

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний технічний університет України
«Київський політехнічний інститут»
Фізико-Технічний Інститут

Криптографія
Лабораторний практикум №4
Завдання варіанту №3

Виконали студенти групи ФБ-82

Дигас М.В

Кудрик Е.В

Перевірів:

Чорний О.М

Мета роботи

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

Порядок виконання роботи

1. 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.

2. За допомогою цієї функції згенерувати дві пари простих чисел p, q і p_1, q_1 довжини щонайменше

256 біт. При цьому пари чисел беруться так, щоб $p \neq q$ і $p_1 \neq q_1$; p, q, p_1, q_1 – прості числа для побудови ключів абонента А, p_1, q_1 – абонента В.

3. 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 А і В – тобто, створити та зберегти для подальшого використання відкриті ключі (e, n) , (e_1, n_1) та секретні d і d_1 . 4. Написати програму шифрування, розшифрування і створення повідомлення з цифровим підписом для абонентів А і В. 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 А і В, перевірити правильність розшифрування. Скласти для А і В повідомлення з цифровим підписом і перевірити його.

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 $0 < k < n$. Кожна з наведених операцій повинна бути реалізована у вигляді окремої процедури, інтерфейс якої повинен приймати лише ті дані, які необхідні для її роботи; наприклад, функція `Encrypt()`, яка шифрує повідомлення для абонента, повинна приймати на вхід повідомлення та відкритий ключ адресата (і тільки його), повертаючи в якості результату шифротекст. Відповідно, програмний код повинен містити сім високорівневих процедур: `GenerateKeyPair()`, `Encrypt()`, `Decrypt()`, `Sign()`, `Verify()`, `SendKey()`, `ReceiveKey()`.

Порядок виконання програмного коду:

1. Генерується пара простих чисел та відкритий ключ і секретний ключ.
2. Аліса формує повідомлення з підписом.
3. Боб приймає повідомлення, перевіряє підпис та розшифровує повідомлення

