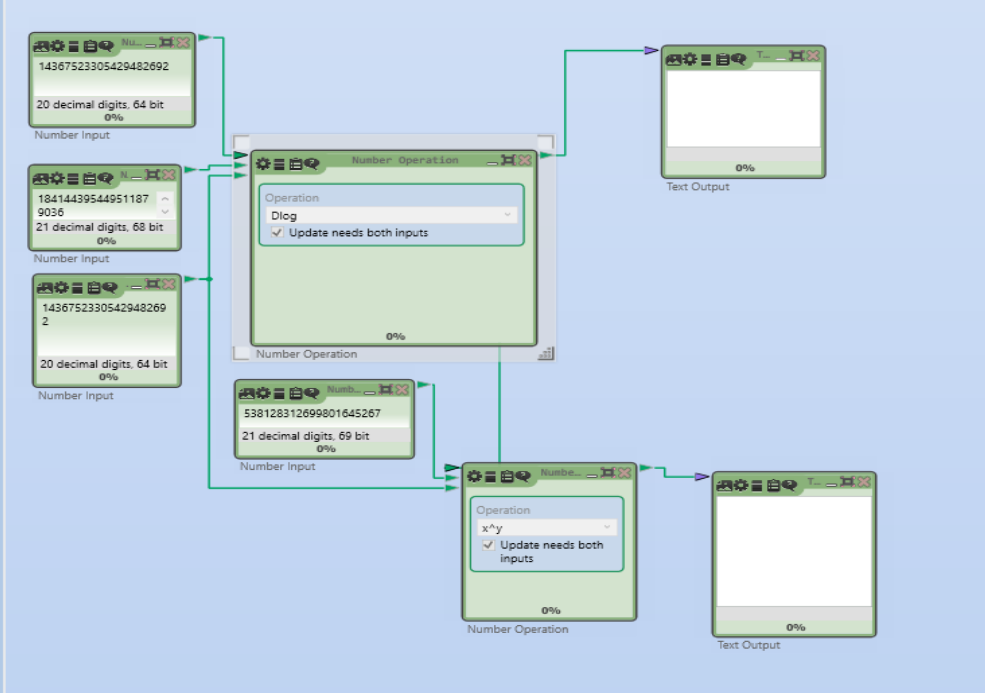
K=121921922448804896175145215825888028432990320938720980864690364590837411513746193148200489901

Obraz zawierający tekst, zrzut ekranu, wyświetlacz, oprogramowanie

Opis wygenerowany automatycznie

Dla danych, zamieszczonych w załączonym do tego zadania pliku, w wierszu odpowiadającym Twojemu numerowi w grupie, korzystając z bloku Number Operation i opcji Dlog wyznacz logarytm dyskretny y = loggY mod p, lub x = loggX mod p i korzystając z tej wartości oblicz wartość k. W przypadku niezadziałania bloku z CryptToola można skorzystać z dostępnych kalkulatorów logarytmu dyskretnego np. strony <https://www.alpertron.com.ar/DILOG.HTM>. Po wyznaczeniu wszystkich wymaganych liczb uzupełnij tabelkę i zamieść ją w sprawozdaniu.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Lp. | p | g | X | Y | Liczba bitów p | x | Klucz k | Czas |
|  | 31102984926527497 | 8915266408258324 | 30946922395485779 | 5049866264231746 | 17 | |  |  | | --- | --- | | 9800980098 |  | | 29999483760320267 | 30s |
|  | 14367523305429482692 | 184144395449511879036 | 14367523305429482692 | 538128312699801645267 | 20 | |  |  | | --- | --- | | 315000000000000 |  | | |  |  | | --- | --- | | 430475964547675191907 |  | | 33s |
|  | |  |  | | --- | --- | | 19947276023641381382652313 |  | | 19663953101072256969945805 | 4324062317819647420365365 | 11495770378149844109080195 | 85 | 72072072072072072 | 16197308466814305945279882 | 17 min |



1. Kryptosystem klucza publicznego RSA

RSA to taki sposób na ukrywanie informacji. Można wygenerować dwa klucze - jeden, który jest publiczny, a drugi, który jest tajny. Pierwszy klucz używany jest do zaszyfrowania wiadomości, a drugi, żeby ją odszyfrować. Głównie opiera się to na trudności w rozkładaniu dużych liczb na czynniki pierwsze.

