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»

Виконала

Студентка 3 курсу

группиФБ-83

Бондарчук Ярослава

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.

p q що не пройшли перевірку

```
0xbc7db8b002f36a9bfc0cc632a395c2baec45fafcfb5e67705551427bf181d658
not prime
0x66196c2a04aec5beaaa7a1d026b9285bb3ca78c9537d303a1612491251806269
miller-robin test failed
0x3ad829070fb0276637c7ca2687d51e59f8bfeca62199df6c39f68f94775fc8d6
not prime
0xbe1962addf80f22222bd665e647325848983ffe478bd501a5c6e4e4d848c464f
miller-robin test failed
0x597904e30a4109bebf987c0d99c2d87a64e4d5929b6c15d7e170e909a69b7471
miller-robin test failed
0x7b63b9710ffef926d1b8e2da1a8617b5399e0a428a734edd4b8a4e09d80ae340
not prime
0x5cf389b24ca18061c68b758a3958ef59550aa2b90f2a8c2effc7a713dc43e4e4
not prime
0x8fe39c0e69d3ebf4e6106db328705852d65925ba191a79ff3b53a27a68021d98
not prime
0x7fa7221a9793a471806fc917f886f51e99894da8f341335d018c4ff1a2309d7e
not prime
0x13d0a7024bed68319dd831b7b228e29548e6061e6e042d4ffedca5c2739795a1
miller-robin test failed
0x93736057ac6800093711095082a1ae933e7e2ad8024b756b239660fc22831dbd
miller-robin test failed
0x6bb2ad6e9a678e5e770cccc1d1d22f5731871f4a3bcca91ca587267a93a281bc
not prime
0x1117f5b0fe3775acc92cd0f64f367fdddb722f745d4d033f6c6ba96ae9ba63b7
miller-robin test failed
0x67719f6697bc2903e62aee1876e4f2955caebd71a261048037d2c4839c32d1df
miller-robin test failed
0x6db55b7c241e1e7afa78a1a7358722a48fffae86006656f2d2a7dc7ca1aa5466
not prime
0x734114c6d78418cad4c4612f1f727081bf8f8e5771fa74a2e7c7d846bd7b7ba
not prime
0xfc6360e55ae8308fa3d0b1aac9be9c033a132123688a0e86d91440dbaef9a2ef
miller-robin test failed
0x9df0e8b5a5cc5f1a3bde8977d75aab086383ef2003a5c7ac2a158b93985c7bd7
miller-robin test failed
0x72f2ac49776a7d5d21e9b779b700382c28eec42c171a90ec53ce5c438c0d10f2
not prime
0x172ca8e49c25c6dd5e6fb71ad6d646c6447a6193cc64aae5377a11b7929b7f05
miller-robin test failed
0x333dd3d8f81d29155cf21bd9707e05db69ee42ab745153ee7f8aed2db4d58bd9
miller-robin test failed
0xf99b495a362e89be73eb8c8b397a5e1d72daedfc6ee754eafe92f14c62c76b9e
not prime
0x42325800353ab613f35819b8b13acbd9f7519f0f6bd640e6bd43fcc5fcf48c97
miller-robin test failed
0x897655838bd5369e391569057fe9121c90a2b8b02c9f6164c1c5907bc535f450
not prime
0xb115a00f3b42c2a21b6123d91328f0ae6b1fffd64aa9e5e7716418ed02a35034
not prime
0xccc398c4dcd542a1884c75e1435d8f8975f9c79bd619a94f7d60a741d6e646b2
not prime
0x8725a5abbb5e6beb445f65bca69705b0ab573221ff61cec9dbfb8971f6dd4fb9
miller-robin test failed
0x1d71b291b603cd2c173e043a84a7c571891605ff9a510edc13d88d4922d4af4f
miller-robin test failed
0x68fcd0d1a2ac6ae0f7637cec42b12cdc8f8c2e6c4ed80759dead3d649376954f
miller-robin test failed
0xf8b923da457acf9d30c6cf9a1c7d73c5a0287ca9ed74fb5b8bba41add87b7f5c
not prime
0xc4a908905d9329c9d9d4d53365f8b64599485acc2452acb5f8c6d76ab748339e
not prime
0xba353c05b864974cdc09c145298041ad0f23b43a1876b2b14083bfa09be447cc
not prime
0xbdc38d43410c7abf53db6894fa6a185b07c47c371904a759810032d9579f7c01
miller-robin test failed
0x33f99ba4d62b816febdfd18edb19779d5b72b37a3884fc998a2e585a557ebf4
not prime
0xe6819799fe19c1f27c5f38c8fafe4513102b987fd06d92ac37d50434b86154d8
not prime
0xd4abebd4adf39a3178814d80b24c6bc60533c7af85126cca94255af0ec300626
not prime
0xda878315236b9fd00c8e3d44cf7f83c00e0337f89cbadbba725a4f17ae7b12d2
not prime
0x771f63da8695da2f49710f5d8c9b72b789dacca7e20d7a9e459c68b58e72bfe2
not prime
0x6f6623398ab687537a4571b060c6d99fe3969f6c546c9d23a76eff5d86a87c
not prime
0x6a4c9f9e27c7a2f1ba44702b27e900ea2b6890629ff0eaf63d0b04a3eac8e861
miller-robin test failed
0x94147fc9fe7d0babd3418667b4ee003ade1e798004babde691536b6358b2f1cc
not prime
0xa5e3dd45c4a3c94f2a40a7d8ad7718c34325defe72dd9ce9c2c05951ab157393
miller-robin test failed
0xba9156cdd5d5cc69cacf2a8f100c8dcbffd757a549ca783868db4ef3b864e2e
not prime
0x5fed680f0911bf2cff3b79fe0bc04ce65288c4652dabe1f9d9ba312c66f7ed5b
miller-robin test failed
0xc2303e5ce5791fd032f827cee6e8a619e59411dba7d67f2de472da20c40cd618
not prime
0x11c7df89eeb4478da614d8322100d151168e532191b2eb1429855646063027e4
not prime
0x1afa425d8261d6aa8eb0b439922293558b4b00f8790d79fec7c029083094a280
not prime
0xb2e1c5d725331ad8539ea4966edb79f46e6e9d59f596542afda52a96d17073fd
miller-robin test failed
0x6ee493c7829a729a6eb6bca1f35fe668f902bab873eb75f83e70af5c0eca4270
not prime
0xbbff0b0485b9c096a930e1dba80c74e51906620c400e92f78740a5317639cf22
not prime
0x5fdf368c82f41d9eb8417d309e22eb6a8faa61407c6ecfa5b827bba1d1301af7
miller-robin test failed
0x3186144a86b16ea190eb8f062c16b99da34c95f7e2e3934d3a630b6b8a026f27
miller-robin test failed
0xe6e0ea176d95935b957b01fc466bfd7004fe719fc1486070c0359d5029ffce5c
not prime
0x365d0f0d1c3e08f96b458ae88087d9b45db63f66cfeaea3997f5aa42b12f5e53
miller-robin test failed
0xdb979ccfe8499c059110d646482bc19a5422a24a5db9ac165b1e2bcbadd9753e
not prime
0x9eacd81746dda774d5fba0d80550c4dc67b389f0b1cd6998266e4ed08abcd633
miller-robin test failed
0x3ea5182f8bc3a864210dd0f67fa99db0c6b8a36c6e943e4ffe58f9eb8f802267
miller-robin test failed
0x703712381ae5a3132b3c378ca7ed322a2f5fc08172b2f5eb6bab642f40f0211b
miller-robin test failed
0x97dd530d3d9e7a1a443276cf73316790616d0bfcbc358916136d2935c0a2f5da
not prime
0xecfecde5f0dd9776874014b28691c784cae8db43694e3505f18dba953a9b6f1d
miller-robin test failed
0x12111925c02a35060bfc5e368f141ae94cbd267cfcb648c3aab061c2667c6f57