Прості числа, які були згенеровані

Value 0xe26a5633fdf388da7e824676aa199ee70b2a2e31aca2c15e6c188caccbdf659 is not prime .
Value 0xbd328e3713a3a8c1dc7f629b4826f1c1a20d5b5b07f3276149c5cc29e019f2c3 is not prime .
Value 0xd208d4d134a13182b61f9e4043cce1d5e3c02e738e9f999aef3e9bc14361f86b is not prime .
Value 0xb6b76e68b29b646fad3074d350c9991af1aaceea48e939876bb1e16d175ecf11 is not prime .
Value 0xada56157c8ae2fea3057c9d04b81e4e4c9a9e7e4f328ef16b5c0c0796d6fd509 is not prime .
Value 0xb57445eb17bca9a6b439d155e1b31ee928a9b8ea8df09c3f1f2038fe85fd795b is not prime .
Value 0xc1b6c0cc7c16245905bdd0ccbcbcaf319d2ac33f10afbcb7059cda1f897f3df is not prime .
Value 0xdda9238ad13da04776f8dc2a362d73bb1f0b9b06fef8705c5cf3291e80ffb0d9 is not prime .
Value 0xae21f5832e40d89a11809c58a692c7b226b3e446076e047387610a42c22a0e25 is not prime .
Value 0xda09e12e4a1fa5241306cb70b7b5af66181695ae24ff30e37460d0214a82bb73 is not prime .
Value 0xfb564b733a1353fc546be5acdc4ebf7d55b59f3128fa93b6d80a0129b23c235f is not prime .
Value 0x9077952ecbd2b9a2d68458922cb01e2a12eec624da4f0115d387bbe08b5b2019 is not prime .
Value 0x87f0fb79189a021f77bc1bd1a34068c2454425e919c50474e37130a5cba88479 is not prime .
Value 0xe4a29fd207b5499561aa4d348caa489bbc25b5afceccb9770799e18021f0e78b is not prime .
Value 0x8ef22ee73b752bc184d5efef5f0e37b86f44e842ade5349a206d5c45b6066d3f is not prime .
Value 0xb9e8d80b53403818f3b2b00144c02308230c8aee21c0bdce414bda994b23ef3b is not prime .
Value 0xa2c3e486066ba70491092abdb07ea2acc636b09f3846f581525b2b25b0ce5d87 is not prime .
Value 0xd199c6e318a4123780ca14381fcfa952cab2a37f3193a54400b7970de26f71f3 is not prime .
Value 0x8b92e764e456a8e4c64d42294db43d2a0cfb94d9e0bbdad04818f995cd0c623d is not prime .
Value 0xa70b72e4a70beab2e0544480660f7ee32490c626d293c74c9e529b42f1496c5b is not prime .
Value 0x8b63775e13da6542bc2b661d3e4e0df6787c20122baf4181cc56dd992cd50d49 is not prime .
Value 0xc3fcf96a6156f34f837dc1e6df2febaaf935ad24d61c09b26d7789d0945ee7d7 is not prime .
Value 0xedf8344ca40b6be90faf0fe50b5620f300d0e901e184b83108d7cffe1a2a1e33 is not prime .
Value 0xbfbcb641d9ba0eeb7a492aa68205bd3db5c6ee1c5ae97e9d2ba5c1d4b9613b1ab is not prime .
Value 0xfcb7ccc66f2eac57cedddc262fdffb9fd2d39a32d496a69263ac1ea99ecbc3 is not prime .
Value 0xa20dfe250324dc65378536bf99583afe68ec2e7ab007b261b6b757d77257e21b is not prime .
Value 0xa4eadf6e12704fa052541b9518d418f6a8c5a17f729a0b34d06fdca7558aa8ef is not prime .
Value 0xaeff0dbcdf8b119c4a8aaac8783607ecf53b4960a846ed6d2ca7df350f7b2ba3 is not prime .
Value 0x8f9a532ad323c3ffcea074cb2e9bf4377850866f3849ec4b0bdb3fa23cb5f11 is not prime .
Value 0xc897f12c63329b67daf5b4914d98a348be7f228bd8ebe1ec2112a7d0e194043b is not prime .
Value 0x926eb7377c75bd219382a8af277479c25fde0997f5ffe6a4ecd0f4903f06bd6f is not prime .
Value 0xbf328d2ee599388d868e3bde72862b6c166bcff449b893f0efd700291002cf4f is not prime .
Value 0xf5a6353c9465dba7f1b3fdd9dc6c9f20ab87743d16bc63fb623f5fe81617f607 is not prime .
Value 0xa488bff1a034599adfff418dc00df96b877614ce755e42ee66c9b79c472a2db7 is not prime .
Value 0xdaecc783ba75d14df31a98bf504204deee49dd9b87ac1a41ada9d6ca1618ce1f is not prime .
Value 0xe994fe16b0b51ed5ef6ae779ff999e749d21ef3982f02927e2ac6519414edfdb is not prime .
Value 0x9be6195bf6f63258c80e783969b0016db1f4fbce5b405339de04e142942e6239 is not prime .

