Міністерство освіти і науки України

НТУУ«Київський політехнічний інститут»

Фізико-технічний інститут

Лабораторна робота №4

з предмету «Криптографія»

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

Виконали

СтудентkиIII курсу

ФТІгруппиФБ-82

Стокоп С. О.
Таран К. В.

Перевірив

Чорний О. М.

Київ-2020

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 1 1 p , q довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб pq < p1q1 ; p і q – прості числа для побудови ключів абонента A, 1 p і q1 – абонента B.
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 A і B – тобто, створити та зберегти для подальшого використання відкриті ключі (e,n) , (,) 1 n1 e та секретні d і d1 .
4. 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.
5. 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.

Опис кроків протоколу

1. **Генеруємо 2пари простих чисел. Для абонента Alice p, q та для Bob p_1,q_1 довжиною 256 біт:**

   p=0xacdba6a3d3804d8e25653e440b823b149dc99d81fc5311a9669594edf5e4175d
   q=0xeb0c3a9f6ea3299b25c117c876163da05b68021f4e9d55eba9b8d7e41564dd81
   $\mathbf{p_1}$=0xec797e2ca3fcfc14af302dfe5918aa806c08ae2e03750ed5aa109e3fe393e34b
   $\mathbf{q_1}$=0xfd25231dcb4b14e9b375c72081d65990c0b0a7f371d1d4827e393b9d1c706a03