miller-robin test failed
0xf9c46f6759f372d7abc3e09df9a560c7601f282e2984087a94b47be5e1b96be7
miller-robin test failed
0xe900331aaa0ca1c5f54fc71d696ed8241d04eb2d3d988bda6baca14a3acb1694
not prime
0xb8df728792ecb22b02ac792b812c794c84c708e231d0ba8d2e9934903d9f8156
not prime
0x12ae4037892d0b60111c90c2097fb1e90bb57bb01544e4821b3851ea9baba3e7
miller-robin test failed
0xfca6a5f007fe51eb1d18bd26036fe626de259a36140cd5a9e6826232ef7c826
```

```
0xb6596fdf7b940effa61870d526fa2a12ba98e328107810a8395ef78dae2ced91
miller-robin test failed
0x12de3fcd60d74ede2f62802f7d1f426be1cc3b0a46b3f0104faf1f3eb4540502
not prime
0xf1e342e71fb416e5861f653ba85694bb3529a0ffd9132fa5e24dacfcbb57a8a3
miller-robin test failed
0xb0c3c2263c4f46472b7b6a1e205de11351c3b1fe22512f17a1eaaf3a8bb09bba
not prime
0xd3a720305068ef1902b14327628b703ef837e871b03b99e169070883fa133a54
not prime
0x84202ca9fedd1dbc01d6815409a05afe5cddff69179cabd350266124bb50adf9
miller-robin test failed
0x33174611861d3bb81b9bd82ce03889d7354af5b4178951fe9521176c9bc9f1f3
miller-robin test failed
0xa398bf8825c498409ed5aa9e2d3d1375a34d0769fdcefbdd1c9815865d5eae45
miller-robin test failed
0x6db64154319b04e75fdc145be81a059e506560ac67a358a1d15f9e57e97c180b
miller-robin test failed
0x3001cdd7f33f5329a5528200268204c5e65d621a50b1564feb9ec9a2769b81bd
miller-robin test failed
0xd0eba0fc64967226977f90fbe550bea6b64d67b45be8cf6371ee2afa7f1a47ba
not prime
0xbeee81499a9394f577986be3a980df3e5688e85e1b23bae7cad2877c8f0447
miller-robin test failed
0x47d2f6101e4d38451ad6e493da8f12d453668bf7828c8b7a27d63c29ce2772f2
not prime
0xb84572ef08e69658ec2431131afaac3c7cf9f6a1ee3990df2f6b73a2661fa67b
miller-robin test failed
0xeb1459f9da8c3d0eba747b00c41dc5fbf3be2f8b1c3c70ff6de06dba48fda202
not prime
0x335cdc8cb348ef475f0edc85fe9b1b75f656d69f3ee951f35e5a45255cd5d893
miller-robin test failed
0xe14ecd08c6506e3f3050811554668ba18d1d53356c9fff6cd38c3dc186b0b28c
not prime
0xcdb5c3c53ccfad71a6cfdb8fc776ca886d546c2d662579d069e81e7c7a404da8
not prime
0x7a04ce55eba25a7c6dd6e8ca8a50d98fcde09c778ae577d48c33dfd5d5a1da2f
miller-robin test failed
0xb373da7205055bcc33325bc6087ee4aaa4180128f83c76c81cb2339a3dcc4a64
not prime
0x9b1a466b1975439ff542fb5d260b0c8a0e9271afd6ea36127d433ad371f23dc7
miller-robin test failed
0xbd1c1d258b0631f25c3b414734cf207c7644900071922718478e27be16d0c39d
miller-robin test failed
0xfa92aadf305cd2190085b701b78b9ae993b2b7f0bd5a27136bcf473e388e91f
miller-robin test failed
0xbb56f9e92a86fc3b6e38c6ebf2c1e749ba9d7f84c86f17c59bd2a5aaf64c1cf1
miller-robin test failed
0x616cb66badc2151a48f0261e3e83829fc8fb29b39b3fd59970144ae016cd966d
miller-robin test failed
0xc3ab6d5561e1476ff9fd336412d73834289990aa068d876b978e5a52b164ae55
miller-robin test failed
0xf0bb0fd88490558bd0c4f32647e6833d73d8d35baba2a71f719973e719729493
miller-robin test failed
0xca6e3ce5c1310bd7dee1eb980e32601b316afc481f25aa394955b9e35ffeefa5
miller-robin test failed
0x6d9e14fcf44013ff829738fc893ef835dd378ffdf57ce44e487863cff48707d8
not prime
0x641b68c3e257597192c6d3880bdd459ab2d9bc0db0bea451eca377d902a080fa
not prime
0x18fcc15b59dba16e8e985bb8bedff6d92e1d4dce67e49159c3b417ca32701b29
miller-robin test failed
0x8d41cc2c556b5844cd9c06f1e3058595d5c073a87f6a23298384704c46f7bc8e
not prime
0x53ed2cc2459edfdfad81f832153b47b3db671187d4d45fe8d32d3c76d3e57e9f
miller-robin test failed
0x161b20fe7b695fd65014850a061e21022b01c8cb3247a61d196e82ebb727f23c
not prime
0xa15e7cfedce79adf618524d57f7dc8d2d94c7288273fb0191f85f0d69ce84adf
miller-robin test failed
0x132113980438953 8c8cacbdc7b60c7a4b348d8833ffdb3608a4b48557a61ae21
miller-robin test failed
0x8ca88e8ee21c26c3d75d7602e383b259337122eef6e2f18ab93d4e04c0a7d4a3
miller-robin test failed
0xbd3666025de831d0378752b08164234268831ce117f3df0c6b1da47c4929bb00
not prime
0xa1c22fec771857f7707da82ec85314a779392491e9fa61ebb10185092b81e9d6
not prime
0x115df17b509bd84971dd59bb3ff4f387d89e79cef3a055378bc1f1bba7521a36
not prime
0xf44c9a1de86cc6182401072f0dceb34b048f6e7753a1ed1713fddc055519f583
miller-robin test failed
0x695cff5a5ad462eb9b50276ba09b3bc74f43d0b8dcc7042004dd3cc1fe438b49
miller-robin test failed
0x955d771951394548a4f30e2f39861643e089837768ab943ec7e654b89467d77c
not prime
0x86194b4cb7e58d7d274f9e3ce81d6232be98d1367479a49fd4ff14a7cb7581dd
miller-robin test failed
0x692e08d88943922c8fca9fbda6e42d88b91a2b037aecc186359e15db6429ddeb
miller-robin test failed
0x36f1d3d2e11f605137753e1d56d4e15c71ca4462066409249e4993953e979ad8
not prime
0x2d1324c3ccfcca280067c8883fc68a28c9c263515053d98bcb7666f6b78fbe32
not prime
0x796440dd89f66766a06e7ee6f3cc4262335f4587bd922eef7dcf81a7032bdb15
miller-robin test failed
0x8a2c3ed3af5a5ea334e031903b068d196d8c86a9843ab1fb660292958bb9067f
miller-robin test failed
0x4655ee606ad195d4aa930433a3f1faddb661b42c7f85cfe9f33502be1a16f7ea
not prime
0x9efe3e0d3fd2a4cdd8efd6fd9e622ffcf709f2dbb642883736a09f27408f4981
miller-robin test failed
0xbb8981399a0e61b115311ab7f04ad8ee52dc667e80afd23884bf92ecb0b2f863
miller-robin test failed
0x466169cfc1602642a24c4f1c1abfe8b70aac0b1a182f772b6ad70e974264a455
miller-robin test failed
0x7ab15dcc0a3a3c0f47cd59cbadbf819470f47e94b5d20ef681efe64c8a5f4f0
not prime
0x2c244540076749df6e314598f771a094eb1f616fae5cd7cb285d5f2c3cb928fd
miller-robin test failed
0xa675cea9f9385798d5aca97eabba51f48864829c3bc610b79e47eee7819b3457
miller-robin test failed
0x9a750e12870d007e179f2b43eb31a2e1279f9186f2ae9e50c7c0deb252b70db8