Value 0xe6a10cc231b04cbd794cf7bd8b7fcf3c93aec5f54b3197a0ed7244ab038f0c8f is not prime .
Value 0x9caf387a8aeaf59fabd1afaa5ec3ae814f2f3738b9ca832ad1db83a16dd584c1 is not prime .
Value 0xdfd410b9dd4da1f16ebfc90b5c5ff4322704b9bfd632088f26dfc9ee86424521 is not prime .
Value 0x96660c4b2b2207f808130d6eb4fa4b220b7861b83f5f32f6694eae2c3189c903 is not prime .
Value 0x9393a52a741cda3ae84a71ce54aba86be504f374acbaa6c6557e0f68d3e99397 is not prime .
Value 0xd3168c295ef07105785ee06fda5485c9a69d2498ef141e3f59c65390b0394d71 is not prime .
Value 0xaaefa49bbc9b32bcb2509192d995ebbc8874ac9556c650bb4686ada412111f4f is not prime .
Value 0xb63e2b74fd963982070a484309343470b8927142a4d42be310395cfb66d1cb71 is not prime .
Value 0xb2fc157449fb30bc9067c54b5ef61ca8b926f70db0317f6bd15ebf54ddf88cfb is not prime .
Value 0x8a2bfd039a7d32a869aac402b808aa39998cdb8900cd833f40961325155b787f is not prime .
Value 0x9c22914c80d0bf596d7056da68da4380666111ca1746bf3fa9ecc536811306b7 is not prime .
Value 0xb575e7d60251d1e0c251163083be432c0f4dd5ff23c0931d2711c47557a3cceef is not prime .
Value 0xecccf79d8815fe51233de8e35837f39ea43396abca0d7a2452a84bfd4d360415 is not prime .
Value 0xb0e87e3db2d0baca65cf207f30562b8dda3e01d0c0efb0f90bfdfc9d8c6cd009 is not prime .
Value 0x9defd8ec929301edace14c91232f01f26b08f3f17fecca0250eabddfa99496d9 is not prime .
Value 0x9c340377d85c35aac74d8956097acf9b053a087f8fbc6b61af1735030cc8ac7 is not prime .
Value 0xe01502edc74fd7c17bdac5e0fa208c0e3db732c374018f0535fa4ef55d1f7fd9 is not prime .
Value 0x91d8e5d4e0df2e2cf5e238a056e7190d085dbfe7b72723195250f45e21daa9c3 is not prime .
Value 0xfb673b3d6a1a5ef825c6937725a6e319dce591089bb1cd369ea33c75f1349b47 is not prime .
Value 0xaa169e41dce8a68d2be7e549376c40aa19ecbd4930eebb1e038f9079b7050e0b is not prime .
Value 0xe036b5e2fb6f5b6f195e24ff6db61af3ead4221c1f253890fc53da9e10e5c073 is not prime .
Value 0x9f12386cf979121a77f2cf017cd84b7c0686c7d4cad365c65af34ed6c23bead1 is not prime .
Value 0xae2cf3809d0a5bce07a38d0a4f5e7363d8b336f499a97b7951b6e0dc82238727 is not prime .
Value 0xfd30d9c495c57591198b44ef17db570d58381367d1460aedb9d3c1d8b7233d71 is not prime .
Value 0x9240c8bab0b091e96b2e7cc0878c7db055d9749c243d6606bf40d5fad313d43b is not prime .
