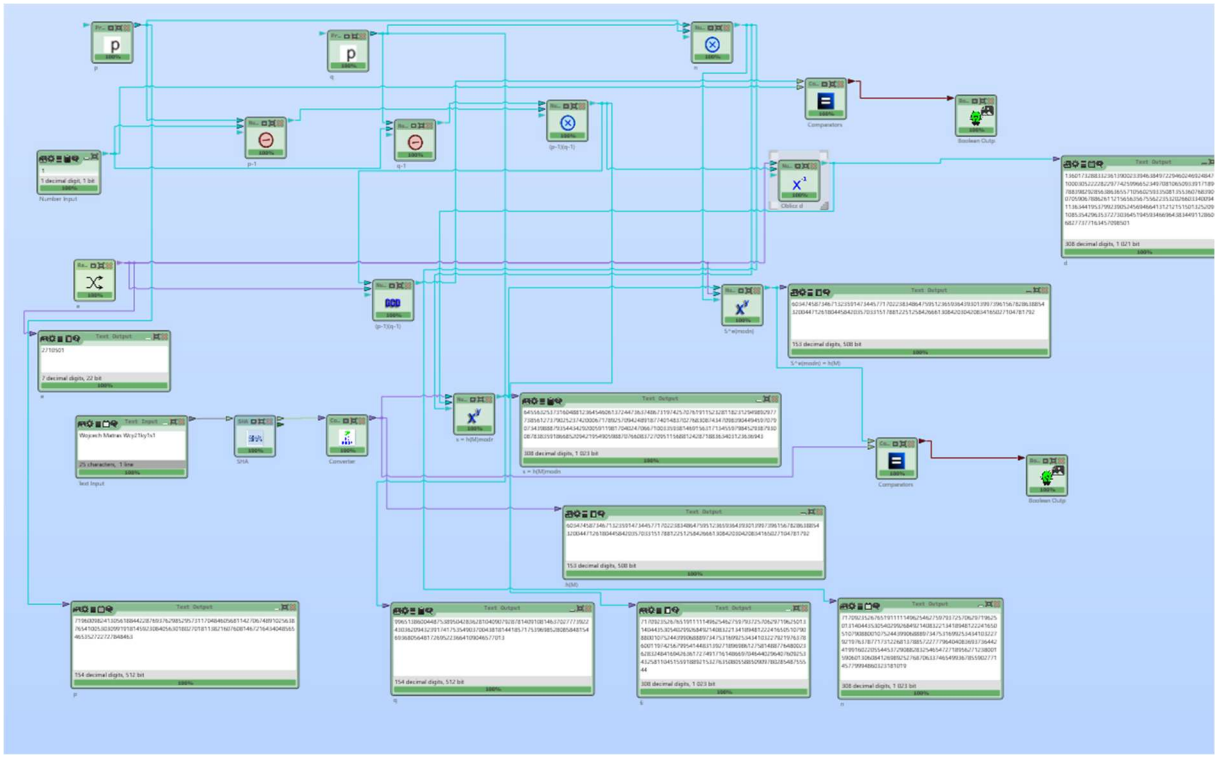
Podpis cyfrowy: schemat RSA

a)

Korzystając z modeli utworzonych na poprzednich laboratoriach opracuj model realizujący generowanie i weryfikację podpisu cyfrowego schematem RSA. Przy pomocy opracowanego modelu wygeneruj klucz publiczny i prywatny o długości co najmniej 1024 bitów i korzystając z jednej z tych dwóch funkcji skrótu (SHA-2 albo SHA-3) wyznacz podpis dokumentu złożonego z własnego imienia i nazwiska (i ewentualnie dodatkowych danych). Następnie zweryfikuj uzyskany podpis. W sprawozdaniu zamieść poprawnie opisane wszystkie wartości: p, q, n, φ, e, d oraz podpisywany dokument, jego skrót oraz wygenerowany podpis.