not prime
0x3fa27ec7eecc81c1483458a0f938e811f6fc179f55b3333cef96e7e17e2eedd9
miller-robin test failed
0x75b469bd27b4251eaa7802b503b34e895d5422fc7190b2accaf801e51ffcbeb6
not prime
0xcc2c0c49acd23d53ad7ba19f854c379f2ae44b1b863fe05b4cfdfe4d6f5b8932
not prime
0x362e1b07e251a49d4313d8861475d92c1ae63b33bc79b8428de940aa3b3a0c23
miller-robin test failed
0x1b038f1fb9ea242c5b0eed2e8a9cc3dc7672cf948426307298df3b23eaea5afc
not prime
0x8081069f68cf61487ce76fb5af901268b5165a4ae0d904331bca78fca6a3b72e
not prime
0x3edd93f3d0db1e8ac5abdddc434f8a83db10ab5d4521cdacff6b33d4f43897dc
not prime
0x2a35c7f0f3327752f632fc57e53c8b741e63e0425a2f61259a93d44a01175e97
miller-robin test failed
0x3e841faa3b307aa406b058abc5c5adb86256e6f2626644a05072b108cf12d73a
```

```
not prime
0xed3ad65c58b9de1cb9a9d4bb935ba6643790e4b09fe01c337001a2f1d0cd792e
not prime
0x5d2d3e89c5f6dfb5fc1b4eaaf8939cc1c8befdd96a2821a4414708aa61ad315b
miller-robin test failed
0x860c7474f5988f6221939bf2696cb92919916e27133bb68b9cd96255b8c78d2f
miller-robin test failed
0x96d31118016477b0275ebc5516fa3c462224b4b53caf6d3e352261f5fd54579b
miller-robin test failed
0x2d58f6e79d42471758c7fdcb903e9a2ae25a0e5c9defc3cf6f0ca8408a98048b
miller-robin test failed
0x8fbcf332ba75d9534d40946c33dafacc5c006cef790bd91b6826cf2026f9b38
not prime
0x511c91c3df8e7e349e6502a0c845e8682463f886c4750e2d8d7e92998676e97c
not prime
0x663cc272885bcab59be3ff93994b67ba0c7c0a4900713e909b32ffda7b12c88f
miller-robin test failed
0xe5557520439ab975fb8d1dcbce0285ffdee94225efedfc43b3dc73ca11f0abd3
miller-robin test failed
0x2107c8d1068c381a6c3e237f02f052ab5a85b55866b389c1fdc91a9cca92f75d
miller-robin test failed
0x4258735fa4c79aacddd81cca43ac1454dd6e55e2fc73556e7190c625b5ef9f5c
not prime
0x1cd01c62fb892deaa09d598f7febfc80d689d58f03d7fd365eeedaef4caadc21
miller-robin test failed
0xa12426dae18f9d997b109add15a3fb5bd1470feed39eb1dae5cae68e69efa50c
not prime
0x671d45cc581457605f678efde325d4b13a0079ab86c349feb2a40f6979837b61
miller-robin test failed
0x256a2a1ea84af154e7e503fc5a1619f7a0c01b32a8d8c92f1e62e9b66e49068e
not prime
0xf856acc0606614c31e4eee52da228f9f318d6e72c859f6a5acf26e6fd6eddeab
miller-robin test failed
0x69465fcc8cea9de0985ee01a6b5186ee915996b78e65cd354b2ea8f17b4f59d8
not prime
0xdae5f9d4354c6897c01a3853ca92f7b93e918e22a62b0d50e0bdd2be219b865
miller-robin test failed
0x56c6b7a8c32deca95a4af2f04112b672625470d82f1d097313d9b773c929bf17
miller-robin test failed
0x6a7e2489f624972767085ebabf983b73653125d8e2e3d29c8f94baf927df3ba6
not prime
0xdc07d42ebf827b48565f719c444774cac52f6ee15f3ee3b39dbf77c9257b6749
miller-robin test failed
0xf7c5ced893bdf242a8d40c3ccbe67dcb0f8b0022d4b0e5e452a8b5ca57e3dbea
not prime
0xbeb8e0ac3de76abeba38cc39d9be2491bc297aa24562a50c747ce50c9a19e0f8
not prime
0xacfcdd50a7eaabe14a51e07968486e12e0623ff977943e67d80bc1deffc5fec
not prime
0xd722baf44df0015e9f3e40f6966209cc2177c8e573814f4b1a83e644295aa016
not prime
0x8f173c06fae6b57e5b30143c6667e749de572eaa9a9e21c6e6a194d44df7bd8b
miller-robin test failed
0xce90df0a932bd18e69999c6cc0194292209901cef323b3cad1adf66b2e703b42
not prime
0xc4328a23c794b6c9d1e062d38f1b9eb6fe9a525a8edd5b160c1bd9404aa0b72d
miller-robin test failed
0x9d529ccf4159feb6be0cd1c0fcb59d428a66951e72c904f3990b0088c1c3f2e6
not prime
0x4a277bf44e37fb7c2b8601e90c1eb7d270a48ba30ea96b4250a2f3402343a9a3
miller-robin test failed
0x86375face5d13d493eeb6c9ea8b3c3ad25d9b452070c56c13d0d89c4de8a4836
not prime
0xaae93a768909ea09eb73443a9d3e0c7d6b352875de3aa4e164f0c7192d1c4a29
miller-robin test failed
0x19e0665f8ad317a8deb84bb549cfcb68cc5f49fbd77aaad4390379bbe9a7bdc9
miller-robin test failed
0xf72c2b2364fc34a88d2fbd2cbab5160c2099959473f58f708cdc10b0f157e3b1
miller-robin test failed
0x1c87544ca50cbe19a8f3fa51f74ce7bbe2c7f74fda18b580530ac1ec6c6f452b
miller-robin test failed
0xeb67f3797e2b5f208439bcea6846c66f0f47d20f3c820a4a76258a29f98ff6fd
miller-robin test failed
0x1030baeee89a03ab1c1c2bff5e716cc24a5a78f85c38a27beecfeb3bdf7d260c
not prime
0xcc5ac86ccada70c57187011b2a847e15f8496d390e6d8453c44f191c23a505ef
miller-robin test failed
0x58ccbff418975aab44d0e66234ebcd1e86eae563b57b9c3d653ecfc50ba88386
not prime
0x3e1e1a0f7a0e82d85f64d1d29dfd66a477a5efe0300c3940babe869aae7d8c7f
miller-robin test failed
0x257df3b93f4ff129ee754ee8c2aaa08071285410e4ebe596c8ba95a98e99e19
miller-robin test failed
0xe5986c36fde3082f101ae43a7518f6720d1d782ed7a06e23ead342d4c767fea7
miller-robin test failed
0x9b40dcc9a94d9fb8f46ef174be52b8dfe207059d6e92bdddf18c3c8e57f23330
not prime
0x60a4fb00e2f432390955cd5a6c256c3f6c5df2928b202baa5aac01bd734b9b92
not prime
0x54d4765dded7d704f8440efbca21ace2de0e4e8084d81e4c72e2cf7318282238
not prime
0xe10b11c31fc1b30f012ba5ef5472feb4eac3a1251ddfb33938d6454f24c225fc
not prime
0x25cc90f6f82fc1d6c9afde4d62c16a2f2d3cf6b8f5e779e28b90ef4c4d15b0d
miller-robin test failed
0xd1e390a60c8ad0a442a5618210b2ab3900b5abb18477b7550dda316d606997bb
miller-robin test failed
0x43cd124150d35d5fb44441d36fb8bb2bc7feaa12e935718f5fa1fdae147e6005
miller-robin test failed
0xabba7e2a07cf3886a3bf0f8b642c32f9b9fc747ac1b8c86e78d5b639cbef5aaa
not prime
0xe3e10a04b2d511c030c1a6dbf03967354890e0c3e2fe3af91590f931ae0207af
miller-robin test failed
0xaa770fa34faf1f8d40808cea3c86177fd8c08d23c5f1d29a3fd9c080824f2ae0
not prime
0xd6ac7049292bee34ae6b0a912dbd91dd0d2e84e2498c04d348171bb9d25fa4bc
not prime
