Міністерство освіти і науки України
Національний Технічний Університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

ЛАБОРАТОРНА РОБОТА №4

з дисципліни «Криптографія»

на тему: «Вивчення криптосистеми RSA та алгоритму електронного підпису; ознайомлення з методами генерації параметрів для асиметричних криптосистем»

Виконали:
Студенти групи ФБ-82
Кисіль Денис
Глотов Володимир
Перевірив:
Чорний О.

Київ - 2020

Мета роботи:

Завдання:

Ознайомлення з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA; практичне ознайомлення з системою захисту інформації на основі криптосистеми RSA, організація з використанням цієї системи засекреченого зв'язку й електронного підпису, вивчення протоколу розсилання ключів.

Порядок виконання роботи:

0. Написати функцію пошуку випадкового простого числа з заданого інтервалу або заданої довжини, використовуючи датчик випадкових чисел та тести перевірки на простоту. В якості датчика випадкових чисел використовуйте вбудований генератор псевдовипадкових чисел вашої мови програмування. В якості тесту перевірки на простоту рекомендовано використовувати тест Міллера-Рабіна із попередніми пробними діленнями. Тести необхідно реалізовувати власноруч, використання готових реалізацій тестів не дозволяється.

1. За допомогою цієї функції згенерувати дві пари простих чисел p, q і $p1$, $q1$ довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб pq ? $p1q1$; p і q – прості числа для побудови ключів абонента A, $p1$ і $q1$ – абонента B.

2. Написати функцію генерації ключових пар для RSA. Після генерування функція повинна повертати та/або зберігати секретний ключ (d, p, q) та відкритий ключ (n, e) . За допомогою цієї функції побудувати схеми RSA для абонентів A і B – тобто, створити та зберегти для подальшого використання відкриті ключі (e, n) , $(e1, n1)$ та секретні d і $d1$.

3. Написати програму шифрування, розшифрування і створення повідомлення з цифровим підписом для абонентів A і B. Кожна з операцій (шифрування, розшифрування, створення цифрового підпису, перевірка цифрового підпису) повинна бути реалізована окремою процедурою, на вхід до якої повинні подаватись лише ті ключові дані, які необхідні для її виконання. За допомогою датчика випадкових чисел вибрати відкрите повідомлення M і знайти криптограму для абонентів A и B, перевірити правильність розшифрування. Скласти для A і B повідомлення з цифровим підписом і перевірити його.

4. За допомогою раніше написаних на попередніх етапах програм організувати роботу протоколу конфіденційного розсилання ключів з підтвердженням справжності по відкритому каналу за допомогою алгоритму RSA. Протоколи роботи кожного учасника (відправника та приймаючого) повинні бути реалізовані у вигляді окремих процедур, на вхід до яких повинні подаватись

лише ті ключові дані, які необхідні для виконання. Перевірити роботу програм для випадково обраного ключа $0 \leq k \leq n$.

Кожну операцію рекомендується перевіряти шляхом взаємодії із тестовим середовищем, розташованим за адресою

http://asymcryptwebservice.appspot.com/?section=rsa.