Value 0xac083230d07c1ac45925c39ca7c7c0a80da46494df6e779c7d9c7638020da6ed is not prime .
Value 0x8a4dc053338af1b0dde8543734d9acdb1aca452697f12f0c55a7104135db115b is not prime .
Value 0xd8d2277066754435374117b9d8b263ba6652f4b99b2e2ecf6a6d8ff7fb0ce7d3 is not prime .
Value 0xcfa3a54388f4123574e2717ded1093d0072e33857e221c32f4f90662679052d9 is not prime .
Value 0x93b7a91567ffbfa6621410dee68b7447dbeec6fa95c5e1cc790ba0b6086db1d1 is not prime .
Value 0xe3d07baff2cd5a4783545185d1a400df77d55ee53da147848ffe9808d7ba34ab is not prime .
Value 0x9a3561acf4038426ea4a2e9788a7c3977b56a7e9c26ae65ecfdb1d275a5d965b is not prime .
Value 0xabdbdf80d5e4ce99936123506a3032d9ee8f3f613d6fa7b0726d1b29656bd4f3 is not prime .
Value 0x962573c965c3d532d8612f2b9c3df4874856664006af2fa285863b8428028f6f is not prime .
Value 0x92421da40d23cbd1f476f91aced48fdc81afc5fd59b8c385635cf12a66be370d is not prime .
Value 0xd88cdbfe11d5c69cd36a720128859ffe157ae98f06f8b9523acf672421bece4d is not prime .
Value 0xef34591bf841980ce85e4095bd5203e885ed25c2c61d8b44fa1d1d342f430bad is not prime .
Value 0xa0ce827b838320b7900aba1000f5bf28264007aebdba008f3b690b8e8781f231 is not prime .
Value 0xc000501dfdb301fd0403858868cc5ac8ef3aca217ae4efd35e3e9e39b38c14b9 is not prime .
Value 0xbd7cf8839e0d63c0bda40bcd594287a12ab2f93be2f12ad77b58ad9a981330d is not prime .
Value 0xb30026adb2d5544c294e2e6a31957863aaf8c358e9c9b077a2991780f95637e5 is not prime .
Value 0x9f474349b1b05e039c81710c09244a3b064abe864fbdafa12bd203d8cc70fb23 is not prime .
Value 0xe1bd23accc43d33d3a8d972b42e0174a5f7f7ec81679de549f0cad5d9184d59 is not prime .
Value 0x96508091e9baac25f9afa421c7ff50d26f1b3400c1d526dd8310e1ff33ba24c5 is not prime .
Value 0xd6a9f5b141d4a816896197b351d453934fa21a3a525011d787452ffefb3bceeb is not prime .
Value 0xe23b354a5042dc1fc2516027d57534edfb9b102367bcf79e2e66209cf35308d5 is not prime .
Value 0xfbd9443d6e105be01ce81d5adb450c2a642854d7b4f9a44258e7c59ab1328725 is not prime .
Value 0xa4de082056743c10f1fa684977b13aca7027e6390219d50b8538f4006b0cd5f9 is not prime .
Value 0xc87db7dec3d492f102d8cfda58392370298be02c69e595eb8834a563ac917d is not prime .
Value 0x8936bf175252be7ca97d2b2c3fa04dd835639590dd64cb6933391355ce28819b is not prime .