2. **Кандидати, що не пройшли тест перевірки простоти:**

- **ALICE:**

0x95c3cf5eed12aeb2e8ef782bc4e5a730cfb4d75f70d24ca26ecb179167b1ac4d is not prime number
0xb7a619d4c70a06c2115cbf76d0b2725343385423922ff3f3e6d8068580b7a159 is not prime number
0xacbd3767adf92f13c349e6952abbbd937c59d7c618e5e3fb8b45f66d8ae369af is not prime number
0xb690163314244183459356f65633e0990fa5a12032d6ea957fbcdc3f61e4a54ef is not prime number
0xb289b81255e91e45eb6f74d6d95da98302a310e356d1bf34f67c2d3759a7fc6d is not prime number
0x923c36066b2302e0c3a09971c0beaf2737a43f93c016dca236204c1b32dede55 is not prime number
0xe6da28637d85126046f32604847078446fe0740f6469513b314a0e9390416f35 is not prime number
0xa9b053be0ce4b8512eae0a754fffdf5e3abc60be62c49f18b61ca8b1eefa0ebf is not prime number
0xb3a7681418e0683f950cec1c37f56b456b2df64010358a916fc5f67708b93019 is not prime number
0xe505e74f0d4b0c97ceba686b39cab1354ff915b5ddec4d5776c43695fb4ef377 is not prime number
0xadb1117c984ab1ba33dce72970e1caf3bd109bdf4721aca172cd3ec58c73dc17 is not prime number
0xb0dd13f4019bbe57e10652cc31ed64ebf46b3a1bd34656a909c70d7bd4745553 is not prime number
0x968fd1d76f356bb5a40a7d155b1c2865163dff2473183da6202548dd765674bf is not prime number
0x8d2051b386300f38330d60ae9fa3855ea06654b6de6200fd825d5c0c566c5acb is not prime number
0xacc64402bdab42658970d17be112fe4537a32f8fc5124d52015c853292737ef9 is not prime number
0xde311ccd05e841e03f9a701006182bbc25202e66c57cc657b7ef3b18da678857 is not prime number
0xf02c3a596955fe0cc70a90f598e5b564d89c2b69638c463e7bb9b13bf4f42ef5 is not prime number
0xa47429b7b7c074b0b0c64bc9de0cc6b2bc1ca0a9d701e6fc2928a56883b01cd7 is not prime number
0xfea21d1207fd7bcb2dffb2fe8f1a55c119e41532bf40e07dfe82e8a08722a84d is not prime number
0xbed00f9989bbb18480ffb76394e830f663659f78edaef29b62eca83c4ec325a7 is not prime number
0xf26397e41ac959dd63db1b669b9b9fde9f2a43934c498dd509a5206c986cf9b7 is not prime number
0xdefede9df8c31e990a98380df66e950ed6b8a426e7fd6703ca37921d81890fa7 is not prime number
0x804c989502b7790e60a8c6c32b0d2da2adf38a5d9ed1cb47c38c6ae7e17cd4c5 is not prime number
0xac71dadc10fab23436732a3dfbdaf99fc1ab0ef661168ebefa81f08c632c4ff3 is not prime number
0x8c0bb26425349d188e3e2d60aa0f42852cbf9edad6a9eba0c71bfbd695c548fb is not prime number
0xbb9948ed3c153da34d01f2811ca3924ac89636e337957c206432e0c8348f2b15 is not prime number
0xb23add75f498993b2e0a35e9055764fbd7b4f40da1eff6fac2b1d3f7288c4c5b is not prime number
0x8170cbcf1f7ef11927436589c3ecf990d8d4c5439524dd5202ed440cf9029881 is not prime number
0x98a69aaa2f37055ecd1ed538c0fe7710c3694c35861b310116dc744d18552013 is not prime number
0x9780d2e562a8bd07bb51978090b227d8dac9ff34e83b41f591ec006888e09199 is not prime number
0xc75fab095aeccaa0af1490d7052cfd1b2b6e39eaf0cba002f4b1b489c8ee788d is not prime number
0x97fe62d85d5369ad56a51df967a0fdef694d8f9c65cfc74a5086e33f7527c56f is not prime number
0xe46c85161f60d4836dbb347d830682f9cc3e6544305513fb3d332db1812bc5cb is not prime number
0xa644f2dbf0549794e9e77e6b127ffae17d9efef261b65fb81ad2772a24fa33ff is not prime number
0xf11738a572a174b28164ee326fe70f65fd09e60d9903488c6cea025696bedccf is not prime number
0xac64528b107c57dcca176c7e61460d4a1792b070c4a602468f348027a461ecfd is not prime number
0xf47652041f771ec4617b14ce7de8f48a183972d707c3e0104a7b814d56faab91 is not prime number
0xa0feda4ec791d1f03c1ec6ae8ceed3485ae590c46fe8e3344afe11ce79a9fe37 is not prime number
0xb3e56307f81f68ce0c8fd16d05db1661355f03e5dcbe7863ab43ddd6c9f9737d is not prime number
0xf4e109aa80eeb819eb5fa1d259567060337764b25b7008d04fe18c207fef07485 is not prime number
0xc27addc6edda7b896559c006ee676a26755bed8096b7a5c494fcc2e5c23ebc95 is not prime number
0xd04d32acac4f3a9c76d076421b225aa9272e7b7e341eb19ee0c650ff3f66bab5 is not prime number
0xd07ec3c6613fa9b013d4f5b245b04f109206e6e89828ea0249c8997a6862ad43 is not prime number
0xdc483010ef8a3076f727286266c028311c30de418bd50a75143e326be373e52b is not prime number
0xe4abe9153c39b1a98b87f8bf49fb8fdfb8ea5566b7c26173e8f3e560f87ab337 is not prime number
0xb92631f6990df939e4ff6adc63796b391a9c4243d042aa710e0723b00d4fab97 is not prime number
0xba9f56629d71fb3b3c11c05ae61f72a344e4db425c12288f08e7b5be7201c9c3 is not prime number
0xc4097c0e254d1bf934b709af8fa18edd53a037a87a303978acb3365f30bd0b47 is not prime number
0xe492ff030f831d73c67b8aad4547dffabd6fc349e045db29b45d2a4c18b40661 is not prime number
0xfab0f0c42238a0f4fa62e94e3336673041051ab29d36b4b1b65188ec5c80162f is not prime number
0xb47502b520210334711c75758e82c413edebc6f556e6eaee6448e3d731aca5bb is not prime number
0xedb7ba9e516ddabb5e520cfa9f1ec0b46a7e4b932787cdd73bd9bacf948df6fb is not prime number
0xf4fb59b12aff383c16a790c70d9367251eaba0b36a9eec6ec67dcd3daa6fe9db is not prime number
0xb69a4442c3eb517d3029c7a9b2fe7ebb837930c9344bb942cd10c9105ec39599 is not prime number