число 254078110500213928685654373010481153273 не прошло на роль p потму что завалило тест миллера рабина
число 26260229146373812977939139292 4752910296 не прошло на роль p потму что завалило тест миллера рабина
число 18673726980048188496545862169667 6390894 не прошло на роль p потму что завалило тест миллера рабина
число 22424146103659395271385614973517 1370040 не прошло на роль p потму что завалило тест миллера рабина
число 29829063948073354468010170223120 1064532 не прошло на роль p потму что завалило тест миллера рабина
число 23224662564136593249954927249088 5881236 не прошло на роль p потму что завалило тест миллера рабина
число 32971698835038379823632239764542 0790025 не прошло на роль p потму что завалило тест миллера рабина
число 21037009338119510137542331461127 9507842 не прошло на роль p потму что завалило тест миллера рабина
число 29448379677739961108947801601796 1219032 не прошло на роль p потму что завалило тест миллера рабина
число 30636891914020301474672667199711 6513397 не прошло на роль p потму что завалило тест миллера рабина
число 27739091288434127670666526473640 6171265 не прошло на роль p потму что завалило тест миллера рабина
число 28396583382155957947629776369988 0218284 не прошло на роль p потму что завалило тест миллера рабина
число 19991859865208586203587169342336 9436613 не прошло на роль p потму что завалило тест миллера рабина
число 32367212073692646087915436045984 3469086 не прошло на роль p потму что завалило тест миллера рабина
число 25386153243364302153804222614807 1884110 не прошло на роль p потму что завалило тест миллера рабина
число 24498637776717580298818885815856 2278720 не прошло на роль p потму что завалило тест миллера рабина
число 25746535040756625484525388045268 9535975 не прошло на роль p потму что завалило тест миллера рабина
число 31515654684715442679148642024047 1066077 не прошло на роль p потму что завалило тест миллера рабина
число 21197294866096227157851503857387 6794931 не прошло на роль p потму что завалило тест миллера рабина
число 31505747337076542488898854517063 6105560 не прошло на роль q потму что завалило тест миллера рабина
число 27333651787245300756460674718817 0701658 не прошло на роль q потму что завалило тест миллера рабина
число 28062995161996003771179135818826 7235947 не прошло на роль q потму что завалило тест миллера рабина
число 25419724584596122472862819908661 2663127 не прошло на роль q потму что завалило тест миллера рабина
число 31604013805384665803866706348830 0697044 не прошло на роль q потму что завалило тест миллера рабина
число 19614321790180399234973195235121 7548485 не прошло на роль q потму что завалило тест миллера рабина
число 26804860654836758037254181916687 3627114 не прошло на роль q потму что завалило тест миллера рабина
число 21215070627472546499881318080531 3057295 не прошло на роль q потму что завалило тест миллера рабина
число 30206865385750032585776905288616 3527980 не прошло на роль q потму что завалило тест миллера рабина
число 18687750254245746131886150147054 7542583 не прошло на роль q потму что завалило тест миллера рабина
число 18881476203875599311309698902038 2364387 не прошло на роль q потму что завалило тест миллера рабина
число 29439780804857516453762851994857 4344440 не прошло на роль q потму что завалило тест миллера рабина
число 29458401003577625104910916325075 2744347 не прошло на роль q потму что завалило тест миллера рабина
число 17579564780073018030002556196139 0396856 не прошло на роль q потму что завалило тест миллера рабина
число 27820827093499737693560243609753 5686153 не прошло на роль q потму что завалило тест миллера рабина
число 19602285199135252079751997737171 3340365 не прошло на роль q потму что завалило тест миллера рабина
число 28095216231377829151003587397879 8198706 не прошло на роль q потму что завалило тест миллера рабина
число 21837370944541038834417404446720 1664136 не прошло на роль q потму что завалило тест миллера рабина
число 19541159566100187969307222608266 5065875 не прошло на роль q потму что завалило тест миллера рабина
число 18813165906076628753805591042126 5925547 не прошло на роль q потму что завалило тест миллера рабина
число 30150926451067939961240124335218 4798147 не прошло на роль q потму что завалило тест миллера рабина
число 25048977698102876517476545861568 1324196 не прошло на роль q потму что завалило тест миллера рабина
число 26726873996145792287635073350427 1096583 не прошло на роль q потму что завалило тест миллера рабина