Value 0xc76da17ac4322fde17dd8d8075a3d036349ea21de27b19a034cf4d4cf7764af5 is not prime .
Value 0x933b6f7d921108ee0717594a6d7f8df5e986ae87d03f058b7c934f5ae790db15 is not prime .
Value 0xc4f1237ca51b54affbfafcece8581845dee95cf4f2e8dee8f84ec1abe76fd2105 is not prime .
Value 0xdb5b6c47f77e74ee56bbba7d2e9a85d0d1786a562ca0e69191e9fc85cd39451d is not prime .
Value 0xbf16caa75c4e75ae589d647b3b7bee59b581eef53b6db96a05674a8fcffbf11f is not prime .
Value 0xdd632f49e17cab8d9105a49174a4630baa0e941940eb518bafa73cbb65c6743b is not prime .
Value 0x90b7046a7412aa79f5e0bbaa28708ec8e94693c50412eaa6bd2785340520426b is not prime .
Value 0xeaebbc8418c691a42f58db0afc00936cdc2b62426eaf7cd5c86aed2112b9537f is not prime .
Value 0xb9ec29259708747c14b749489ed0a0426e7ddd2a96d98b442324398cd6e5b47f is not prime .
Value 0xa2dab7a9f095d8b31697967596d74585c1e4f0bb9e91095e77acd07d9833647d is not prime .
Value 0xe954d1178e5d7df5d5aaf1da8f85dfa990210d9e26fc91bb39b5be19e78a7a55 is not prime .
Value 0xe3dc5e6336bd2af7b328cfd973464f9c3cb8a332df283006b9044a99671b1ebb is not prime .
Value 0xd837a23110fb4a02de666211f7b9ac522f963d5499abed431b2e962d2ad36803 is not prime .
Value 0x983bc073cd1dda9dcb983364c8580e9a4f0b896425ad990d32d2649c97ca69e7 is not prime .
Value 0x8d174c3c7b3b376791fb96edb80721e1890f404dff8658d0133858b3b62c6393 is not prime .
Value 0xe54a97c3a3517132daf51c4d7ea71bf803ba8873b801ddf34bbf4a635196effb is not prime .
Value 0x8da4005f215bf1575270f19ea1a595aeb530898eb7afa8226db0d772498d70e7 is not prime .
Value 0x97a117154a0863c65ff5608f9bbc2f2fdb3aeaf59f7a59a0f3671602fcdd0fc1 is not prime .
Value 0x8a324590925c4f5a2deae41fa18663273ef2357777670461c3401f28a3ebe21 is not prime .
Value 0xb9ff46f0ad3030fe67969517193fee57c100293c9d708d71f7515b23c32982ff is not prime .
Value 0xd4db9f365529bd2fd01e56365d497202262577e2ebebb161893d1cefec9f0b75 is not prime .
Value 0x8eec14e5a1b3ff277e1cdd7aa2cc5edc003c6bbc4ddcf7338c9ccc582d478027 is not prime .
Value 0x9289a26efe78d45c7a9000bf5e67e80ffa7c205c5aaf46aa3542dc3c23da0eb7 is not prime .
Value 0xac7696a70bd767b7aacef6401fba76c3bc3aba558e57e7a6d07a85dc03b8df99 is not prime .
Value 0x8921b333e4873778e96e85e9e446be5f6bfd9496d3a9f455fdf35fdc36624aa5 is not prime .
Value 0xbe93749d454f995b5e080cecb339161b70a57421ae16edc89e7ea4f2ec1f9815 is not prime .
Value 0xd1e69792956316d36bfdd6dcd721b7658e4ece007c2530cdcf7d62ccadd3d31f is not prime .
Value 0x986d77f14c0a0fe792a47dc7b9a92b6178193472027ba5a43d231b0e71953e31 is not prime .
Value 0x81c4528f31fab22f9c3838c10d3affacc464fd7a3cf2111faf7d1ceca4e433d is not prime .
Value 0xf1c791852f4069a9c14fe0b15a6633ad3e1e58909d953360523028405ff22f09 is not prime .
Value 0xeb3c531dd7de8f4df512f138bbea6106f229adfceaaf3a357603650023c33aeb is not prime .
Value 0xc3ef4b58793cafdba6fbb06a368f80e5d2a8771f5a0bf3262a80ca823e686c5 is not prime .
Value 0xf8b2403f6ba20b0e9e6671124f8f3c0895549d572ff86df510326164b9b9f7a9 is not prime .
Value 0xe4ee5f8b71ece8ced525a2894f522c4ead549dfa8772f02f166431d795aa0dd is not prime .
Value 0x95cb0f194659841cdd2f5eddc166aaf164e73de9b9ace5f5cacb7901909436f5 is not prime .
Value 0xe105689ea3531dd608935bf30b3e402f0ac9c4c874872429d01603105fda7c59 is not prime .
Value 0xbb5a93f97c8c91e2f37c47b7065c7611ceb6ea409d934c1b5b38c3012230fd23 is not prime .
Value 0xf8a1977da306adda1817141bd243db26b2c9154d874a2f6c5b1ca238903adef9 is not prime .
Value 0xbd0e3111997a793b9721d2d5dad47852c7123905973c4446e97bd00313246185 is not prime .
Value 0xa96d022744dfbb1f119ee3f661f79979a5b950675097c38e329094a91a33a565 is not prime .