0x3f94b5a6d1d1765e0a9a00bb8c41de6e2298096b8d761003eced26894781d66f
miller-robin test failed
0x4b13694d1c46a20296539e4d251e595c1de147133de6ea85753c84a9c881067b
miller-robin test failed
0x7dc41004b03df0a1d28a40ecec7a8cfb7a7fdec8c740ab65add126d6f4cb6212
not prime
0xaa5a462b0fcf7d31c271e91882977f21877d699fa4e81bea24a12ac354e07d31
miller-robin test failed
0xbdb8daca53b0e1761a0af9a51bc8fdd5b354d9893f4fdc9f3e599d6602ef542e
not prime
0x7b71421934acf6b43142f2a8dbcd77e058f2d42407fe5c0ffe0d1e4f4f4b7042
not prime
0xab65ec67b2f650d3f2fe09fec9da4c6b0c110a344fff65aed0059426f1ac8e93
miller-robin test failed
0xcf1d1b2a42eb0f4e1febe4cb10e4214550972a6d8c68f30c49245342343953ab
miller-robin test failed
0xee1a0b28756b1691d2259cc4d6b965da14cb973911a657fd569f4b755792c17b
miller-robin test failed
0xd0ccc6d6f55e7788995fc0ea7a0360514e4ad8bc60a8009052c3cf073fadec32
not prime
0x9ef46eb17480c19d9dac18fec4ed28ece3e7c6485faf4cebbdff8e3d39208ffc
not prime
0x7557f5c26f45aac6a436c39245425cf7ad80abcb50530b42932f59374855eb40
not prime
0x752639a414b19ce99e1c21d18b867dd3fba9bbdcd49656ae77a8a952b50c08f2
not prime
0xc3b773a1a8894c1d12e69048c3f70ca928f242ff336d02fdd9037855922c35bb
miller-robin test failed
```

```
        0xcaf7e60de815e77d05d553406813689e57551b15e0d6a12b9362f7aefed1bfa
not prime
0x704aca66a58b790a5b50ae20d51a88704a5e04e9da3e0385e17ef21c796ea574
not prime
0xbb697427992cacfa6661744ad74a84eb125d6ccec9076bb663f609d177300f8f
miller-robin test failed
0x64b104bd202504afc7258592ee46b727cdd822a8f0cbf6cbd348226300e28f69
miller-robin test failed
0x4766651f5302ae775324d67f1204ac656bb16eb06a147c76a255b781c8abb97f
miller-robin test failed
0x499419f35184157679711acb8f8024e33353987fd2aa8901f4922f425b12dc7a
not prime
0x7ebe53eeafa365cfcfc4f82fa84213e612f7c49577c5b64ccf09057cc089e566
not prime
0x87f13b53f8e3f7feb0d8b91c81ddbf35092328b679e7a26a77e39b45c301a8f8
not prime
0x6b301c99eeaad1c42a9bc524fc87678e868599b6c5b2237c4436021bdff3e065
miller-robin test failed
0xe7e4520cd6a7506671c5fdbb768dd43a7a6a6ae4b0ffd98f4bd28fb360ec1a1d
miller-robin test failed
0x8a36497e853706a078a4fa71f458af2756cec73ef89657ea47b692eb3536556c
not prime
0xe7332a4e703b791d1ae31c36904c47e9077ee3aceb35dd76ca57a4585b67ae2
not prime
0xb27bcd3930c09ebf03b4d8e38d22d26670c7e1348d208608e3def0abe841e7b7
miller-robin test failed
0x112afa08cc8379e4e6b213a618b3f3ebb3ca524d659e1641bc6aa57b353b9182
not prime
0x31f9ee9b68db88b61e582e8488900f48f315a02230933747c8259df1e5572a81
miller-robin test failed
0x3cf0aa3b12141323af475f9d44a6bb1c094f9d37891163709b59875742989757
miller-robin test failed
0x3464ba765ce024e3063013d7ba6aab8ef83a4baf3fca868c8f8bcf9b7a06bfc7
miller-robin test failed
0x4498389a408e99e9a49cec524ee74ed7e77f9299088716c38c79d6d33ba6b696
not prime
0x17bc0eab74ae233bc44228f01fb1dc9e0d7270ca4e13ee93f69504cf74dcc544
not prime
0x3c6df2f472fb1545b7573892120c03fa26548f9a1f6b49d5f392d0db09900226
not prime
0x8ee7de9e238a1ecd520f8153add3744cb891cb26bcad6549b25276bfb45b6b50
not prime
0x2b81442bc500ce4f177629ba66ccb1bbd429a575067646627055343bc813763a
not prime
0x91b546fb040ab557d246d0cc72e6958f3fc167f30b069b555721793b4340abc4
not prime
0x5db8519e36d0b8041f7f3b0ff639a7be9690eda4acb2012ae48aa45780a6b604
not prime
0xa522b23b19bc68b203a62b8b45083741753bd479b1efdcc07e2400da561daed1
miller-robin test failed
0x195dede2f1cb6e39e5cafe0cfb24670a77266b3fd111a057a5f59d5049f08fee
not prime
0x68687a790b25102440cca3364f4ec6413a29818d642d87471fe2069dfdc22e29
miller-robin test failed
0x71c509187af350c9ec3e608b720b3c24785ae50bd429408c60bfedde1e4bda5e
not prime
0x68cb6fb450bce1040aa81fb6b78b4dc147da8fa8ec17aaf5743084e6a4fcfec8
not prime
0x30880aa444a16d45865ec4165676c26b1180e5894afdabc8bd58da95565a12b1
miller-robin test failed
0x4771655723154f5055697857bfc32fb5b58220ef8f49b093d7182393b4059616
not prime
0xa4e12b63509a52b0b0a887e00a778d2ac76c3f936da9816d7c476339638fbe6a
not prime
0xb96b10613fe00ebcbb4281d43114bee3e1282a2ee9c5cc3824403cdfdb94e9a5
miller-robin test failed
0x36ddab852cdf13ca1656d27c458d15c2d6011d1fb5bf22fcdb201610ebc2c59c
not prime
0xb67dfb6fefecde7eaf3580920bfce67ba3c1b2b4f9d4adcfb3486aa783b71f58
not prime
0x1341877e77c7f6cb0e39659c481681cbf5ad01eeb5aa0d9528b9726ff723acb6
not prime
0xd7bc7732b8513d4b588ed3038143a724517b437648170b3b02b3e52ec839bb25
miller-robin test failed
0x434ecfffd3acae940ef435b782b1dd96dfe5b3d8eb46fd049647ebec020b3954
not prime
0x6f92e577343d0ce021ff8458ba55a0e4b22a400f3105a082cfb95ccd5be26cf2
not prime
0xcaf03e652a1cc97e61d4915830c956e2a09ffd4729a2c5b6be6cdd9bb79a3246
not prime
0xc37000142f70ff42c6a48857acb5afab707fed547f4a227aec648faa8070d800
not prime
0x5380dadf8eeb417f1812f3fb5a155fa501e705c6c83d05f0a7fe007c15def0f4
not prime
0x9361a928eaad6bb79a1ad1e3f9107b894fdb2e0b1d1a53be26bfcbac4e56fb57
miller-robin test failed
0x2473bb4d4c3384b268367ea4ed18946474d7739d19249e1f475b25a918bb1e89
miller-robin test failed
0x76ea1dfe2e1ad8161ae85fe4b5417d32a51ba73d035d47409e271ac0bae346b0
not prime
0x79cf34a009a405096da7cbf1b890c2c5359fb2c880fe34b7c8ed837111fc3192
not prime
0xb7aa262682ed9362da61d863b4fa27f91b1f1306ee440855b99db93c0dbc7b2
not prime
0x3a8093d247717fcc6a2e3f9c7c48590bddb83b84cc4b4f0fc09ab98be3a0cbae
not prime
0xf2f4c49bbc38a8263017cda4f424d8aa6af333bc198b27427d05435088969204
not prime
0xf1446f3b44f587f24707e69957a58980a2fd7f8197555d4adfefd54a8229612c
not prime