число 22650728923629569099703371465814838724З не прошло на роль q потму что завалило тест миллера рабина
число 19585511104037901948486359605873220713 9 не прошло на роль q потму что завалило тест миллера рабина
число 21521520123670675935339579480236670929 6 не прошло на роль q потму что завалило тест миллера рабина
число 24614116059856447899757276797030245468 4 не прошло на роль q потму что завалило тест миллера рабина
число 26546254376100276760067788338478523354 9 не прошло на роль q потму что завалило тест миллера рабина
число 18840799609612142542372916465822901752 6 не прошло на роль q потму что завалило тест миллера рабина
число 17622688282882132816085619098723800820 2 не прошло на роль q потму что завалило тест миллера рабина
число 30349630267526864157967222207466743043 9 не прошло на роль q потму что завалило тест миллера рабина
число 32921866853915632046080198916140582886 2 не прошло на роль q потму что завалило тест миллера рабина
число 26456351767093718009843106665820963398 4 не прошло на роль q потму что завалило тест миллера рабина
число 17138658896479271080637622355727285404 8 не прошло на роль q потму что завалило тест миллера рабина
число 32343471719425810590542412291577542151 4 не прошло на роль q потму что завалило тест миллера рабина
число 29487884782016404823569097462637082061 7 не прошло на роль q потму что завалило тест миллера рабина
число 19375158120167905802172894011298192616 2 не прошло на роль q потму что завалило тест миллера рабина
число 19928564019884516733190222539410703028 5 не прошло на роль q потму что завалило тест миллера рабина
число 31807251681032481982509318508959684394 1 не прошло на роль q потму что завалило тест миллера рабина
число 33129789201527992447198651695102437624 7 не прошло на роль q потму что завалило тест миллера рабина
число 30135570871304704403448819422956300148 1 не прошло на роль q потму что завалило тест миллера рабина
число 21737811916979772342654083632723760584 6 не прошло на роль q потму что завалило тест миллера рабина
число 17584381297068314096896571907813279651 6 не прошло на роль q потму что завалило тест миллера рабина
число 18439203804804544346909267046084446827 6 не прошло на роль q потму что завалило тест миллера рабина
число 25092447578368440307260142967025300077 9 не прошло на роль q потму что завалило тест миллера рабина
число 27825471883125338538815912463194914884 4 не прошло на роль q потму что завалило тест миллера рабина
число 26291864489081330553680496888923383822 6 не прошло на роль q потму что завалило тест миллера рабина
число 27442727690278609097714828876557767558 48 не прошло на роль q потму что завалило тест миллера рабина
число 20596411600983579534202140215739203090 7 не прошло на роль q потму что завалило тест миллера рабина
число 18401413280023699960206626629676705613 1 не прошло на роль q потму что завалило тест миллера рабина
число 22588517175543787512914742147940696506 8 не прошло на роль q потму что завалило тест миллера рабина
число 21908239908996360321709811289722968152 7 не прошло на роль q потму что завалило тест миллера рабина
число 28391326989398873983657016877587994079 3 не прошло на роль q потму что завалило тест миллера рабина
число 27386649736898889453556933342400507400 2 не прошло на роль q потму что завалило тест миллера рабина
число 19672876521859045640273105385169742664 5 не прошло на роль q потму что завалило тест миллера рабина
число 21340837554636752601581960800744831313 8 не прошло на роль q потму что завалило тест миллера рабина
число 17121408063793264295540351623588915445 2 не прошло на роль q потму что завалило тест миллера рабина
число 31494369504939203625139308963121989099 3 не прошло на роль q потму что завалило тест миллера рабина
число 33244060428961245570283995191622392264 0 не прошло на роль q потму что завалило тест миллера рабина
число 22130519331044509061189199891304379854 6 не прошло на роль q потму что завалило тест миллера рабина
число 24204052532113029427907628916100467764 6 не прошло на роль q потму что завалило тест миллера рабина
число 21964477214610653218735363360046194152 9 не прошло на роль q потму что завалило тест миллера рабина
число 30614005697779173090778829329150518845 0 не прошло на роль q потму что завалило тест миллера рабина
число 18555559427729335219085159955250225921 4 не прошло на роль q потму что завалило тест миллера рабина
число 26397864067239120705987837920298444421 1 не прошло на роль q потму что завалило тест миллера рабина
число 33714945438070021176652431980135534390 4 не прошло на роль q потму что завалило тест миллера рабина
число 21001260294881883959372347347780721896 2 не прошло на роль q потму что завалило тест миллера рабина
число 17994522187562944034717948772814541044 0 не прошло на роль q потму что завалило тест миллера рабина
число 26465424026105618786285557927756111536 8 не прошло на роль q потму что завалило тест миллера рабина
число 29792080407973123761374536179316902946 8 не прошло на роль q потму что завалило тест миллера рабина
число 29153939769876605034596311002905492293 7 не прошло на роль q потму что завалило тест миллера рабина
число 33659582971559812702943283210528451445 3 не прошло на роль q потму что завалило тест миллера рабина
число 19865150028876437087009755082016865323 6 не прошло на роль q потму что завалило тест миллера рабина
число 19572147087823340938891087138291204660 5 не прошло на роль q потму что завалило тест миллера рабина