0xebd3945057b4b10f671d9af7d2cab00239bcdca593383347447 12a12069193e5 is not prime number
0xfcbc22290b0267f32d005889bf61b1fd8ace8a4afaa6f89b09c68255f4cc15dd is not prime number
0xc0bb884d55db053d26ce9dc4a1ba839f1fb429141f628d82094986cef480c453 is not prime number
0x81d11413341ff1f119be722025e988bd5bfa4c914f31c1246c7a25970806703d is not prime number
0xf6856c547d4fb98078859e25d184d3bc48c68b67efc14aa4c38e54d75357b5e9 is not prime number
0xd7b3d0765da5e58993776057c9b9d243b1f159e7a2a29dcf69915ce11f83113b is not prime number
0xf58afb0c4dbc332b4e3d55a8c99d895319caee2f4a8e5380a817b3d9a4089a1b is not prime number
0xe6fcb26fb5f7e57f687d28fd7d954532eb251dd4267ab310c15b5c40dd6a4c71 is not prime number
0xc99293bae50eba346bd3c9c8bf6d4498622a14b79ff1a5bd9eac4d4c387b5239 is not prime number
0xe9ecf1cc1d2d24d01a1dc2fdce6e18d6e3cd763a7de3cd446be11050d531223d is not prime number
0xf8411e7b7406e11e4eab5256f3dd39d68e1f34c3a768c6ff13fbdec1fda7daaf is not prime number
0xed437eb9a30fa576710cef8bf0b8618e6d17e5650ee23bcbb5f99a098f9b2a35 is not prime number
0xc8bf1f0e37885e2aa58209d8d923d7c81fcc54048dc4f21e13efd096373039c3 is not prime number
0xfd02c390b13ec81c52d136016453006ced054c550e851336ae95bd72cc899211 is not prime number
0x9620cffa7186ccf280403647becc7acec9bbfd33eae60afbd64a08279a48cb91 is not prime number
0xba494ef81f8babd69497c710bf508f4df546bcd285ef85230a46d5f8a423cdff is not prime number
0xac577d16a16e2f60a5de36a6ee067048f7e50f74762a66c192b718e75e1418e3 is not prime number
0xf63aa74865caa6274cef4fad5d12ecd96225608d297b1c9a3f3e094c03a53f9b is not prime number
0x867630cd4f5865ad706eb6b05ec8e69542896050c3e4f5d55a907ac980e86f3 is not prime number
0xea2ec564091ff2e0f06470eb34d3ee774cd165f7699824d7ed4cd02d08060be5 is not prime number
0xde8804815b41e1f7cf3c3c1639ba88f48c296e800f6155d23a5c8e9f2c925263 is not prime number
0xeeeeb09fa036f15b64e326d7ff9ba88aa5cde28bd71c907a980fa1c2885433a9 is not prime number
0xfb86201a231773fda4e82cf6a7b50cf9fb76644e69b304f421d8e0c7f2325e87 is not prime number
0xe0a7db7995c85d4c8cb2e9492fcf78dc73203cb917b324bbbff1bd5cef49002d is not prime number
0xe8b4ff40410264c959a1dbe1f36d110fcfdeb102bc5f5b731a273e3cad29e3ff is not prime number
0xc45942be1b9de5a48629cc3439803563cd882d0687cb7b15ef484233a259ef17 is not prime number
0x9ed464a325df59b3728e758e42137d97dfa4fb706d4df1ceef610a15bc14f1bf is not prime number
0xc56d14721116aba2695f22ecfc2b045af3193edde6dc0a66406e294722870b99 is not prime number
0xa5b7e8bf76a73a71713d0df90de7bcff6b292f7c1976d8865a7516f9c68abd25 is not prime number
0xd35fe298270a3aec84203583b8dcfbfe74f8da05ecbc8041b6ba098a8aafd9b5 is not prime number
0xa08cbc78e307b5698eda6218c25ec0a1e9b0f8ccc283a0afe835bf3a0ed24951 is not prime number
0xad12ff65d980ea3488fa4b5d8e8fadd7f6d4bbe75269abce70eb7a2144ed932f is not prime number
0xa5617ef085c03116dcd7f0343135737b367569fab43e6cd02f1a063e54f16bc9 is not prime number
0xa4cfae9f5c04a8741922cd4807eac6ec33e720a97efef5466a12176f3ac625a5 is not prime number
0x93796c9f8b63d0ce44fa4429b725e58f00135178c6cc49b97b3092bf737a99ad is not prime number
0xce28e4e7bb79c207c29e5654da23130cf04a8d327b2936cc026eab47c2feaf5f is not prime number
0xb19b52ac4e3f6d2dcd81b438e1c6a5c214ada5bf80f4820a709cd4e52f757b85 is not prime number
0x9c9da15f9b9c47689ae412b77d293a57340510b6ca530459aff2b3ad19922e33 is not prime number
0xf3a7a84c92249a2e8a62bf79ad7af0aa5c6ef0290181e0f7080f79b563d79a47 is not prime number
0xfab59e03464fbd45a32bfe7d119c0bfff65ced728d4e281db2939cab97d71c39 is not prime number
0xc45949a762e113f9119f54cf52901e8c430dc3b69e6b76ebf0914a1df4f47fb3 is not prime number
0xf15a1f9a6bc150ab3afbc0e4478a3da7957207b5f6316e31e2fc8f9b218cd65f is not prime number
0xd28e59a3a6edc01841855d20f886611da107fb4c29ca90d3eac3bb5facb2aa63 is not prime number
0xe3444252f4ca6e80aaf2c8891e0853543c7600b48af0374273f9c198e919a27d is not prime number
0xa1c8a36ca15d0ab18d7833c300b81878113803cc308ac47af93eb574f8e8d4c3 is not prime number
0xa5c83c0c1d005a6b330fec03886050fac793d7caa01eaff4f9d5c27b6f3c4549 is not prime number
0x90b912b8b3aac77b0223e35f15f51879be370c45bd1c4494125dff91b32e18a1 is not prime number
0xfccd74a0b6422cf7dd96241ae4fd901acc8afa9c089c527a40eaf017c68900f5 is not prime number
0xbe6137905a50c00fc64bf825ce1f2c2adc01631243265cc9ecfb6c2ecfe59429 is not prime number
0xfe2b07a669dde8f25f542f1f125ceeb335ddc2242390e9181ca6a70f82eba675 is not prime number
0xc4bfe4eaa73097e446f6e8dbefc4e1a7c876bc8191a35159b99746054244075b is not prime number
0xb5d294e9501fedde1b76f0cec64a01c7b1a223f99aaa5e1cf56c724137757757 is not prime number
0xce347f09b7570faf73ba2538aea52710022e03fcff9b5456ddc2bd1305e4f43f is not prime number
0xe6316d42d2abd1f2bcf112be99f9f3b22ebe18132d1dd4d50f1811737e1cd091 is not prime number
0xd9e566cc42a4be45e06130b6fb0bf731d07556b9fccdbdad7e734768d6b76ca7 is not prime number