1. Korzystając z bloku Prime Generator opracuj model realizujący generowanie kluczy prywatnego i publicznego dla kryptosystemu RSA zgodnie z jego schematem. Następnie, korzystając z bloku RSA lub bloku potęgowania modularnego (jak w zadaniu 1a) do modelu generowania kluczy dołącz elementy pozwalające na szyfrowanie i deszyfrowanie dowolnego tekstu jawnego. Przy pomocy opracowanego modelu wygeneruj klucz publiczny i prywatny o długości co najmniej 1024 bitów. Odpowiednimi kluczami, najpierw zaszyfruj, a następnie odszyfruj swoje imię i nazwisko. W sprawozdaniu zamieść poprawnie opisane wszystkie wartości: p, q, n, , e, d oraz tekst jawny i jego szyfrogram.

Obraz zawierający tekst, zrzut ekranu, diagram, Plan

Opis wygenerowany automatycznie

P = 52411818354499935842632734716080601889549467449959861248053971759238942724912517662623209589462582680684196254191766015077711093547748479498053736571514560357

Q = 32532549164697819527517207729395154679094670844423722625319267188768389588753974810491502704970292035828073621225451501509988437448796418747435551548564996801

N = 1705090057428980733755750070462500287743225572088660525578932256858208059338828966684479162810449957934900495758396418766137598835837099402272061156679619809945746083369135903265184226780899074144775827297379583552939591713697562528565220979680283677252561598827599318949183542482781950607699639036033216962626417957

Phi = 1705090057428980733755750070462500287743225572088660525578932256858208059338828966684479162810449957934900495758396418766137598835837099402272061156679619809860801715849938147895034284335423317576131689002995999679566352765690230214898728506565571382819686882315329443531966025895082419611154740790543928842546860800

E = 44727133305292621147716771108105224228025920920055666455179655688979352704442607923873801208414344907852154172490156471132195392820757136224513122707046732741