число 22365395754938229758559630519746262574 2 не прошло на роль q потму что завалило тест миллера рабина
число 19553303244963268450239497047160664872 6 не прошло на роль q потму что завалило тест миллера рабина
число 26488265374540401651857096667874800722 6 не прошло на роль q потму что завалило тест миллера рабина
число 23872976767418745425743576023413635964 8 не прошло на роль q потму что завалило тест миллера рабина
число 25522070929281520981018045822248857646 1 не прошло на роль q потму что завалило тест миллера рабина
число 17064906656488678377888504214209920088 2 не прошло на роль q потму что завалило тест миллера рабина
число 28606458473912651296319230401548317714 4 не прошло на роль q потму что завалило тест миллера рабина
число 31179678932732467087817764927556000288 0 не прошло на роль q потму что завалило тест миллера рабина
число 22431121668457851679997395682962051877 8 не прошло на роль q потму что завалило тест миллера рабина
число 33557478853995900393735463493609230506 7 не прошло на роль q потму что завалило тест миллера рабина
число 30383884223938551637256514553199479963 4 не прошло на роль q потму что завалило тест миллера рабина
число 32694919468118858913823365003079987388 9 не прошло на роль q потму что завалило тест миллера рабина
число 17325803291994535688433711566893530794 0 не прошло на роль q потму что завалило тест миллера рабина
число 29013578889682278427424750465595770177 1 не прошло на роль q потму что завалило тест миллера рабина
число 20808969747328834694135676483357987221 1 не прошло на роль q потму что завалило тест миллера рабина
число 20954546098323064132561687628979689101 0 не прошло на роль q потму что завалило тест миллера рабина
число 32533755723425455031915672339687144682 8 не прошло на роль q потму что завалило тест миллера рабина
число 32572224043550607041483723667761262514 4 не прошло на роль q потму что завалило тест миллера рабина
число 32423560948882882006428490738454598505 4 не прошло на роль q потму что завалило тест миллера рабина
число 20489465068322453217255481277312374839 2 не прошло на роль q потму что завалило тест миллера рабина
число 27350019383947654586859234413414298060 1 не прошло на роль q потму что завалило тест миллера рабина
число 31715075289923366256307204470353897151 7 не прошло на роль q потму что завалило тест миллера рабина
число 25802547223034429111039669130896931463 8 не прошло на роль q потму что завалило тест миллера рабина
число 33264514340932454647428957018308372366 8 не прошло на роль q потму что завалило тест миллера рабина
число 27458265785812750524531275503238659120 0 не прошло на роль q потму что завалило тест миллера рабина
число 26139618901933737015776134141691029101 4 не прошло на роль q потму что завалило тест миллера рабина
число 25734868431715673547791201045214597930 9 не прошло на роль q потму что завалило тест миллера рабина
число 25704662996688893734628585563083781066 5 не прошло на роль q потму что завалило тест миллера рабина
число 32910507312418431613412359470593494647 0 не прошло на роль q потму что завалило тест миллера рабина
число 29094844038347442694058715453117053325 9 не прошло на роль q потму что завалило тест миллера рабина
число 19878541921166588675191574077114294742 8 не прошло на роль q потму что завалило тест миллера рабина
число 26326789024089662945891965659631605097 7 не прошло на роль q потму что завалило тест миллера рабина
число 20232998170986821657729673986630640992 3 не прошло на роль q потму что завалило тест миллера рабина
число 18850869573027964220800027151592026583 5 не прошло на роль q потму что завалило тест миллера рабина
число 29908677250520175028056988629770033738 4 не прошло на роль q потму что завалило тест миллера рабина
число 28162418237530576554212707483996795623 9 не прошло на роль q потму что завалило тест миллера рабина
число 24394193486652274535177822681410650605 5 не прошло на роль q потму что завалило тест миллера рабина
число 23095826733531079301188411976536930660 6 не прошло на роль q потму что завалило тест миллера рабина
число 27093274127636119175802751712691017285 1 не прошло на роль q потму что завалило тест миллера рабина
число 31682508780958128183849773689908418378 6 не прошло на роль q потму что завалило тест миллера рабина
число 27332398975709402575286637115563096702 6 не прошло на роль q потму что завалило тест миллера рабина
число 29578394270857245089639508466651030455 8 не прошло на роль q потму что завалило тест миллера рабина
число 26257189592788025068256574208500375052 7 не прошло на роль q потму что завалило тест миллера рабина
число 24511639773778169659804377560384229960 4 не прошло на роль q потму что завалило тест миллера рабина
число 18751464439339122090013658922892957143 3 не прошло на роль q потму что завалило тест миллера рабина
число 28173562592132531856214903972304092468 0 не прошло на роль q потму что завалило тест миллера рабина
число 20356644133684508422231029783314520811 4 не прошло на роль q потму что завалило тест миллера рабина
число 24961169680118132734191319019083999805022 9 не прошло на роль q потму что завалило тест миллера рабина
число 28738251677326231174152859869291251162 9 не прошло на роль q потму что завалило тест миллера рабина
число 21050409380381430868176228229001697320 9 не прошло на роль q потму что завалило тест миллера рабина
число 28363554857659841987546891171572111501 4 не прошло на роль q потму что завалило тест миллера рабина