Wykorzystana funkcja skrótu SHA512

p

8136286979543742250487788860985322679474934320726793242355575759018325252371709424924951035147325384626043797582639075285518754578879732441871666114486909

q

1130587480837162668872164024754656881398056062112364020488798489258687821689647719808049058495181015126947264563289363303457204711115038754471527549889339165226334983694788183557217012316378253418504545757948563377982449521108430635615325277172915868010697980587963806747362063142767014511143256118419

fi

9198784199570566823253195462873928792803903140999815412751660957540334658770100174407002914104825749903709579574162571744344765294025036156021177878209578950283691

7731096604448535907502532551886088331156807109851438791177277898025292180763017370517803737997249425476505525548665656037311264702792420164273812 0

d

4520021513806560733548233062620029762765390551095525828504100339319643511353492743261610330201087015792632742454088789282170549749787529648556329844400882023406901198648743265853498027745150539573466597433302031906710317145832083744352356281082233411543448024749832332938201045622444273038976815001975797533 1

e 11162411

M WOJCIECH MATRAS

h(M)

8244718752170530053449598137479276640223102261704665866003995373789403534514747881760449311222775561076339853435778794313762318147860737923682711384286735

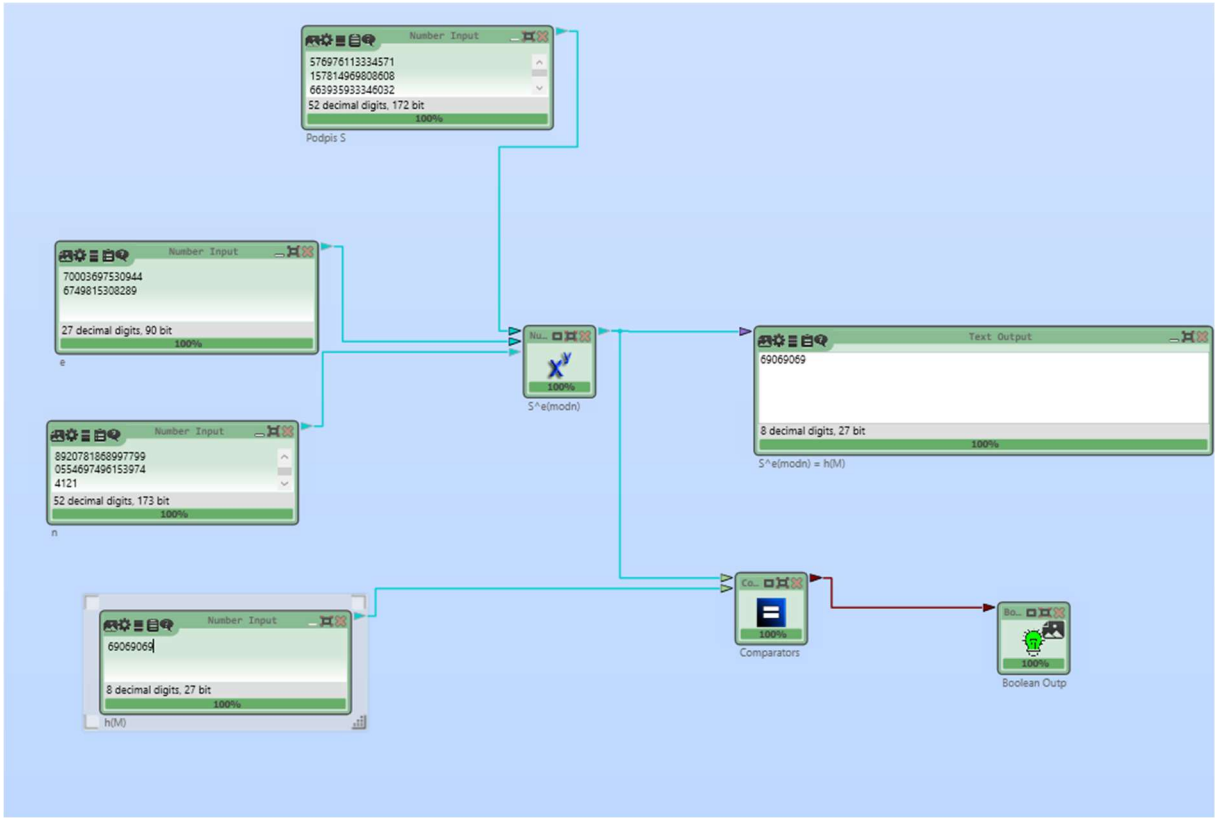
Podpis S

6213990719078196743623462691408565506149579264389821918954309979048538824984633871505540780458513963889442274363528970975838247674820841757225983059186325295814152999444920871219180819974817479506441649485280718749573847496136696875172631486007834383142213254621725383633838746661653808306878469448774871507 9

b)

Dla danych, zamieszczonych w załączonym do tego zadania pliku, w wierszu odpowiadającym Twojemu numerowi w grupie, korzystając z opracowanego modelu, zweryfikuj podany podpis. W przypadku negatywnej weryfikacji podaj jej przyczynę. Po wyznaczeniu wszystkich wymaganych wartości uzupełnij tabelkę i zamieść ją w sprawozdaniu.

Lp.	n	e	h(M)	Podpis s	Ważność podpisu	Przyczyna
1	7151481937393920892078186899779905546974961539744121	700036975309446749815308289	69069069	576976113334571157814969808608663935933346032 3613337	Tak	
2	7151481937393920892078186899779905546974961539744121	700036975309446749815308289	69069069	410424381304	Nie	Zmiana skrótu dokumentu co jest równoważne do zmiany dokumentu