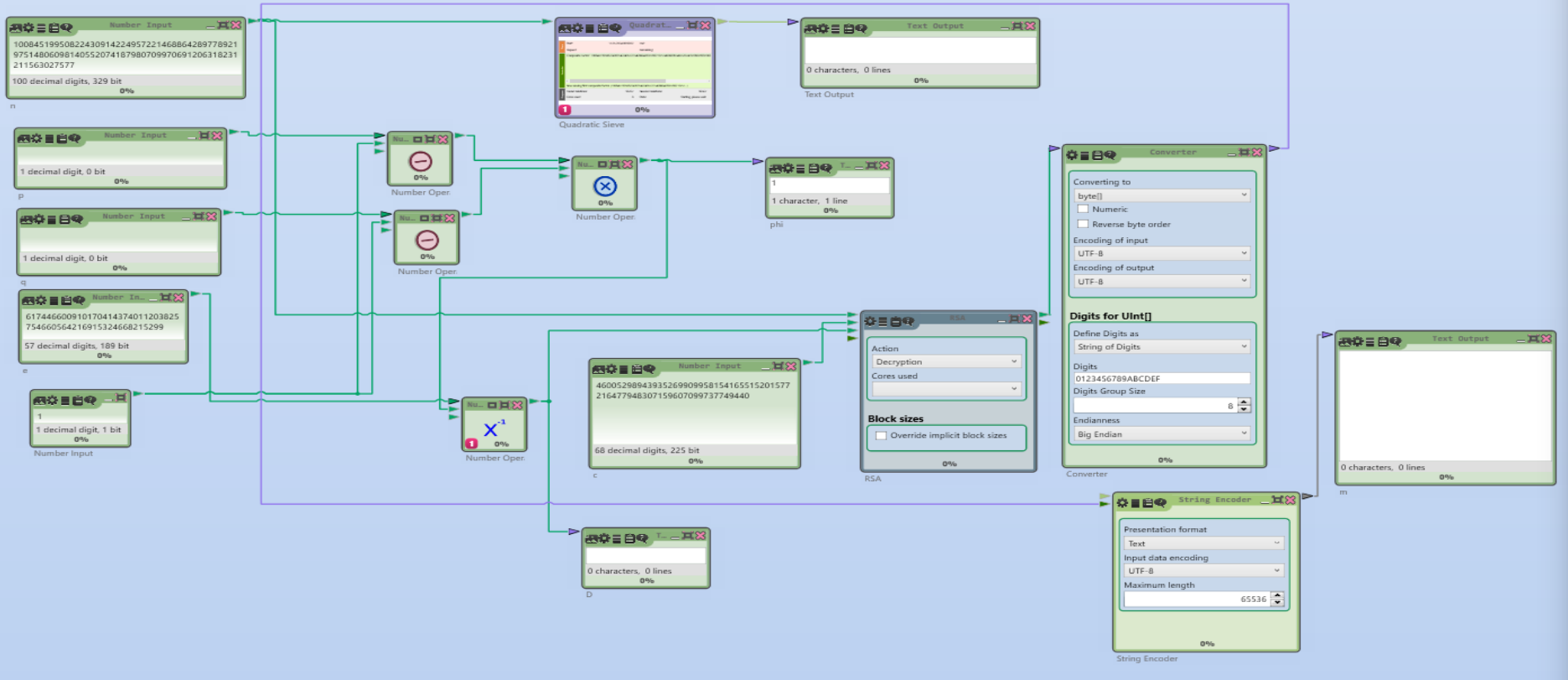
D = 569902489602966579620981295500493911933900060707763201553809462473987296573079945193707697894894672614449576818470524376432360712785259315277316264954098884497351508028116778479834886867404516290957427858525376403324884158850164114918977130413753038369910863310197979313655148824314217870467632324131393557698075661

Szyfrogram: C6 E0 40 12 53 BF 40 A3 A5 96 17 75 91 EE 2F 3D 55 F9 84 0C 95 71 0F 49 98 53 F6 24 7D 0B F3 E3 BB F9 89 3C D7 D9 E4 1C 3A B4 9F 76 9D CF E0 01 28 82 1D 58 AE 56 81 8F AB 66 A6 79 E9 35 3D 63 2B B2 62 65 FE 5C C8 25 BF EA 3A E5 9F EB 50 A5 5A 69 F0 CB 3B 8B 92 88 BC C6 88 7F 88 6B 94 DA DE D1 5B 5C 1B CD EE CC E8 73 54 C1 6E 5F C9 58 F9 AD 0C AA A6 8B 16 8D 94 F0 CC 0B F6 06 F9 B7 E6 68 83

Tekst jawny: Arkadiusz Ostrzyżek

1. Dla danych, zamieszczonych w załączonym do tego zadania pliku, w wierszu odpowiadającym Twojemu numerowi w grupie, korzystając z bloku Quadratic Sieve wyznacz faktoryzację n i korzystając z niej oblicz wartość klucza tajnego d, a przy jego pomocy odszyfruj szyfrogram c. W przypadku niezadziałania bloku z CryptToola można skorzystać z dostępnych kalkulatorów logarytmu dyskretnego np. strony <https://www.alpertron.com.ar/ECM.HTM>. Po wyznaczeniu wszystkich wymaganych wartości uzupełnij tabelkę i zamieść ją w sprawozdaniu.