0x93a054409531443b74be0fe11110e168765450b93889e93f88437cd0413b10c7 is not prime number
0xea7530ff4c8073ade2fed4b964437af74aa6c359930abee91348b743b2190235 is not prime number
0x95e7cd3946c0a30ca77cfa16f0dc5ec42b61902f5a96ef6154c0dbe94bb6864b is not prime number
0xad447a499f1d30bf7b98dd916b13382115235874656e7c7dea2b5e9c90b28f03 is not prime number
0x821c7a48a53f0fbeecab6789443184a4898fd31395415191376bd3ef425015b7 is not prime number
0x9b7b42bdb93d8c28612fb6c3391ea19ffb8554511ae634c1a38b035da6288ab1 is not prime number
0xd465af39be02f6152da3d51b7bc2c46731cf367893824de113edd2fd4951dd15 is not prime number
0xb0945068c10b897520b20d66194f8308b66c02481db082f686761707cfc6073f is not prime number
0x97229af83c480b68aa1f753b197bb5d6da5f86ffd2749b9d402c22b103415b4d is not prime number
0xbcca8a3af99746afb9b93c62db4148720a784d0398f225015dcf7de1305e4943 is not prime number
0xe441566a50f8f88d0f36fb7efcf5a375d85fdd888a7b479708fd9edb0c5d8357 is not prime number
0xf2de99f69d55f13f20a7dd3afce807dc91d03054bc940ef0cf3ac8e17469c9f1 is not prime number
0xb36a00dfb746742e6a35c0e8d64a8ac0605204dde4249a9b35340e963a3ea3e1 is not prime number
0xaf396b590834100913507d8519fb62b09eadc7c332060ac9ff06fcf4b822a3e5 is not prime number
0xa6b83439ea6909086c94459a7d76e7301f8985b967e6db677e0dc80dabde6283 is not prime number
0x8f31e3551994ff578b350acab6b906c9ec5cabb15025be20c1d2bdc5e1a5f3e6 is not prime number
0xd5f7a6c380e007d4ff349e3ac7ae2657ee5bc0ddf91338f333dbbc7f66067ddb is not prime number
0xf17c001c81f3ce191c7eba40a183d18bc48dcd2332b19c5a0f4f62e885f05aef is not prime number
0xbfc14b2603bbe15e767e44a0e812d7b61169c7f51a1d28f92c5ceeddbdc231fb is not prime number
0xf30df203acdbe0c743cc07d6ddc42d56f424dfbda3d456e0070ed9a35b1a695d is not prime number
0xb641a1c16990559b329c7038cee1f9fddbfc4082365dfcacd85f75159f3c4e99 is not prime number
0xaac9a8c375627242b815e57499700335fa7ed23e500f585202b17c0b29854661 is not prime number
0xc6c0e3082ccc8898fc5565f8c26b86f01795989d4b4df1a48ccd3cd8787d2ecf is not prime number
0xfebc207fc85f7993d0093d650a1cbffedf27a56c6320a1ec2b902daf1cf9979b is not prime number
0xa634dd130a6b6424a97d4b98048803f5a45e63509f82cf294ae5b1790de77b13 is not prime number
0xc31aaff4b69617c5aac6e49c560a3dbc7cf088106a43d6fd08bef7f18dc85d21 is not prime number
0xdac3e67fadd729ee945ebc9a1578656c0989df49b58dd806d5b43aa68024ddd9 is not prime number
0xf1873498474ef9462dbcf6e311c66d852efc6ed83d2218274f2c18f62bff5eeb is not prime number
0x9a42723996f506bdab3f773a9d8dc20b99a7227bc417ab9904c671aadc72dd39 is not prime number
0xde5066a8c6fd5f2b51da63277dee3aea62e78c5718bbed7160f195a78ba7b85ef is not prime number
0xb3c999022162b4777812ec9a9122933b3639c511ab81be3fc1f4616f65a7f3e5 is not prime number
0xe9a4fccc93ef0090d6f0898df1ed5ccf16d15288ffc56372f0feca1178ff7fff is not prime number
0xb91d92b954e50c628a4f053963f9d1ea9de981d1c52276dae769d719c3e4ec59 is not prime number
0x9bf7437ec21fe6b73d6503856c972a5c8afc19da4fe870947e4713ec6af871d3 is not prime number
0xbaaccb0c85b88e9db6102c67b8dfb73bad9549fd44492e5553ab968b09326569 is not prime number
0xb3633c727a7301db0095385326c39f11a86e758dfca0d514abf64d95c29efe1f is not prime number
0xed4b5d41fa5115b3729b9e85569046d8207846dbbbb916f5d21d69980f0a1d09 is not prime number
0xbaaa8334a776580ac2736551dffdc54f6d704072c06cdc2c722de28a139dc98d is not prime number
0x938726630ef8d61556017239b59edfed1a3a8f32755fba42d166cd0720cde3c5 is not prime number
0x8d8249af9e6f72414a8b3b5de76d98003be7e429adb95ccc6ae8d774027aa4c7 is not prime number
0x84a52cbe5fddfe0976c3fd9a9e1c763b1a8792e43559c78d7c9484fbf9e04f3d is not prime number
0xb5b052a72dcdc25493ac6d1237bcb9600d2fe27af83d76d34327f1af80a21475 is not prime number
0xfbcb9968aed0b2f44e62dd7e4515c93d4cb8a2a1bbf27581dc368cb9884ccbfb is not prime number
0x8660048fff23947cd38d43a870aa7e02749f2d26aea211626a904e039653cdcd is not prime number
0xb7b02ea1d165e39325dcc613af3305603753e6d628c139fc8f93c995dd39f21d is not prime number
0xb3d21cd3097610462f7a054e4fc97dd3ca5ab4fb345ee51edacb0cbaba770e49 is not prime number
0xdcc751ca9d0df511905e3e74cd910fbcd93aac8cd7a2bdbe8c9436dd6a589e0b is not prime number
0xdc2f206a06887e9845f00f7e680f898ea867ab81714f56075dd2cc1dd22f1981 is not prime number
0xa4bf0c425f723a57b563e45a0020948ea05a5fe39b4559acc6d7c4773a4ebe0b is not prime number
0xd424351da7dfa29c7488682bd25441d563f9ad1e6830199efefb4ea03b7c15f5 is not prime number
0x872117f761212b23aa4ff29279dbbbb298c307028aad2b222bbf4155e2c2929d is not prime number
0x92896a007056f156139bc93dc0f463c60c1ad587a87e93b6182372dd4e7b0e89 is not prime number
0xf8da909b34621fd0e2e4439e269954576503d918d513e5eac895bc15c20b73a3 is not prime number
0xce5d55d6b3bb5ce3bef6b3470823ca63887f0526cb11692d76b39be162512ea3 is not prime number
0xbec9ac3643f5696a56b9a7248cb9fd413d84d562c0959d81fecae1a65ac02b3b is not prime number