3	7151481937393920892078186899779905546974961539744121	700036975309446749815308289	69069069	887974857856	Nie	Zmiana skrótu dokumentu co jest równoważne do zmiany dokumentu



2. Podpis cyfrowy: schemat ElGamala

a) Korzystając z modeli i danych (p i g) utworzonych na poprzednich laboratoriach opracuj model realizujący generowanie i weryfikację podpisu cyfrowego schematem ElGamala. Przy pomocy opracowanego modelu wygeneruj klucz publiczny i prywatny i korzystając z jednej z dwóch funkcji skrótu (SHA-2 albo SHA-3) wyznacz podpis dokumentu złożonego z własnego imienia i nazwiska (i ewentualnie dodatkowych danych). Następnie zweryfikuj uzyskany podpis. Generowanie i weryfikację powtórz dla dwóch różnych wartości parametru k. W sprawozdaniu zamieść poprawnie opisane wszystkie wartości: p, g, x, y, k oraz podpisywany dokument, jego skrót oraz wygenerowany podpis.

Dla danych, zamieszczonych w załączonym do tego zadania pliku, w wierszu odpowiadającym Twojemu numerowi w grupie, korzystając z opracowanego modelu, zweryfikuj podany podpis.

P=

15121816644627668485835080296061347325302451444890241374015809917265046397910386152892310761744039732689080821184952728559299172943161874362097258048023733712523281615318270523693653876415845979525064033500540811316261010507971436972201979818021862966144507623912676346473936620872372288071481984631207179938 7

g=

441969021554875835032634278110172450639279958887491647078608996841220945660910346
000565705094256925263287832239619316814713334951936775851896291868562010649425185
148626649563034595466496506486886494011146859580270858579400955969053712940833 6

X=

211621602405102374045191475074828580535071480177355037845627183050481287548646694
375118812412383743339033716708394452131855078761704868895692395705585958510235583
262734246476530118806001285431579308974767604312054724514228577789998442486297 4

Y=

542863045265592632778474938399117008696862435720043761068728074470464132583264233
470574999714145898430814433027693919177557458171641423120460428127613109001081863
050373913484115205793211976130017738785558277275616810385923740520809360218921420
859119274769156908638892843240794322613430854629328904602538911 44

K1=

528429704200046579833496782122698987680053055302338886723530904285725406889134012
731106981168713681565170683424192736408237330675786492720261672988498234869958656
188278250046837377218822936029108624712524091315360634577560612295320856031413 7