0x33b73ec219d64019134a9ae84b7f796204c77c63e3a9e1984468177a4a498e30
not prime
0x23431dcc8d793f44f2a82dc532f1b99cd8b224ee7f72623e501629efec51fe16
not prime
0xef6d8cced494c2962f17a4e9afd539099bb7d5510499f584a559009eff43317d
miller-robin test failed
0x3423c449da5cd2c2de488d2db6824c3e113cf1f8193fc128dcf527369613c8f
miller-robin test failed
0xa60c549e59df7ef48de98363ebf5710a314694d6f838aaeeae08a13ddb4b32bc
not prime
0xdf0a212a2b73bc509a5ac77b5e6f56ce593b503f831569c31851fa72221e0d32
not prime
0x107e60e568a35ef68af2415179b4e8fc6d6c396ef398dcfd6fd8f9effabf210c
not prime
0x644cfdf2a4081ec3fe5668b647d47681e6fcd1440b3abc02e0ad5caa0b70115d
miller-robin test failed
0x7c98794c62ee81f6feb712f147d52c2658f6b98b4c4fc882c860f6e38de8fd7a
not prime
0x94760842ecf538091fa25f2b650d988c82d98a814c984193d86463b1c444299
miller-robin test failed
0x3b0d6613d4e3c273e4e052be922955a13275f66ba210ef61493141e3c2b94dfc
not prime
0x1361b9bf997eecfe2bcb6aff6315d1613af9af8ce603ba7c96c6dd62f6e063ce
not prime
0xa1571c39b302b72038832df41692a255b0f59cb6460143d13e2f2fc6681d7bf2
not prime
0x46d797035b50331c4ec831635bebd7e4ac78a4067b5860b1b0edde463a12b9c
not prime
0x505e1905eac949a5977fe3d1c4afaa23a8f4ad71abf3513fbd00e0413a1138c2
not prime
0xaf10edda6c7c0ac29009b29164ff9b8f389a92b6b597b74983a5b2a9ac92ccf2
not prime
0xb429977dd5024d88593600c8e161c901d1fa98ebfb7e90b642920d58db4e695f
miller-robin test failed
0x36be9a00e009555a1a6cf8f26ca0a1207bcc062573a710b3a35792c14fccb561
```

```
0xc80582eab4e8fcb0eb2c6c16fadfc788220703799ae38c95a24c583409b6d2e5
miller-robin test failed
0xd48cf584d8e2c93493c0f8389fec130feb49a2fc8182268aac9db8eb5929e256
not prime
0x6ac32f019f1c2fc62d035863987d8871e1c2eb518bf96b170c47861eeb860c90
not prime
0xb4eca40be025e07770a0a13abbb3e4d582e1f9908609f8486d43457e7f6e6211
miller-robin test failed
0x5cbaff5325cad0c0a0dc174738c10489d120855e286bd03032a11fb5af902dc3
miller-robin test failed
0x5a22fe47f8a4107a887b5d36fa3eb6b523ae9893e83c5c8a6747562a56f2128f
miller-robin test failed
0x8f54f7f6080aae151c026441659275ff471a92b1715c707ef9539dd61ddaa54b
miller-robin test failed
0xdf272c1089286f1881103ee482c0da958b4a2900b8120f5e4b2397c379f82a35
miller-robin test failed
0x85b4105fc083943f811f578a70de7ed96b2e0ffdba5c883ccc8daa733b32a896
not prime
0xed3060a996e2f5a5b07115a7191b501029e2723af9cbc1c6911c2351986eb423
miller-robin test failed
0xec0628cec444e1fc6429fb6d16c88712ee1a9fb1f1aa26cb8b4a3d1aec266695
miller-robin test failed
0xcaadee3db21be817564086012d3331ad4ba8d2e2628576c2311c6c552d64f4c
not prime
0xb27d84812bbaf1e0e3457cfca02f583fcdb4c7ed22ffb56cba336450c72bf460
not prime
0x3c4a837acb82d410a9bab9848db2551124235e3438805ea45ecbfcb2ea21a9de
not prime
0x87eb2693460fcd2c14fc3b280eaf00e10ed855b8ce3946765accfd9150ab882c
not prime
0xfdb20a5856dc42a65ba7aa5b98f37a838d579e87b77e4811a0d1fdb4d7f023cf
miller-robin test failed
0x9621f69ee0d412f0f14a8b864bde65242d4e19c85ed908acac0a9a2930b3eb33
miller-robin test failed
0x2c3ad63e38912402e4252e5623f52bff72bb1baa8355ed623c2d4b4cae6ae40f
miller-robin test failed
0x71ec938dcf58566bf65ab037ff282c0039a06411c09b3a7801e9e80308783e8f
miller-robin test failed
0x37431f7459f8d9c0e6470dd06119764594b4ced959b39c04134f9925386e93e3
miller-robin test failed
0x83a4ee3a18b71a50a44518e86e04dec4f62301de950c1dc1d0f345aa6cfc3ea5
miller-robin test failed
0x4b4a7d9297a4891e964e459b3aab992723efb79ed74171cdb8527e19838d2b6b
miller-robin test failed
0xe1d37c76458b6ede5410486a466f2bbf6f82d25dd6e7bb14d16b67d43d534ecb
miller-robin test failed
0xa5e8c40476668ae802ff1f6347fdabaf27c4449950eaa8f40a22a81a501da217
miller-robin test failed
0xd009326b38d8e8419f7bc99ff75cb2108acfe218309dfc268273e8e43c1e8d87
miller-robin test failed
0x893d40c076fc99373d8fca0a98a9e688a665a9f13ff266105ca2b7f0177ab0be
not prime
0xbdfd609c2e5f313c2b1083a48a6da2f5c74b9d016ec01f721c5026149025e436
not prime
0xa776bd6712eef7f92d6a6d6d44e9378fa2737a97126ccc367f932100bcaa206d
miller-robin test failed
0x12fae1c2bc7ab7abca71e881a496e48abf2a42457616d4f5245c8b0100de39bb
miller-robin test failed
0x23c723cd8d91dc9c0e46d7b7089481bf1d0fef643693ad3718d6a16b9390002c
not prime
0xc94426118ec8b3584c8287dc12b094e5fea26beb6bf94c3c7af6c30c49ebe4ed
miller-robin test failed
0xfc594a6614a0865c9e9af262604bffb1a456c8c6ef5a0222d5c25432f005db00
not prime
0x8f5a13624ebfb23b8ebf5955600ed5c8169dfb831a35d58fb8ccbd26fda92209
miller-robin test failed
0xeeaabb0e3de9225942b84b26f94288b80a1af623f1d466ff835925e41ca81564
not prime
0xf860cd36d4e7744cce785a86c191f6788e515e99e6ee88cf7760521c59b68992
not prime
0xa939a505bf408820bdca0a440c2da3a5f4b0d5396188c9ca8663bed45d4a6e41
miller-robin test failed
0x573b495c5ff44684302e30bc81dc2fc3897c074ca4688cf1e38075ba6acfc691
miller-robin test failed
0x7555ff8c54b1f93465ab3bc9413ef7286203957f598a24aaf52d55af24756516
not prime
0xa9610fd572decb2f4d723d79d4cdc41cae0e540f295c593bfed054de51657467
miller-robin test failed
0x2fd536bd333c23f5d2129a94a2169000516e5c4d675e46a981c79ec389b8fce2
not prime
0x3748d469fb865eee5d69d026f9bece440c1bd26828b0330de88be8c52c157655
miller-robin test failed
0x6a092acb1bb9dfeaa5f6e6548a60625cbd3265d77f8071ca1a40755e047b7416
not prime
0xb26a812a5bd9a302de572dc3761077c4076c9deb06661967b57806bfd487bc82
not prime
0xf94b81e48358a638c271e160cd841a52adcb9e81d34ead51f8da3f5d2d58efec
not prime
0xb5e7cd1a52a8d21a35f9fc97bef0cb9d51bd17ad250f23e82239926109245808
not prime