0x9e07ca5af61e2c369ac4c622c6f43bb478ce306fde3fc5a4b8d7542862287f65 is not prime number
0xfdd93a8a036c3e880846802eff71dede35cc2134b1289a1925dc70aa9793c399 is not prime number
0xd84bfbd29aadb07dd1b5a954a61d2c92329bcb9b1e840a710f1f46995c1db5e7 is not prime number
0xa244cf9aa3e5d14c8fecf0fdbe54ba9abc646b298add5fb0565cbedf69672511 is not prime number
0x9081ea66aa6e92828cbcebc686df9ff49c2bb1821db07c653bbb1ab4e86fc927 is not prime number
0xc5478d134b07349aa8ffbe8d6d6b0b649d9f52dde483c7cd07dec30b47f46b69 is not prime number
0xeeda99e2038a42b86c845b349bda470396fa6f21ceff0cdec26bd3dda95c0aa9 is not prime number
0x9cb0f7100f77283c4b6c1daf0be2f657da022717e369e1c4be4cfe1c15631f6f is not prime number
0xdf18358bbf4f0d8e9e91c35dc348ed82737681411f403d5e01864de79ec8e0a7 is not prime number
0xbce2c6c3eea375b3e745fba800fbd4f2c843e2a56bb67ead5e751ae143ab78e9 is not prime number
0x85637fbb6857539f56509692add26b060b7aff95f3c3f6c341c6dc4c90b8d9c5 is not prime number
0x9c52d153558c30178cba490fcb5dfe7df05c3ef9d6ac11cd3759787a139a2741 is not prime number
0x8a81cca06684dd1f20022908253265ba6d9d7d18c2b0c0bf332ef376fb84161b is not prime number
0xf263828e21c4b0be1ef1764b9105dd466a8108b25b8998ae98d6fd9922b62d2f is not prime number
0xf5bcc8222be6d4c82f2754e4ab9ad337af7ff8e38c16e78737cff5153d3c8157 is not prime number
0xef0d4fe0e9989a54b7e389bc700bdb5d5523fcbe9ea01a01abd0c889841f5f7b is not prime number
0xea1f6a9c116a70f8f446fdd667005f30f8e6a907c418fc7dcb8fe5185a1464a5 is not prime number
0xc76b5c0ec7a6d6a48640fe4134dea4dd6c7f565ee3b61d991dde1a1eb2fd4cff is not prime number
0xae0104f3c5a3562c5c0c897bcc9c7f05eab0f6684ee1f3f0c381748b662f248b is not prime number
0x85fd4d333de790076d698e2df1aeabf2d77cd797d4bbd8c1cdfc52f57898a82b is not prime number
0xbeb6c6af9e28d3426d48959386312ac68979270275e568d51e01011 16ca81ad5 is not prime number
0xdd7dc49137f592ae4c4bb02f19e36a76dbc2ff069956741e0585ef79f5f5da1f is not prime number
0x9fe8103798d3d209cc29449f627f735024679996ea0740c1e848e11d2b7198e5 is not prime number
0xbb60fa65681caedc278d200a066e7a2d257cab267793fbe92366d84d079439d3 is not prime number
0x984bd3499ad7733e0150ad67fe6a90cdd5b99f47c2628f30f147b4f49eef66b1 is not prime number
0xb7e961963ba8c34f5d58da32d7f40d1eec472ed5eca99df037bc2c1771ac38c5 is not prime number
0xed05713477401dd170464b33b3fd9680775ff892f0ab93e05a0b262b8036788f is not prime number
0xb787adf9499a3ea267746ce53d66edb90d3c73966685339483b0bdf734597a8b is not prime number
0xaa6817e58ec2075d46335152a16adfcd7038030ee72d9d0cf4ece006de52cdf3 is not prime number
0xd09363c4d1249dfe785e10532ec7aff7d61477b53a0a0089261e3e0d2d6bcb4b is not prime number
0x9e1fb15c70875877ca8062adbd9e2f2669222ee53ad034c5461c7e6b199a9503 is not prime number
0xfc555563026b5d3bb7c1f173688a7c20351f732a9a065cdd2fa2c4424a558659 is not prime number
0x8444271bfd329a6527749a57909540389d010c0ca7195d19abe35209c7eda3c7 is not prime number
0xf904ab67a59b15ce6432ea85b4977ff4ca86e3058c6d1e8e855e60728e003d73 is not prime number
0xeca55997b018be098f81b1fc8e24f92d578418b3e029f2b0ce3bbe3952957305 is not prime number
0x8cb2fff0954e483033b88f7be81f7616844765210570 0cfd034f4c7c2c5b8891 is not prime number
0xa39774ac09abe24616872118f761e436f5cf3b5d763136b5b691eac14d6dd85b is not prime number
0xa477e624eae0c4fb1987a2448b711d5a86df8cbf8cfb89b2eec7671e1990f247 is not prime number
0xa8997e63dac6557ed0bed1a2d720f916c04fe80dd15ba5080c6759b9f9ebff65 is not prime number
0xd26f79333c6da063befd23f54436bc8bbc84632b9351f20ccc90caf3845d30ad is not prime number
0x9a6de367dc7cd225eb9b6161694398590 73d86c0ef0736282000ca707801cf57 is not prime number
0xae990249d483a71b73cb42d41f977ace405551857e64e4b873d412fd81542133 is not prime number
0xb868a333d7a6bc5f5c56f4f229b98fe865c676be441efbc6d8d5d1ab575936f9 is not prime number
0xf248f8cf363c5a16a7b9ab8d083f8db8ea2fd657fe16e3d3667d89b7b0dcf525 is not prime number
0x9b561957733057f30499f9e10d1dea47a4d5b76b0f523b433f5eba51cb9360de3 is not prime number
0xed15baa630da3bec9fdc881fd92d36f73444cad99a906d5423a074e478650dcd is not prime number
0xb20ba7bfc2b15b8fddf85464d1f458fb6542e882b4ce5b80e1befff4079983f3 is not prime number
0xe86b4964913dc6801227d4020a4892792027d6a7a0c3e2d210d9ac1ff31a12f1 is not prime number