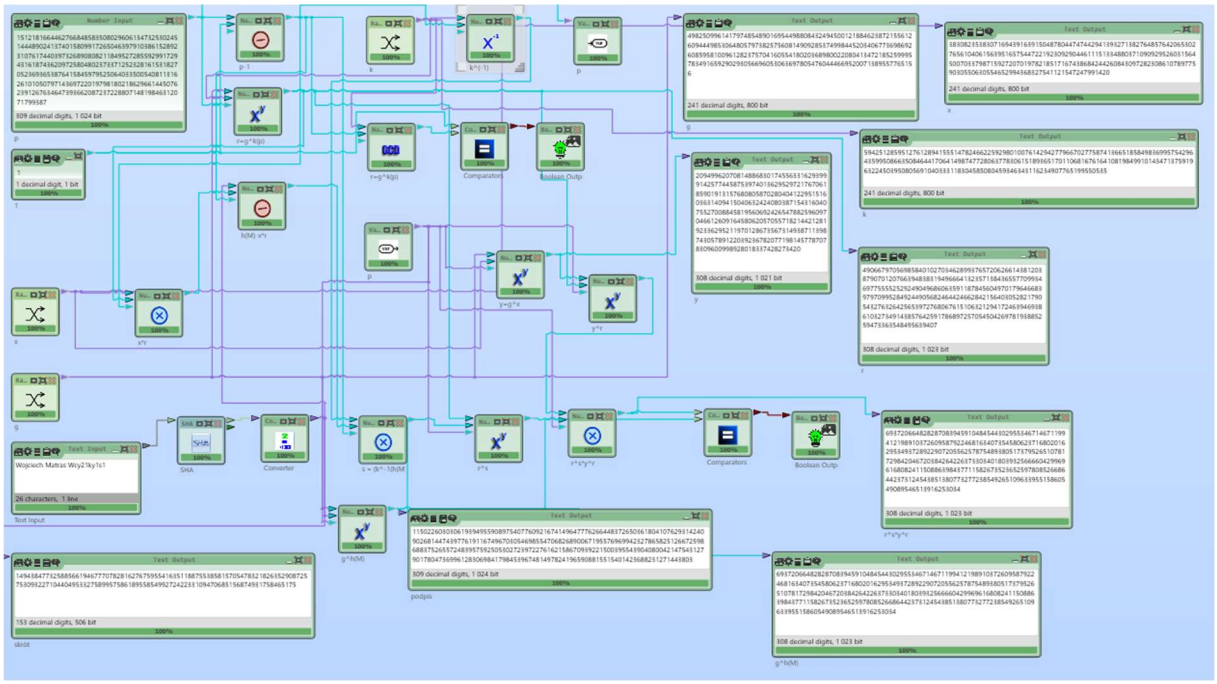
Wiadomość

== Wojciech Matraś Wcy21ky1s1

Skrót=
149438477325885661946777078281627675955416351188755385815705478321826352908725753
093227104404953327589957586189558549927242233109470685156874931758465175

Podpis1=
125574165476919946036438110398010997362472221028585198865936471392665378704781822
006609779688229868591171383470548017630932841967395748639108393383889332944169175
452071221329609195021836520235455895900167411677923808176440492334966991435670945

782373329317609674929324406354819760609083382272822982722254431907



K2=

176153224976448670874494913976452849415693078941991395011664317317199895199518943720538558402008609641652811220749490146792980045037794461858961487543863780225324008921622463526467935151283088153080030510542852077037800857862378407670751720 3