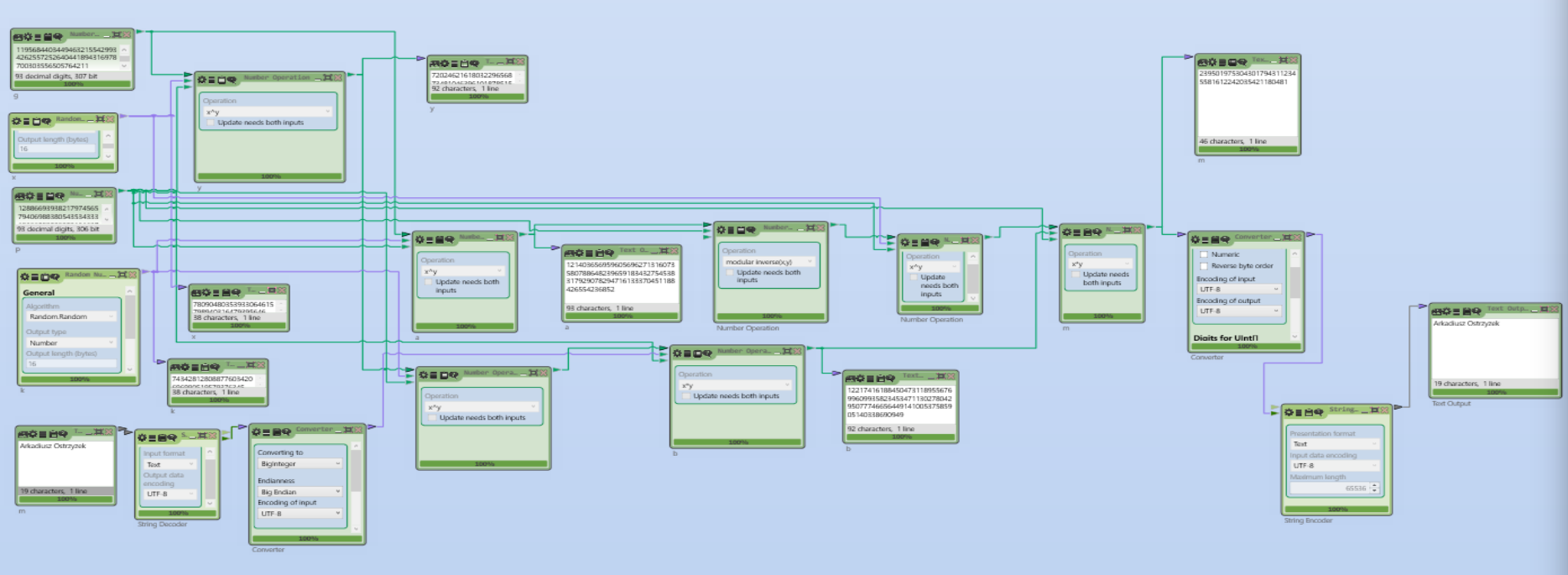
|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Lp. | n | e | c | Liczba bitów n | p | q |  | d | m | czas |
|  | 91077743101110258039520299192229328623305865941505089377755386086987 | 384347559558273626629478597152503884843138337042713280515 | 710312730877634821481699439680139578087877844310182036783632978964 | 226 | 3312166410232582084941196289900723 | 27497936945358591005452303870197769 | 91077743101110258039520299192229297813202510350331998984255225988496 | 40727769635612595664172590066206804192034802955533116576385631990251 | Potęgowanie modularne. | 10 s |
|  | 1109776977686922376875653584001858753798338438399039793426898363169992536657219330269 | 176698942093539901710740879717680562466300395533951234735068782681653249 | 636586070592084832858344978431805566676694124014374287666325436457845328121523042412 | 280 | 897404225785106021796224293362891229233263 | 1236652275306614729459768427916736795246963 | 1109776977686922376875653584001858753798336304342538701706147107177271257029194850044 | 1042000716348042242179981596332943298055483089948177149799858782243956301320506930509 | Twierdzenie Fermata. | 55 s |
|  | 1008451995082243091422495722146886428977892197514806098140552074187980709970691206318231211563027577 | 933062520171307872281375991446871123927837694593846322869869103901868651560666440663041 | 919503437740832071679133104385009149362604980730959799142276537631366421044922134542808196511906530 | 329 | Found 0 factos. | Found 0 factos. | - | - | - | 25 min |