- **BOB**

0xa0d6ae2a92a279d937a14bf395dfc6918020bd92f337d12c82a469fd4ba887d3 is not prime number
0xdb64c91a9d76a2529af6d881a845dd33ca62682072ef799ee09d79879ccd7965 is not prime number
0x85623bde2130f0392819d2ebdd27baf2b9ba490970ce416dd20358367c226f25 is not prime number
0xa6a62bcef07007b2b933a386c292286f576fe4ea34cae7de0a383134ba319b97 is not prime number
0xf2db018660952df8e48d2577f6d86eed751bb57969599b62eb39ecb00e45c74d is not prime number
0x80afbb9b18c550e332122473d59fcc0a37c784d47cc6d4bdcf21411bfe80ed6f is not prime number
0xf5f46de5a10c8e0b9de4e02cdb9a139d82263d4b58c96b9ba2a5cffbf8cac74d is not prime number
0x979f10fdac3c7893baae532e4d8f250589060bb8e7947c48d6c4b9b8e1f7f41b is not prime number
0xd447b088a7c80ab9fca462b853adc12c106f1076d9df5441bc92a609012db89f is not prime number
0xcfe954a594d9b2dc69b8c33478071c9a96bcdf41f4355495c8392d6056e8e3d9 is not prime number
0xb3f4dbeefcb32245813cdc282493e8a312e1891ce7f6c21bbade0cbbf3386685 is not prime number
0x9085bc658531345f446a000b34fc297e9f7d8155fa1bc3979ae02a0dbcda10e3 is not prime number
0xee57a2e6eff0fe73bfa98e3453da6efc1d8108df5dd8bdfbbb36d443390c8629 is not prime number
0x86df1a73fd4be9d3716ce16f5a0b059b808fed5f04fcc5486b3dcfe976f3e9e7 is not prime number
0xb05cfca30188a076bd440effabd90007b98b3060451fb75878d38f23c6031969 is not prime number
0x8d045a6fd938c0a9a391b6517ce4bfe05b845fc1511a5c1ddb7863802a7bf855 is not prime number
0x9204d74e64295e61be2a1ff1356f9875eb70edaa18a9556e102792ad1f91b5ad is not prime number
0xcd4c929ba29662f8ac318edd4ccb151deca0c2b172437e737393794a9c4f88b3 is not prime number
0xec1c35b202dab0ea4dcea84efd0ae67429428d7e98d905a3e34a30bc756ae8ff is not prime number
0xf44ed750ceb7add6e80be15f526abab5e3e03ef3706c13f3231156520233a9a3 is not prime number
0xb2d305e652e55e80b290d7bb61882c734ce09c28707d4dadaf4ba32e4b75139b is not prime number
0x97ccd095399c7718d76d05ed8fad2296f126a2152fa18f428ceb99984ead09fb is not prime number
0xcee5e1455af1f63f76e1cf27ef80a3d3b64562669038d1e6275d600b535e1f6b is not prime number
0xb7fa744739bb3654514fc7ffd973420b5f9635fc4e468fb9133299d8760e4363 is not prime number
0x978c83725c4269e20b2a1387a823dfced45445abe2e6b8c47cecf36d87b2e491 is not prime number
0x9a71976375182c9f607f5639337426849e47afa3e3bc8221668c1c8876e0e66b is not prime number
0xe81b1e42a19f09195c0a6173966c99e5c9c3964ab39fd256d95382db8c3870ff is not prime number
0xe7e2a2ed28788d0a7369b89a45634df8828604083fa7896a93d297832307406f is not prime number
0xdb20b046c7e2c624aaaf4baf9f80019a12987c01cf82b6bcc2ec15bfb9b1782d is not prime number
0xe7233ca708413c356e2123a2b3197f7ff4f259d02ca762b34a7ad48a14491139 is not prime number
0x9801f0bd5261ac534d7c4a826fff0a7a4014f1d1d13d2da7ac2e4fbad493de6b is not prime number
0xe31d3a6017a471192fde94df380db315a4391b87fed76df632244ab0e124abf9 is not prime number
0xedc3753ddf37b27d27c54444773c556a24ddcebc1fcd6cdcadf3f35797497743 is not prime number
0xabaaabe1fcacb2fab0419b8b49adc2eaf9e971aafc9369ed495d96d93a2dc78b is not prime number
0xf13dbc1e34fc594573c9bc69b289c5971c8bbc81bdbb30ad575eac85d76f3dff is not prime number
0xeac5989ea4e993a09399c6800f45df57cd12cb42c02f10cf5f00a941510ddba7 is not prime number
0x858013fd23fe928620e569c706297b26253a71c5ae1499ef23e44f761a3721e9 is not prime number
0xe226df070c4596e3ddc526de741f954b61a5a78c202fe102feb4a0b6e7aef8a1 is not prime number
0xd8e9189c59554ef44b82a254554e63ff890a4f5dc8bbbac69f890fe7c522e65b is not prime number
0xb2eaf7277f5cf3cc4da84f95939be5155d27c16431d835904a014853009afe89 is not prime number
0x8833412442c06729a5729efff6bdb4b85bb9c51be4adebbf9e357bab09b15c2b is not prime number
0x948c1511d084d9d7d3a66a82bab59be04578380fda8e52ff26627475149e3e91 is not prime number
0xa1508a27dda18a28c502d8c9e3379db66678fc87d14e8ba039d7332bbf06e407 is not prime number
0xe288da887ba1aafb2c5378b13e0372d358e335447a07c9a967427ca27901bfe7 is not prime number
0xf1e4f31102220f5dc78aa7d6a40eec1f7b04592d14dd62c8f0a1ad5e0850ecaf is not prime number
0xb02072fc5afbf17327c01f892761ddf3684d2d5d6b8e3980f240c92fcb593db5 is not prime number
0xf04db682eec0038077fe5cf45264d1ef9cb01d66964a0d3199bad7e048dab537 is not prime number
0xe978314d7a9ce6900904da66c1906fa808cbbdca850fd9ee494599f98edc8909 is not prime number
0xdd82f3f4a7c993265e7d7b9a4c64b6604903c63a37027ae2b34f85425a1dc0df is not prime number
0xb5b711fd276534f9e2bb4f9f8b6e34281476aa8f1e821f68f58e880a87e556fd is not prime number
0xe4b04024331eb957a38fa776240f51075f29cb07af82d11ba8e2d8d95fd4cad3 is not prime number
0x826647123fd67f1da1940a358cf615c3010ea015cd17247f911f8949f7631ca7 is not prime number
0xbc2de3cd6cc04612e0ecacb4c8cc34c285b7cdf1fd0614828885635037 9d1173 is not prime number
0xaabc869d5e0095b455966abb03c729b34f5589280d8c44c839f35ef852115231 is not prime number
0xd5ff720d6a437e73b6878c832f1e81451e48f7082cfa4c56fff215a47efc868b is not prime number
0x994223b697542ed248976ed8324aa9c11429bb55fd64b399c54542f9c6c0195d is not prime number
0xd0f07246a177a5da4065bf15cca72bd6417281f473d1699641d0cc8b365914ab is not prime number
0xbadeb2027e3d1b848b3ff01319377e85badd023a91e39e7b4ab332a950e2c4eb is not prime number
0x88b689755ae35695e8e01c1ceb43c140ea5773cbf43208c59ade3b821e674575 is not prime number
0xf706604b4f0a305af81426c68b8d7bd31982ed6ca409be2283bf845c59b90a79 is not prime number
0xfeb01ab1ef9fdf43c7a7ce956e53e633d6738f05eb884ca4d261fb398156ef81 is not prime number
0x9d6fa82e701fbaf0db9887856f49b0f309f2f8cd1fdcd53254ee4f41a3f8b10b is not prime number
0xb6573e3231d30c40d8ef8c3c44da3c7bf7eb52ef93adfb4754d27330900afb47 is not prime number
0xdbf62752c34fc81fa5047a5b9309a7c310e158343215a2f2b1430b2b1fc0604d is not prime number
0x937d71395424cf6a73fabd8d24c3973dea322786bb19d25ae31cf83beceadd33 is not prime number
0xa971d52f3c85971a98b66f01d957d6e2ede5119b7a1c864b3c70d77c81c2430d is not prime number
0xa245af2d908c9420b205b5db2a4dd9af698754d01d06e64dfdb4829985e5331b is not prime number
0xc97384ff2e9b33f21dbbc2caea36b85663ceef57672e0ab186fe62cc88f8c4e3 is not prime number
0xc5f3ddf03c2228072de87d9a83f0f5934cc25516414d089434093e42c86097b5 is not prime number
0xf277b116cfcc8adecc6d92fea6444bc20a14e977914b54a420029eb2d7bf9763 is not prime number
0xe0de3245e14d08b8a7ba22b6cf81b58e65425bbc6b404af5b6291dbfe1a0fbd9 is not prime number
0x9acf67e0040446dfa89f57a055033581647506e40048d42c9545b90ee813af39 is not prime number
0xda62ad2cd853fb57299bb9bb666ef3f371744b7a0a8a5acba20798e2ea577c2f is not prime number
0xf6007ef83cfef53805365ef631be5e6df0412d973b242a8ac4672aa24018113d is not prime number
0xfba26f3aefd8842566ed04cc08875a5d6f90486175d275c63aae6d1e9d22e187 is not prime number
0xb9f8ac10502c79b16dc5a31788961907beef7693c9d24050e93997aeb3540147 is not prime number
0xaee7942535b2a9426c062550c79fe2976ac02aa75da546806171a9ba71bd3a15 is not prime number
0xa31c070e2e7d6e71e882084695f21bb639d011313b2ff01ed698f6b62ea6c5a3 is not prime number
0xb529d787d0a873431ca8f0e48e0e5edaabd199e68c6b5e35e8170b753cce9d49 is not prime number