Wiadomość

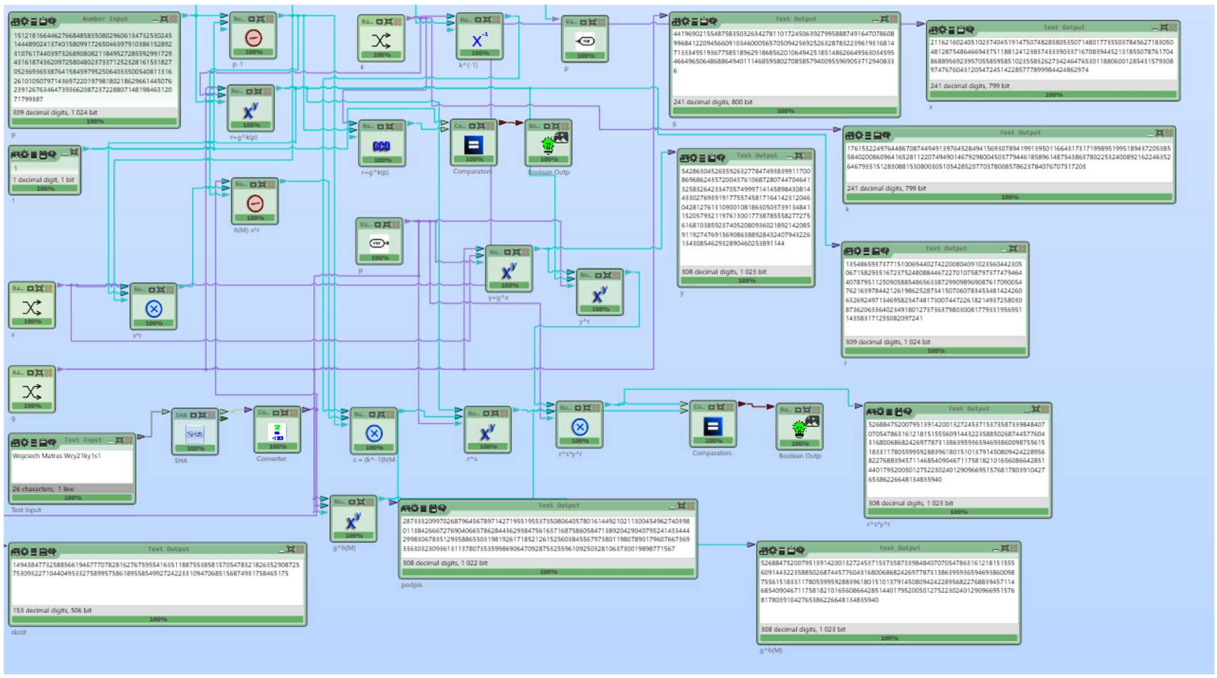
== Wojciech Matraś Wcy21ky1s1

Skrót=

149438477325885661946777078281627675955416351188755385815705478321826352908725753093227104404953327589957586189558549927242233109470685156874931758465175