число 223346982543550701835094502557236177847 не прошло на роль q потму что завалило тест миллера рабина
число 32938729740780414840007806654911232405 1 не прошло на роль q потму что завалило тест миллера рабина
число 32301092943294241222407738295257218871 6 не прошло на роль q потму что завалило тест миллера рабина
число 22321010749019835937632891656439515571 9 не прошло на роль q потму что завалило тест миллера рабина
число 29928339021571794488250791679350217178 6 не прошло на роль q потму что завалило тест миллера рабина
число 30578238900920421468666091636789446751 4 не прошло на роль q потму что завалило тест миллера рабина
число 17427604686141328340650516699821506995 9 не прошло на роль q потму что завалило тест миллера рабина
число 32640536109192939736455182602287148213 1 не прошло на роль q потму что завалило тест миллера рабина
число 26883987236771823919697294035939470899 5 не прошло на роль q потму что завалило тест миллера рабина
число 23729164202540005534092549679099024841 0 не прошло на роль q потму что завалило тест миллера рабина
число 18830837671211526924409712043857639421 7 не прошло на роль q потму что завалило тест миллера рабина
число 24766948625165251703586314449471711703 1 не прошло на роль q потму что завалило тест миллера рабина
число 29470288869972042816087748241098144793 9 не прошло на роль q потму что завалило тест миллера рабина
число 31004163099869491938865469782626875968 7 не прошло на роль q потму что завалило тест миллера рабина
число 27619964620010196819245545913075145544 5 не прошло на роль q потму что завалило тест миллера рабина
число 26097344120084996659671241298295283617 2 не прошло на роль q потму что завалило тест миллера рабина
число 17331302595442250705960698008602971462 7 не прошло на роль q потму что завалило тест миллера рабина
число 28502821873609415893000944851637795066 5 не прошло на роль q потму что завалило тест миллера рабина
число 32216301480655246697283639186408172493 5 не прошло на роль q потму что завалило тест миллера рабина
число 27307864302246754083261431628810031295 3 не прошло на роль q потму что завалило тест миллера рабина
число 29226040401062301882454154188848306889 8 не прошло на роль q потму что завалило тест миллера рабина
число 18477526989985032193397046270576075693 9 не прошло на роль q потму что завалило тест миллера рабина
число 23656406176385436461954225077040705279 4 не прошло на роль q потму что завалило тест миллера рабина
число 30055098428729460914379166244444002623 0 не прошло на роль q потму что завалило тест миллера рабина
число 18142105176674977568781527912388741488 7 не прошло на роль q потму что завалило тест миллера рабина
число 26562945454201884663314209409498153825 9 не прошло на роль q потму что завалило тест миллера рабина
число 19343552753059177375064448486220917750 не прошло на роль q потму что завалило тест миллера рабина