0x8c2f81b934336436f3977cac567b0dc6577b48ffbaf5999c2643d11adb52b535
miller-robin test failed
0xbfb1ea06137b077a43e6a39a3de389874cf7108a3b62ad8e32746ec0c8025319
miller-robin test failed
0xd9008503f2eb62e35cf45d3bb00fc112aa87d8d200c817dda60b61b609c468a9
miller-robin test failed
0xd957730b08fcef09e807a4950078460c06d167ae84059ff50f1415e6f925f71a
not prime
0xbe7ba5f8015f3566c44860699e2eb9d9a212db50050971eaa110bb5b5a7aae95
miller-robin test failed
0x78b78fa637caa011b1ce019dda7c2082d9db81c635808fbb392174fe08bcdba4
not prime
0xef52ab3606f8ad3cf578c3abdbb32e64d3dc4fe9d506e1895389e8f216d5b398
not prime
0x934493713610e0c6cbf97deb455072e45de1f8e61714eb0d662860129d26d6c3
miller-robin test failed
0x9d399e349c5599a16de263e2dbb3765c1db4dfdbfa7c3edd08f92fe76e7caec7
miller-robin test failed
```

```
miller-robin test failed
 0x8de6915070186c0859f3324179f7c234db9af80ccd52f7aa75e71a5c05b21dc0
not prime
0xb1b929c642084dff598f5b91b9ab19c58e3ffee9c7bdcca62ff417680a18c9bf
miller-robin test failed
0xf2ec12b01504a0e81d8ec39ec0e74d677800c7240aa1966fcc630f199c76ab74
not prime
0xd05d012ca91b30effe51bab892acf1bdcc4c42d246d8573ee13f839b0eecdc44
not prime
0x42b2de2afc0f0351eaca086fd4873d146c821bbe4531b24611ff0205df6d2445
miller-robin test failed
0x8c714d0907e2810817abdd72db4fbb479f85868e9a2f09e2ad0ca39e9ef88644
not prime
0xb79f283471a31ed0af62d95f72a91094086bc4720866fe4926cf5c48a303b5c2
not prime
0x8b1f41fcb6f9b8c41b9b0094f379bc2ebd944836cad920d4d8f734ba251a588a
not prime
0xe2ef7f265147f2b3ca2384c7d66bb22d75bee342262bec9bfd6ab1f5846ac34
not prime
0x7237b648667c6b545ee81456a117cac66ec6839c577c7912e1f3c814c90ddea9
miller-robin test failed
0x940b914dd6929d1e61d33c7dd5c4cb833473ebf4f4c172a49a13b6cb05a08329
miller-robin test failed
0x64b025560ec5629a1f8747b671191ca9c990cc578683d57257669a46da871613
miller-robin test failed
0x49e0f6e51be056c92d35a2f227e3b966c9beaf3b042ae61783db54cfba2be1a6
not prime
0x42daa4ffbe62c459d8240125e28cf5d5e9e237b278a1a2fc4744029261c15bbb
miller-robin test failed
0x6e352d5ebb30094be2b9ad790cc4e711cdb48acb928c19b85bf027e54895b220
not prime
0xc4804b6b90634dd00afbfebbb123c6764033e4468bc8124dc070e3be0398de0e
not prime
0xf0c623444b0d5c796f2776e1fdf5721f1b8fd0008ad777b8064a0c9137629b29
miller-robin test failed
0x851f95a5a2cf6d0757b8a9e2eb5eecd0b2f4c77ce166fb92cdb35e599318cb46
not prime
0x2f1a19cfd4769babba1cb0f3d9e26a8ebdb4980bba1f63f7a85194cbb04bea4d
miller-robin test failed
0x9b187788f1604bab7cb7f20a794f9a0d545a16d057e475f73022c06da305d889
miller-robin test failed
0x74cb3f0978d416505dfe3c2f13d5be93bf4869a176a9ea53461cbc60db0bfc65
miller-robin test failed
0x5a95aaf6a7df2b1edf2af073d8f71a99616102bb5dbc1641d19393d72127180c
not prime
0xa4f2e221074dcd9f9f8575464685a6dad352fad4c188f04ee9f18844bd2f3f9e
not prime
0xa727d3862cccfeaaea1bda6cbf94b4b51561f602d311abb12f6f3f9823056531
miller-robin test failed
0x364a055b0d2acadc5b75e02d1751a680a93a17c4e582179d9c531b7899904529
miller-robin test failed
0x828cc6dd1a64c25a372a54eff04667cb6fb15db6ee442196c503aa51d74a495e
not prime
0x83d56e3915d6ec1f00a574d22352af1cc5e073b29d5a6d654326ae9eea86dd92
not prime
0x2e462082c3863a6fb2a43862b2a3f5e82a96241ab941a55081f1c89e2f77cf21
miller-robin test failed
0x8f001cb56aec11bef34a8fca44f9e966a1c6faed3344b68a5bc0e33ef00ff889
miller-robin test failed
0x7d4094a2ebc9eea5d055c0243b6eb68e1f385cba13c18314c67a62c9d82d536f
miller-robin test failed
0x82c42b8993ff12433d0a76a90e37ce8998960c13923ecf3e94008166516e3114
not prime
0x66b69177bec02be068977e147a5feb09879d3e0e4f24385a46c7a96f742f0b4f
miller-robin test failed
0xf6d835426b6c918cc51f4dd0dbee450e7e9b1f88862b17aba184ce0b0fdc9c7d
miller-robin test failed
0x7edfa331f114c8859dc2904e3a096189e76d02a37a6c09f92987012e20566e5e
not prime
0x3820537aa6fe463d4a1c935de7bec7ca2d69b73214b899b3dd3ddf06c16b9a29
miller-robin test failed
0x40e974bf349cd569371bd89ca4818fe588dee50faf622965fb41f708b5eeeb3d
miller-robin test failed
0x4071370ee09240a579512230a97664c156ea0d1b546e4f385656f9d78581e99f
miller-robin test failed
0x1b32fafb02866eb2a546f90184a1deec3f5f5f7ae83419e19ff79779e17921b2
not prime
0x8cff241098ea343c37cfb5cd1c0af7f2054f5bf2274a45d0d275148389a1172d
miller-robin test failed
0x6acc5a789c6778b45752587cd0bb5be4075bfbac566f6b1967a8047d70c22070
not prime
0x132ff6c6842419e66d2a27d4cc4d0524824ed6c8d36e97de6c96ed536fb09325
miller-robin test failed
0x97a53e3be8447aad89ff69568a09f7b8caf30df5a411adb06b8467546f8574bf
miller-robin test failed
0xbb8ce41d416c05d79ebf3d9c265052b490170509de2b4b1af8ba8616edafd75d
miller-robin test failed
0x55782f92d8a772a02a2ccc1956908bf612080a326964ca975b447d616384ea77
miller-robin test failed
0xb416d23e0025c8b366b4e888105adf4ed4cafb521b6b94ae446b9e47d22b6fbd
miller-robin test failed
0xf6ede9b4da4dce56cbff8a8d197a6385fcd95215f99d463bf138a91b84330fc9
miller-robin test failed
0xa30afac2251626220b3035e622c37972c46bbd3761f46cb7c7e95559f409c5f2
not prime
0xfbbadd4a0546ec002d9664125e70b11965da21eb8741ce1b73835d9e5eb07982
not prime
0x69b14552acb59f518c37fce45a3c617f76c34bbb6dce35d5b4af9d134ecff147
miller-robin test failed
0x499a691edbd1e0a7f6bbc3ffbd0c9e6d68b52deae57c9a749e9af4d09df925aa
not prime
0xcfc514e82290440b49f609300e366465670b01994b896bba1d641df097867c9c
not prime
0x259c3e0263813eef27f12b027f2741cf87ba7fa10141627d22d6f9fd68b77988
not prime
0x6e18d4ffb37233f83ad5b9e78accc33b0e41b33c3bd0f6cb215decc38d900b3c
not prime
```