3. **Генеруємо ключові пари RSA для AliceiBob, де(n,e)-open key, (d,p,q)-secret key**

- *Абонент Alice формує повідомлення, використовуючи функцію SendKey(), де ще використовуються функції Encrypt(), Sign().*

  k_1:0x63e1da0366e5b999edd564ca0a520a64300574bc8aa1a66a0013ceb0e53cd2849478d9777e4e1ea368cdf4bef3d88c9eb45e1d256b3a9ec9283ebef5491efd74

  S:0x49b65bd0180ba94c8802c5550d8523157f142a33a3eeffea535ca321d747fb565ac0d77441b5a4b9cdc6883a3a31c74c753062b31e3a4c31d17dd0552a14c222

  S_1:0x8064176cc66762565fd484cfbabf468482486a769519cd2e8c28c900ca2bfc868038b2c280365de4764e9e9787c3c9eb63d75b5383843fddda066a1352024dff

- *Абонент Bob приймає повідомлення і за допомогою свого таємного ключа перевіряє підпис Alice.*

  k:0x4b7b18d443e25439b0192f599f33f13e72bab8460c86fcf966e2b549a527aebbe79c03cfa1cfb2519e525430109bd73127d3f51b9a6cd394c61278efa6feb842

  S:0xa4b09bb0270af652422f71ce71c04570e911dc976abdba71d674154c34a710ab7f43c6935e1970d940bc1db14f04c8a91b4d1062c3ba1049c35a03ad1a7b5c3

  S^emod(n):0x4b7b18d443e25439b0192f599f33f13e72bab8460c86fcf966e2b549a527aebbe79c03cfa1cfb2519e525430109bd73127d3f51b9a6cd394c61278efa6feb842

  ***S^emod(n)=k**, отриманий підпис правильний.*

Параметри криптосистеми RSA для абонентів Alice і Bob

	Alice	**Bob**
	Open key	
n	0x9eb5e3d99db6dc6dfc9d1f7c02cf60b550acb824825c298f1482ecdeb1aa15e012a3154418673c98528281811c34f6d58c8a046de5869bbf43ad2606916f0edd	0xe9d65fb17c51d021c5920ada11c159f925b82977cb34ec4e8a3c40dd960fb3a77c6895f9d8967a9fbdb19e6ee80d0aa83088d0c9e20ca2044557ba898ba8b7e1
e	0x1937ff2f1beb4c688cf1bfdb213a0c05f798969b89d1f40822d26ac1f4e4bc0b289a708fc3c91606900804ba027eb031a60a03cd52c33324620af4db5362fd07	0xabd4a0fed56ad78cd0f120384b7a36490d84098e19e113eba9071b050d3f18cbe7584d5cc3c615233f09300a69d52f860698d138b4a9226a7ebf2cfdd748da79
	Secret key	
d	0x46ecc1bc0cb430d9d5bf8473da3f41f56d9136dbb9262a890722699ce206d517b0b70cbb4fbab97f4cab990e0239683eaad293433df651d5b40447b9087fc4b7	0x4a7c7f9f3cf1d056d86e59d6df81fe77fdd37ff851376769941b137b02d61077cda4447348caca54549e04dc590e9bbebe80833ade06ef77234371a9520433d
p	0xacdba6a3d3804d8e25653e440b823b149dc99d81fc5311a9669594edf5e4175d	0xec797e2ca3fcfc14af302dfe5918aa806c08ae2e03750ed5aa109e3fe393e34b
q	0xeb0c3a9f6ea3299b25c117c876163da05b68021f4e9d55eba9b8d7e41564dd81	0xfd25231dcb4b14e9b375c72081d65990c0b0a7f371d1d4827e393b9d1c706a03

4. Чисельні значення прикладів ВТ, ШТ

ВТ	ШТ
0xabfc3834e92a7abf1f1b21c9f38ded97b4bd192ff765116f45a8aa625f68f018bb8c961a28eabe65752c11d9ac6f77e347dab7306e7f3c53e19e86a7477c569	0x63e1da0366e5b999edd564ca0a520a64300574bc8aa1a66a0013ceb0e53cd2849478d9777e4e1ea368cdf4bef3d88c9eb45e1d256b3a9ec9283ebef5491efd74