n1 сайта 0x980e7fa40453c6b05b7e21e36c697315eefcbaf56aa79aa7b90b90daeca41ebf

e1 сайта 0x10001

Таким чином, параметри криптосистеми мають наступний вигляд:

p користувача denys 0x922c81e2109ee5612542f188f4b3dda9,

q користувача denys 0xa1aed769379b0fd3aa20c89fa12880f7,

функція ойлера користувача 0x5c51d2eee93175d3f128deb2d7f337ddde34c17d76d77eb9ec45d9ce5deaff70

e користувача denys 0x10001,

n користувача denys 0x5c51d2eee93175d3f128deb2d7f337df12101ac8bf1173eebba993f6f3c75e0f,

d корисувача denys 0x49e0f92a53d74ef1c305efe1b34b6223dd54de9ae6e5e0f62c8c6196f235c321

```
p користувача denys 0x922c81e2109ee5612542f188f4b3dda9,
q користувача denys 0xa1aed769379b0fd3aa20c89fa12880f7,
функція ойлера користувача 0x5c51d2eee93175d3f128deb2d7f337ddde34c17d76d77eb9ec45d9ce5deaff70
e користувача denys 0x10001,
n користувача denys 0x5c51d2eee93175d3f128deb2d7f337df12101ac8bf1173eebba993f6f3c75e0f,
d корисувача denys 0x49e0f92a53d74ef1c305efe1b34b6223dd54de9ae6e5e0f62c8c6196f235c321
```

key sender

k = 0x5b87ebe0be56f78e1ab0808c6a4779b4bf9368485646cacabca9b499cc3c1bc9

k2 = 0x48d7374a29fbe551c11408a53087c41a461d9f9da79492d1fd8bc79e0f2807e3

s = 0x5a7564395e9b649519526ffb42820f2dfbb13c5488c588166086a2986089d490

s1 = 0x5d507453dea4d68279b5b004aa4485c995dbc5def3b7ddfb9b8f36c32b508fe5

ответ ReciveKey сайта:

{«key":"5B87EBE0BE56F78E1AB0808C6A4779B4BF9368485646CACABCA9B499CC3C1BC9","verified":true}

Висновки:

В даному лабораторному практикумі ми ознайомились з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA. Також практично ознайомились з системою захисту інформації на основі криптосхеми RSA, організували з використанням цієї системи засекречений зв'язок і електронний підпис. А також вивчили протокол розсилання ключів. Цей практикум дуже важливий, тому що алгоритм RSA використовується у таких сучасних протоколах як: PGP, TLS/SLL, IPSEC та ін. і треба розуміти як це працює.