Генеруємо ключові пари RSA для Alice і Bob, де(n,e)-open key, (d,p,q)-secret key

	Alice	Bob
	Open key	
n	0x2d1e6286f610aa464f06fbd1562c39ba34792a7d230ff8262f05b45ad8a627e4f1f22f86f5b9bb1d7cb0eaeb39af96ec63e0edd02cfd93192fb46281ff8abbf9	0x5e2fc579dfc098f4921d2e7a50c80fbf00d362327831b49f1fab00cfff6c7ed3a305a6d17a62dd7c2e79fb4f5afbd32d23972c56b8ada744aa9e823dec7ebbdf
e	0x10001	0x10001
	Secret key	
d	0x127bb4c2d74d3fe11b1a398bc39e6bc29735d98878b3167d5c3a0ba848dca322f878820745a9e82b6ccc5494c971e5e6a2c587afe3d1b23794c156eb2279801	0x1ecdccee3129d25c9ab50490687f25f73813ea57cb4ba6612c804701bfee0204584682addc264829bbfc701d22a4e263341ff33c78ade6c4f5ab519471a72381
p	0x22977a425135a96bf029e605c31c5170365f726fd81f9930deeb4f51c7c0b903	0x766407b6f799d9c0581151148a2f8de3748f77a959e18e53caefc17e999829a1
q	0x1f4421f0e41c7749f4731143499f925d209eb045d0ae9760c659d9841408f3a3	0xcba9a2df9230d94f4abce3ec318a8b5f3f7056f65eefa5f60d53f143e84bf57f