1. Kryptosystem klucza publicznego ElGamala

ElGamal tak jak RSA jest asymetryczny. Można go wykorzystać do szyfrowania i podpisywania danych. W przypadku szyfrowania, nadawca losowo wybiera pewną wartość, a następnie oblicza na jej podstawie wiadomość oraz wartość zwanych kluczem publicznym. Tak samo jak w Diffie-Hellmanie trudność dla atakującego polega na rozwiązaniu logarytmu dyskretnego.

1. Korzystając z danych (p i g) i modelu z zadania 1a opracuj model realizujący generowanie kluczy prywatnego i publicznego dla kryptosystemu ElGamala zgodnie z jego schematem. Następnie, korzystając z bloków Number Operation do modelu generowania kluczy dołącz elementy pozwalające na szyfrowanie i deszyfrowanie dowolnego tekstu jawnego. Przy pomocy opracowanego modelu wygeneruj klucz publiczny i prywatny. Odpowiednimi kluczami, najpierw zaszyfruj, a następnie odszyfruj swoje imię i nazwisko. W sprawozdaniu zamieść poprawnie opisane wszystkie wartości: p, g, x, y, k oraz tekst jawny (m) i jego szyfrogram (a, b). Operacje szyfrowania i deszyfrowania powtórz dla dwóch różnych wartości parametru k.



Szyfrogram = 2395019753043017943112345581612242035421180481

Tekst jawny = Arkadiusz Ostrzyżek

p = 183333237870103747764160111956844034494632155429934262557252640441894316978700303556505764211

g = 128866939382179745657940698838054353433319336592503252131637024636761218014958897320844331561

x = 78090480353933064615798940316479395646

y = 72024621618032296568734810463961018785151019029074939639197758457372851659562670215838354252

k = 74342812808877603420696990519579376345

1. Dla danych, zamieszczonych w załączonym do tego zadania pliku, w wierszu odpowiadającym Twojemu numerowi w grupie, korzystając z bloku Number Operation i opcji Dlog wyznacz logarytm dyskretny x = loggy mod p i przy jego pomocy odszyfruj szyfrogram c = (a,b). W przypadku niezadziałania bloku z CryptToola można skorzystać z dostępnych kalkulatorów logarytmu dyskretnego np. strony <https://www.alpertron.com.ar/DILOG.HTM>. Po wyznaczeniu wszystkich wymaganych wartości uzupełnij tabelkę i zamieść ją w sprawozdaniu.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Lp. | p | g | y | a | b | Liczba bitów p | x | m | czas |
|  | 27333716067421196469772662866003 | 6637276400806347536187596301933 | 6637276400806347536187596301933 | 15227664096228362909542904372691 | 27333716067421196469772662866003 | 105 | 440044004400440 | Asymetria | 35s |
|  | 13202041157530128899789145217407830011540406299 | 12371929723632740263519053052556783755093750501 | 11465342676995288000484220586091700433375058134 | 6818296524580249352377035142578720462063150194 | 190244149895040260128864191302355077127806001 | 154 | 41400000000000414 | Logarytm dyskretny. | 10min 47 sek |
|  | 16822632650836304447079915654196545995154312591163612494561619 | 2475193217267708170827775297979858946669315493682288916910797 | 7328976643485654636996009177978756048124024371625106522496011 | 10210296879290389856004574275877338547950605807569351740802756 | 13288929401865124603292995446749531694975534390515876965015601 | 204 | 73073073073073073 | Liczba bitów p. | 21 min 02 sek |