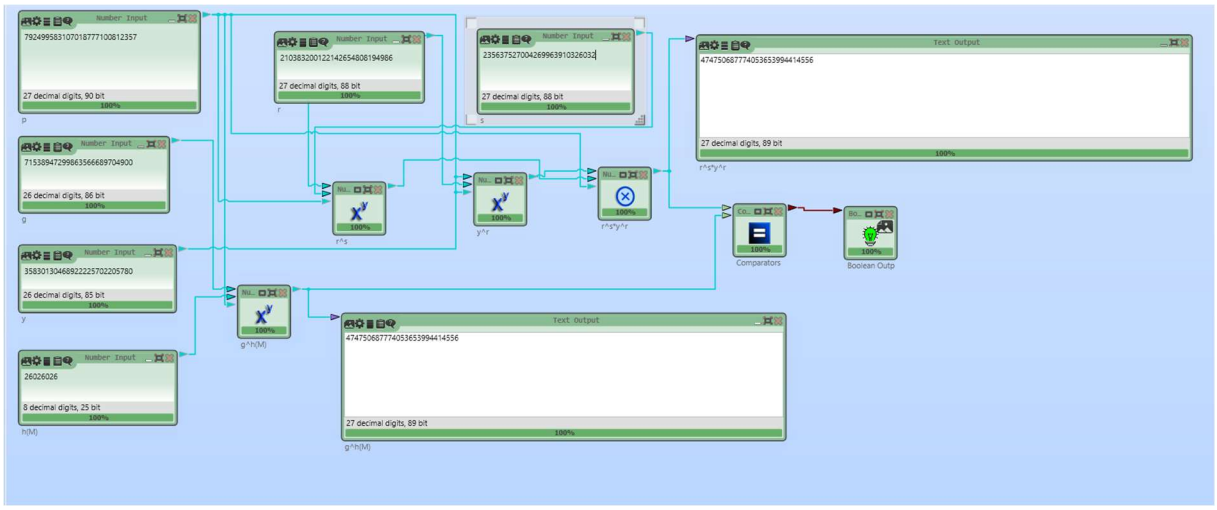
Podpis2=

526884752007951391420013272453715373587339848407070547863161218151555609144322358850268744577604316800686824269778731386395936594693860098755615183311780559959288396180151013791450809424228956822768839457114685409046711758182101656086642851440179520050127522302401290966951576817803910427653862266481348359 40

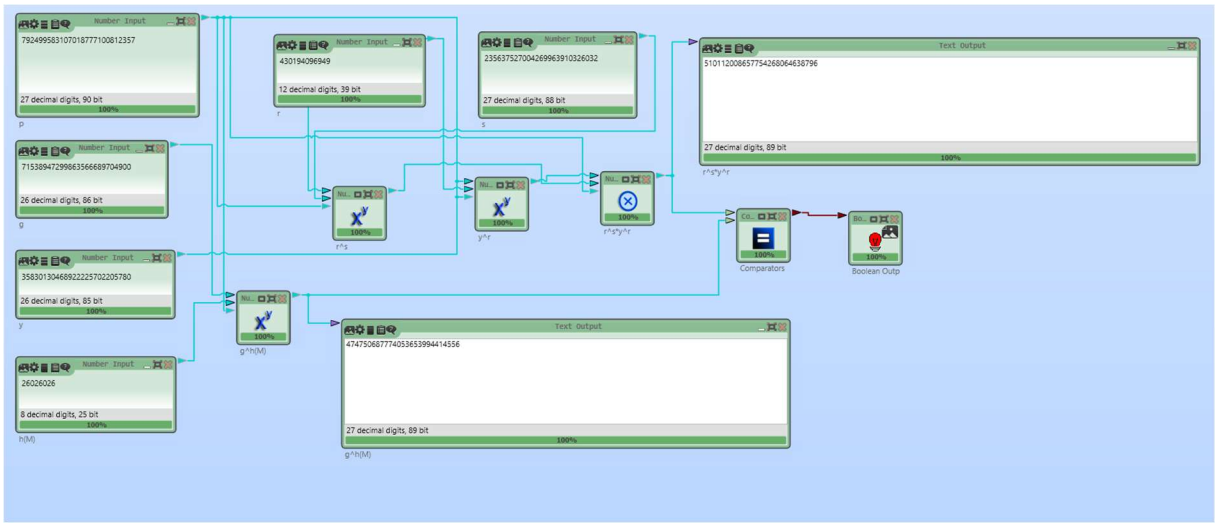


b) Dla danych, zamieszczonych w załączonym do tego zadania pliku, w wierszu odpowiadającym Twojemu numerowi w grupie, korzystając z opracowanego modelu, zweryfikuj podany podpis. W przypadku negatywnej weryfikacji podaj jej przyczynę. Po wyznaczeniu wszystkich wymaganych wartości uzupełnij tabelkę i zamieść ją w sprawozdaniu

