**RVB Algorithm – Known Answer Tests**

1. Algorithm name: RVB Algorithm

2. Test name: Public key exchange

3. Description of test: The two peers „Alice" and „Bob" agree on a mutual secret key by exchanging data over an insecure line. Expected minimum number of decimal digits that match in the shared secret on both sides: 100. Length of mantissa: 1216 bit (approx. 366 decimal digits)


Common parameter:

common x:
0.1234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678


Secret (private) keys:

Bob's secret:

123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890

Alice's secret:

987654321098765432109876543210987654321098765432109876543210987654321098765432109876543210


Public keys:

Bob's public:
0.37401427564600702986654027324975381855316111809961581956364711850416163245580021957358004091694180595276498120036417659606179452294916154970619781278144489070644539729542640884426675215829540161861023774203083854497348381060011678082777701959201647414762682593879328491775020173277816671304741165980860206520653013559512329497408394406162036383537700612371679751234


Alice's public:
-0.18139774594441226931214246408996383492718969831782203782261152953475999507771190741311993825953604297346330746348581003180789211016991705741154345509891674158946624727560906193571150141332253429575827689949298268545050587721068629164761626128360604040790491046575856480305206362570479245089002096589246780669770976669054184798212960688150889324557499460583041530766


Shared secret:
-0.82885051571924963314714846985123829885829304761699293357736498226707801215538129227624158136785118

1

4. Control parameters

Difference between the secret key computed on Alice's and Bob's side:
1.32491260726707472517875181145980363367552344105813327043505074862989828305890 5261921237223365387049039296284887245236340332326464331075934673571696738583112 58451800934955295351126787061514002275683385456409159976474596413338930386110848 43134751784231877203205953794140487471183350008584979796575234817975997754383782 84278201601292224394292331171498792506332079722 3e-168

=> Almost 168 decimal digits match on both sides.

=> Please keep in mind that control parameters never appear in the key negotiation, and are only stated as a proof that both partners share the same secret. The absolute values of control parameters may vary slightly when mathematical libraries other than than the given reference implementation are used.

1. Algorithm name: RVB Algorithm

2. Test name: Public key exchange

3. Description of test: The two peers „Alice" and „Bob" agree on a mutual secret key by exchanging data over an insecure line. Expected minimum number of decimal digits that match in the shared secret on both sides: 200. Length of mantissa: 2176 bit (approx. 655 decimal digits)

Common parameter:

common x:

0.1234567890123456789012345678901234567890123456789012345678901234567890123456789012345678
90123456789012345678901234567890123456789012345678901234567890123456789012345678901234567
8901234567890123456789012345678901234567890123456789012345678

Secret (private) keys:

Bob's secret:

12345678901234567890123456789012345678901234567890123456789012345678901234567890123456789
01234567890123456789012345678901234567890123456789012345678901234567890123456789012345678
90123456789012345678901234567890123456789012345678901234567890

Alice's secret:

98765432109876543210987654321098765432109876543210987654321098765432109876543210987654321
09876543210987654321098765432109876543210987654321098765432109876543210987654321098765432
10987654321098765432109876543210987654321098765432109876543210

Public keys:

Bob's  public:
0.7910003205562099268500100671985365281368515476149584721864447712247020075649555
71598466741242393256726879420311667181142318574540083531101611186092009140895031
82442383870924622736391190618604040971130410218210551469775363359598514654226482
65496250818601557104023140149404991028075684266398708315859715871565194163908977
07929917394828973532385521209661572666805270738110506270491207143512905050460034
08267276645735860299740044208199840351553910703058009846679718167213182995204780
63588222425334730550923244784765884838183797003520177535538404254310758611869586
88990352210151286549325633940956132589435676024279765695269525444984058817543592
19701403796369217

Alice's public:
-0.578962340144241484276752962566194514859469669497055836272175512328928973504685
08219522616157792515062844936080179921197107250892829798378782551655621404614796
34610061791229598833631902271759324380053334106105026200706554502835779250832183
54749224827782212230531404428664584943447182801349223443539701164978599910201010

234278672424040104576787422036207622989891313783846206065920999762057092763367907308698670442447151190034855500845982107735277190126551060804271160325205758637070026482558495336918653443175339217430236377652242351760422450264769568828043879566006778628286319581437376275581419592845738120571756011048002300184026906283164711271550117587745

Shared secret:

0.3149201328083857469002356956645332657130731354094361046640829662130289178165034909248475335845755566684406961945654256273016978253310587689605562432571976798012948034782246810859823544823222896388619

4. Control parameters

Difference between the secret key computed on Alice's and Bob's side:

1.644730362385693708044252088558027811317448875282693527189356799696612304141138377002433795852952319377080073122576171084254611189321277465096457156740383479325686368385927764648227487427580505155727988305673662432776496660733603631662197589453612316888485800660485044409046109374302662077193527292087178770516982863080079830085751307840547236537668786535412340263445293074060116141280239435038303728773037198068220579695705366911648845850344707242753154807894025255640765304208258662204723372666995306945131160936213392396527815420030551085311559576748201617494940072808552172937793540095017164330262472546692881797421314712809630407393605689965688175_2e-257_

=> Almost 257 decimal digits match on both sides.