Цифровий підпис для Alice і Bob

Alice	Bob
0xa4b09bb0270af652422f71ce71c04570e911dc976abdba71d674154c34a710ab7f43c6935e1970d940bc1db14f04c8a91b4d1062c3ba1049c35a03ad1a7b5c3	0xa4b09bb0270af652422f71ce71c04570e911dc976abdba71d674154c34a710ab7f43c6935e1970d940bc1db14f04c8a91b4d1062c3ba1049c35a03ad1a7b5c3

5. Опис кроків протоколу конфіденційного розсилання ключів з підтвердженням справжності, чисельні значення характеристик на кожному кроці

- *Згенеруємо пару ключів (e, n), d довжиною 256:*

e	6ff54717ec39a2de7eaa643b7dd013d2ecac39b6ea0bc90b26e14f5b1ef1a317368ec11a500f57f3b8c636c281473282fde611e74fe423c940550ba45e4d8f49
n	ca9affb4878a72aecd47403acca994396b1c5801bfe39cbbd531bfbd5ae6fcaa1d6a52caa63798c90c36eb2fafb82fb078ae2d64a8b23e0910fc1c977b3c4cc9
d	48feadec6d0dd8167be341d9771c055473a5cb757c3634d24ca227ca34373bdf2496f7bf2eb42e961c6077ed62f335bde6cd0ef06009fb6d1777ddac454778e9

- *Надішлемо сайту запит на отримання його вікритого ключа:*

keySize=512

Відповідь:

n1:102899124144368114935777188151737301657485118313575615897843127188052647435841018820541161073312840746593026636281731265774981941666337305904505618953020 89

e1:65537

- *Функція SendKey поверне нам значення:*

- **(S)** цифрового підпису ключа k = 1234, який створено за допомогою нашого закритого ключа d.

$$S = k^d mod(n)$$

- **(k1)** зашифрований відкритим ключем ключ підпис k

- **(S1)** зашифрований відкритим ключем сайту підпис S

S	89e124abe42daf8dd47d38dd34eef4f053c89cfa5a21c14e457059b6971a80395c3c0ee7c62600e2158ad141d740b4428b3175c6972d0144dcb179bbaba6b1d9
S1	16c356abd35e1765803a9ae1f08660f15d3a0339c57af0ed69952c93a2c93167201923734cf31945d877ba44df9e355c8eaaddb1476f0b0050c131d8c292ae4e
k1	18d87c963cb6f6e6af705ab9877b69d7f3c92aed28e8c680a231d36896d0ee46b1ac1804102497934d1f896fb0610559d8231bfb5ce677e7534b09d7cf404e62

- *Введемо пару (k1, S1) та свій відкритий ключ (e, n) на сайті. Дані запиту:*

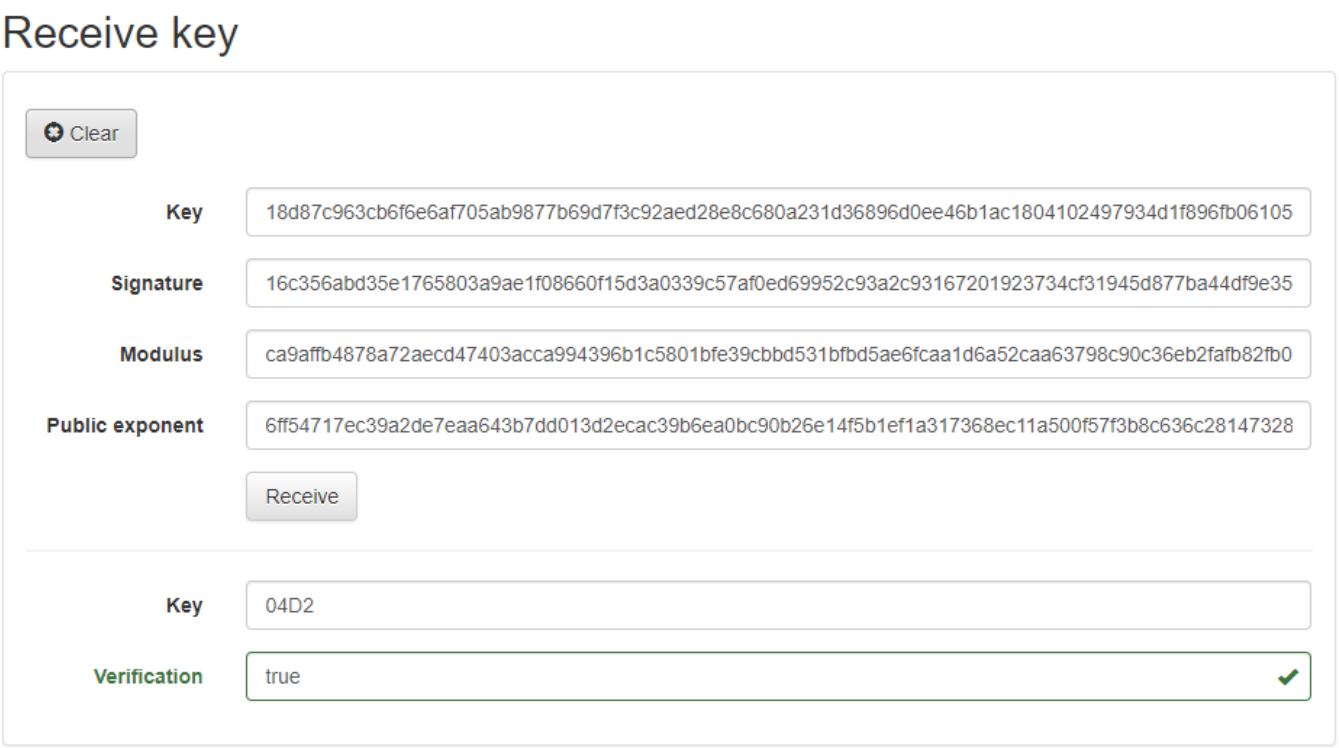

Figure 1

Висновки: в даному практикумі ми ознайомилися із поняттям псевдопростих чисел, тестами перевірки числа на простоту, був реалізований тест Міллера-Раббіна. Також практично реалізували протокол передачі ключів RSA із виконанням функцій генерації ключів, цифрового підпису, зашифрування та розшифрування повідомлення.