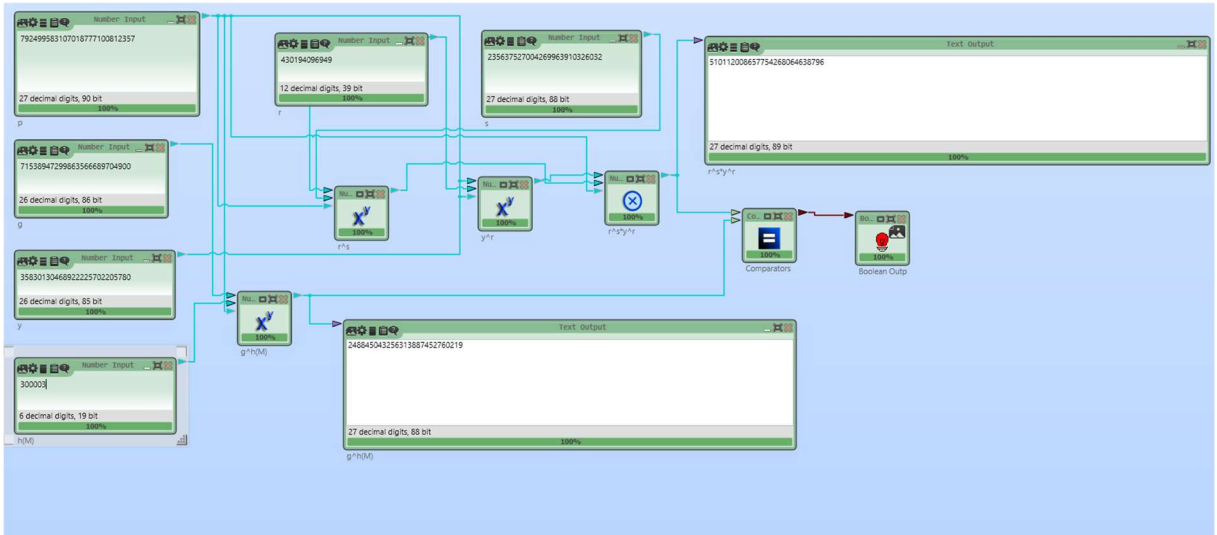
Lp.	P	G	Y	Skrót	Podpis	Ważność	Przyczyna
1	792499583107018777100812357	71538947299863566689704900	35830130468922225702205780	26026026	(210383200122142654808194986, 235637527004269963910326032)	tak	
2	792499583107018777100812357	71538947299863566689704900	35830130468922225702205780	26026026	(430194096949, 235637527004269963910326032)	Nie	s jest zależne od r a się nie zmieniło
3	792499583107018777100812357	71538947299863566689704900	35830130468922225702205780	300003	(430194096949, 235637527004269963910326032)	nie	Skrót podpis nie dają odpowiednego wyniku



2



3



3. Podpis cyfrowy DSA a) Korzystając z poprzednich zadań opracuj model realizujący generowanie i weryfikację podpisu cyfrowego algorytmem DSA. Przy pomocy opracowanego modelu wygeneruj klucz publiczny i prywatny i korzystając z jednej z dwóch funkcji skrótu (SHA-2 albo SHA-3) wyznacz

podpis dokumentu złożonego z własnego imienia i nazwiska (i ewentualnie dodatkowych danych). Następnie zweryfikuj uzyskany podpis. Generowanie i weryfikację powtórz dla dwóch różnych wartości parametru k. W sprawozdaniu zamieść poprawnie opisane wszystkie wartości: p, q, g, x, y, k oraz podpisywany dokument, jego skrót oraz wygenerowany podpis.

p

648774711828981726107308107557041901614493228763008937898347760184704810825074802011699011576276766045412387084971773530572273413606347785452018451242283005579584430922489771460294177870481763873783400287004769151159825328252087850143232741484798279972982570313455741 3

q

91007390642367661832076559092667555491152263374307136308730628401060853364369

g

383694051461272512216214481278057410354527478946476014650551823537055170476629434030697493423630984519765718967009702163082337748448394918659034514633085821883392466660897966792552842734820440179506104664624584364220184152486528981363454528882740461009017130458698 11

x

601751178268874615155708265911123800584597 7

y

316034936917226848472128806462708126947584534663649843066148910145939652939832675424634278495038128046762650979612535898830608818768554172453434952074164265980394861700161554255104487279453790988358470482499093590475164434930490200938194081695365043980832197622264210 0