--P--

0xe864e8add38a4827ddaf8ca082c7861dcaeb0aa2457bdfbb0f48d83c638425c5

--Q--

0xc70ffeaedb5befb84be0ba35793e6038950b31057c5804fe6f4a7b07ced928cf

--P1--

0xd1646374b3d6be8ba69800d85cc4ee37262d48285a01611a5cc0927cf8dde461 --Q1--

0xe80316b8fe3903b43baaa3eb50c95a10c64c823fcbb864e9d1ecf76d8df3bf19

Параметри криптосистеми RSA

	Alice	Bob
Public key		
n	0xb4b4f5fb9c3449c31fa2a17724910eb533294b13c0a0329f895b2271ccw4c91ce2b088c7ce9593d2bf18d69e9269dd8d2ffa6ae6b06e640e52da9a92ca7be524b	0xbdc580e4ddfc7898094ec6ef2d0bdd394236e3991c08b0a6448a9e9f21bda884180ba230035b4ef576940e50ff48c7aab3794822204b89df660bd1981022ac79
e	0x3ca5ef075033175626d74051a92d0de62f1313baf93ed870efdda8d1661a75baa27a522b22ff111714fa6c301da5c17dfc8aef0d896bedfcd551a28d799805	0x2c55148c646ba3c7e56baeb050302589c3cedd05b736d962e7df3afeedfad6ac66c6c064be3987567a30167eed90d02345c9307b6e431ff84b15508a43287191
Private key		
d	0x2c95003ddacf3d8c0affa37f18dbe77678e0061f0848dbccaa7a568f9147f1dda32ff9cc438b5c57674942e1e99a7328dcecb20edff4d55f89e8dcb196e54dbd	0x53e54d4710d8408f9007641f35d3a7293bc14e69d354a2cec7e64818f198c1dd4ae54af1f85f55b1fd6d50df42e892faec0241511e2054489a3c8a354634e371
p	0xe864e8add38a4827ddaf8ca082c7861dcaeb0aa2457bdfbb0f48d83c638425c5	0xd1646374b3d6be8ba69800d85cc4ee37262d48285a01611a5cc0927cf8dde461
q	0xc70ffeaedb5befb84be0ba35793e6038950b31057c5804fe6f4a7b07ced928cf	0xe80316b8fe3903b43baaa3eb50c95a10c64c823fcb864e9d1ecf76d8df3bf19

Чисельні значення прикладів ВТ, ШТ

ВТ	ШТ
0xd1e77dd67beb43df75800fd82fa02a4e31d0c6f4733233ca2d4f642c82308ab2408157b686b8079613005afc87b48fef3331dcf68334656671e382dcb6ccde2	0x65b1e4909bbeb32af15adbff697fe4b6f446cbd02ad7cb65f8a97c32a0e679eb093aa42a69fc4e4f69e9d318bfa1b5e010084e6b08a57276c1895519a9555223

Цифровий підпис

Alice	Bob
-------	-----

0x95a136c008cd7849594152a9403d4bde4 a90b3a5b814c032ac92b576c4a686b1d93fb 3c48d6326590c96d0da94ebe8b9f0bf98d9c 0620861bdf0e2ba26f17a15	0x9cfd292d664f43d41e662bd8c2e0b9073e dd2beb4763c05ebd1ea6a62c2a01260d21d 0b03e14ca55b05c3daf30473fae2f09417afd 7d7a4711dab07270180b61
--	--

Перевірка з сайтом

Get server key

✖ Clear

Key size

512

Get key

Modulus

A704985A75C8D3D37710B0AD6EF70FFCCCF94850C4275F95AE48B60C13048D14EEE232F4227C65ED59A32

Public exponent

10001

ReceiveKey

Receive key

✖ Clear

Key

7A85200EF47F5AE97DCE51F4667D1D8E8CCF5B4DBFE127C59FF4B3B3F3FCF6BD0513E6B9C1EB2A951C3

Signature

883AFCE3D65FB583

Modulus

A704985A75C8D3D37710B0AD6EF70FFCCCF94850C4275F95AE48B60C13048D14EEE232F4227C65ED59A32

Public exponent

10001

Receive

Key

883AFCE3D65FB583

Verification

true

✓

Висновки: Під час виконання лабораторної роботи ми ознайомилися з перевіркою чисел на простоту і методами генерації ключів для криптосистеми типу RSA. У ході роботи реалізували функції шифрування, розшифрування, підпису, перевірки підпису для RSA.