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

k₁:1e357867dd1d30331d12baaabcddc6146e861c593c30d406d0c653115a157b5ec68aeef8e45e11584ac550517cce0231309920da62d3ebf696704fb145170fca139cd492b10638283da9075eeb1254c850b391e6dba1d55e2a17813ff9b4b8d1f279c9a9500a2320da6f135c6002f8f54933675adb6e0b488b30d1479f18d955424889d03a16294c129f2d01bafe32cbaf62a0553d3379f4dbb08f2b339d3620826762ea797fae2e7ebf656bbe5dd52a8912e215673f27a97cb2145974061a77

S₁:247f9ad8cd1b6c3ef97c505bd774116b817fa5e10c50209e9dac31d13f4d17d79255f5957f05240515d6970277314856ec37fea120ab21a0b9b19eb22cf2fa38583dd06fb58a208a25e2c007e9cf08b96e8349d1fb85b3063ffdd20c5f4d8dfab662e1ad87b27a8fa8bc17086a4e7c05de74a1107dba4ec9cd807d7a343b750e0134f8d99fd117167b085b1e61996c408520d77477598145891fe5d6336a3cab454161e7c086995cd2b504f1282355826f3725dceb0668c1d64ea3a90a4ea5

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

k: 0x175
true

Перевірка на сайті http://asymcryptwebservice.appspot.com/?section=rsa

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

keySize=512

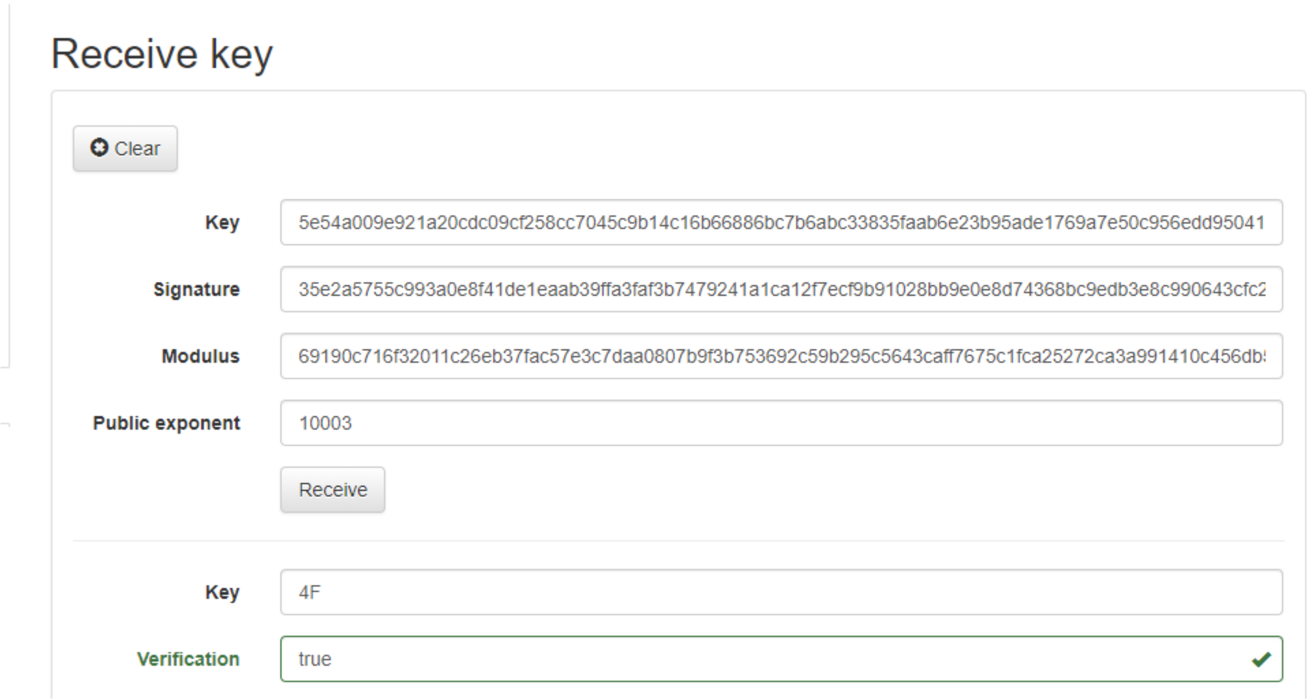
Відповідь:

n1:C80E8DE176A8C0ED237D2CC982DF7C6EA1124D5E620F84A3A99E4B6C6C421202BAEEA682BE3667742A7C4E018A21EF0B6A2DCBE330AE5E20379B597A0F5F430D

e1:10001

- *Функція SendKey*

n	0x69190c716f32011c26eb37fac57e3c7daa0807b9f3b753692c59b295c5643caff7675c1fca25272ca3a991410c456db51a5051c83b88e008fdc0e0cbb659f07d
k1	0x5e54a009e921a20cdc09cf258cc7045c9b14c16b66886bc7b6abc33835faab6e23b95ade1769a7e50c956edd950414a145a044c7f060e57f10eec6ab185b9f5b
s1	0x35e2a5755c993a0e8f41de1eaab39ffa3faf3b7479241a1ca12f7ecf9b91028bb9e0e8d74368bc9edb3e8c990643cfc200a31df83650d832a38c26526d52e0c3



Receive key

Key: 5e54a009e921a20cdc09cf258cc7045c9b14c16b66886bc7b6abc33835faab6e23b95ade1769a7e50c956edd95041

Signature: 35e2a5755c993a0e8f41de1eaab39ffa3faf3b7479241a1ca12f7ecf9b91028bb9e0e8d74368bc9edb3e8c990643cfc2

Modulus: 69190c716f32011c26eb37fac57e3c7daa0807b9f3b753692c59b295c5643caff7675c1fca25272ca3a991410c456db

Public exponent: 10003

Key: 4F

Verification: true ✓

Висновки: у даній роботі я навчилася працювати з шифруванням RSA та реалізовувати перевірку простих чисел. Також реалізовано протокол передачі ключів RSA із виконанням функцій генерації ключів, цифрового підпису, зашифрування та розшифрування повідомлення.