=> Please keep in mind that control parameters never appear in the key negotiation, and are only stated as a proof that both partners share the same secret. The absolute values of control parameters may vary slightly when mathematical libraries other than than the given reference implementation are used.

1. Algorithm name: RVB Algorithm

2. Test name: Public key exchange

3. Description of test: The two peers „Alice" and „Bob" agree on a mutual secret key by exchanging data over an insecure line. Expected minimum number of decimal digits that match in the shared secret on both sides: 300. Length of mantissa: 3200 bit (approx. 963 decimal digits)

Common parameter:

common x:

0.12345678901234567890123456789012345678901234567890123456789012345678
90123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456
78901234567890123456789012345678901234567890123456789012345678

Secret (private) keys:

Bob's secret:

12345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678
90123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890

Alice's secret:

98765432109876543210987654321098765432109876543210987654321098765432109876543210987654321098765432109876543210987654321098765432109876543210987654321098765432
10987654321098765432109876543210987654321098765432109876543210987654321098765432
10987654321098765432109876543210987654321098765432109876543210987654321098765432
10987654321098765432109876543210987654321098765432109876543210

Public keys:

Bob's public:
-0.99253267369730281972150176032754022118790992105624507125543320769336941348575889869922418727214057034920994848538647867692319245164459346692514884141253885
77735710057008550976005637967377589543126591621901428384024752233100380495584066974101789677545338179579041079664981256829357775961687944316156560546531793818
51888811385406547957517241732567421014847179510803106424185958189932857411486498590043876689012733309990432817699434372219624839600651365924415416830648193670
13197778620763251079128814038531433871825365724909593862892327773748002925578364495121968721955957357273546210698609042165143341570053608713369168494781862871
02252168519084623359139820998358680536085513909422894108113926797629027042944948159615324349338649389234125557127043525008996313748149642520944279487063275182562100733403811873715137444314968362655939404894278710946095581927907208730303836421587742684650762618046489746552413945100503646486004071007752823258931233973
6

092207755612

Alice's public:

0.750348407569602736287911772398803015645598923427393152319177463451099980459205
703658231147587160551500843974558883279705391514371551350096617529013277529528155
237914429610313294538048979596042149067010148998091000289037969876844839040964
606051284133323254099807890071042191585405867109890532129458352663969455106603
408140780895259528453695824715427847282172800419353364972845295019441716809988875
3229533617499239112621368146966475176657580466608186594513300341770975802842659
07394199677811276710164702315774944186628176954855494729008275356019549445273186
02020297196132737067705657218484049464742037706104430971144882532134625922793565
324617783336373198628242329907985404598802950684850165587277671199128598700848133
505812819645495626082686490819970157873491564987358192957392938349660481068026
9859634634964211692083956012659599346397300435513955184701730689112074109444008263
8209506652817897915147316054767445584112292499343963469122440811531705004813040
10741271

Shared secret:

0.975643583047356413021305580187178368002408650449780286569898544785756025853881
491970369665965892451320479580125318991298068091148630595042433460698812965928630
03131635138305072501068859979180704962494871060884517918610160867561354216130
46159957301049583804071228904772374564768305888314181872940970

4. Control parameters

Difference between the secret key computed on Alice's and Bob's side:

-
8.276525043580174938958349765421949982937977253083607225185901462566162213187898
796625993333751041046792030766101637995455083093692412532232300931549260993324
2800815638198945576637870086383545735758230324782039609096189757017814075557406
92326336734337838882997092852350582123273670851286219253946411964267983677893665
88396316940520981547329350276134542496223626622875367893335328539840801293156339
53305775089376388503056364471246964664134284306577169669536153670843280178766577
69124083327114567216215539476384252321027838435857335868107226320826070737788992
99551787980423894401227547369463230174049815823089406886376448300687822609898211
796068328214229964921783338570288832359135181424632436740205665061088478796947927
37435972758691043010735285870829611102568079644913465881007888878307666128742
40970197472577006759345982376320417735225962329615943421370273986944635228376311
63999272178155221990900595962766697570268001992709820950053883812670778969346291
463464973e-366

6

=> Almost 366 decimal digits match on both sides.

=> Please keep in mind that control parameters never appear in the key negotiation, and are only stated as a proof that both partners share the same secret. The absolute values of control parameters may vary slightly when mathematical libraries other than than the given reference implementation are used.