Wiadomość

Wojciech Matraś Wcy21ky1s1

U1

173861593646484713379509572819542831166061444228150163841283078035123048596 15

Podpis 1

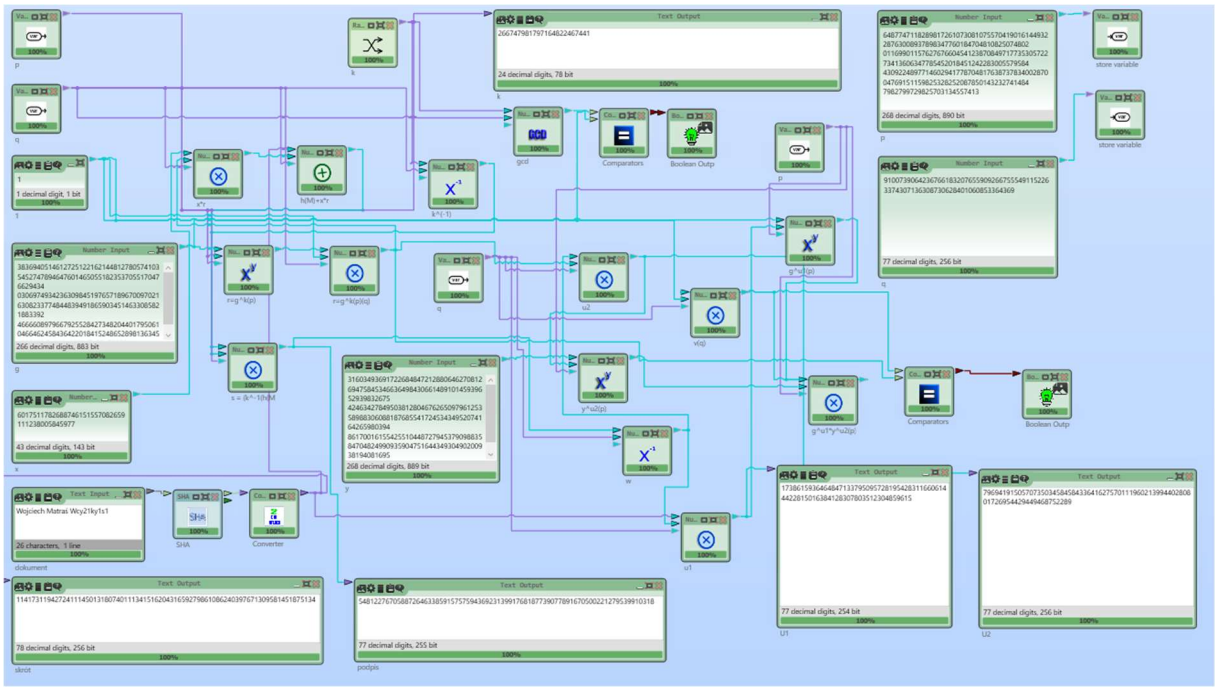
114173119427241114501318074011134151620431659279861086240397671309581451875134

U2

796941915057073503458458433641627570111960213994402808017269544294494687522 89

Podpis 2

548122767058872646338591575759436923139917681877390778916705002212795399103 18


p
k
Text Output
26674798179716822467441
24 decimal digits, 78 bit
Number Input
store variable
q
gcd
Comparators
Boolean Outp
1
1 decimal digit, 1 bit
x*y
h(M)+x*r
k^(-1)
r=g^k(p)
r=g^k(p)(q)
u2
g^u2(p)
v(q)
Number Input
9
266 decimal digits, 883 bit
s = (k^-1)(M
y^u2(p)
g^u1*y^u2(p)
Comparators
Boolean Outp
Number Input
x
43 decimal digits, 143 bit
y
26B decimal digits, 889 bit
w
u1
Text Input
Wojciech Matrai Wcy21ky1s1
26 characters, 1 line
dokument
SHA
Converter
Text Output
U1
77 decimal digits, 254 bit
Text Output
U2
77 decimal digits, 256 bit
Text Output
skrot
78 decimal digits, 256 bit
Text Output
podpis
77 decimal digits, 255 bit