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

Студенти III курсу

ФТІ группиФБ-82

Ясинський Нікіта
Владислав Кравчук

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=0x4ceabfc4049c134e8e4260d5a2050e5b051edb54f20da579fdcd2a4e08cdf41181d6877
   q=0x16fa341d24117ff675091364eb27688e3a40b83c41c40b91430317ac445d4c4cc7129d5
   p_1=0x19f1c85ecf6e463bfb938464dfa9b3169f50d091ead4fe9d1afdd0e42b60141e6de445f
   q_1=0x4ade08bfa81ccb92febb43b5b8d876a00200bae14efef9a592604c31172d9955cc27d9d

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

ALICE:

31878 809 588 742 781 377 390 292 513 686 735 321 344 268 518 358 377 576 910 493 914 223 682 875 740 643 202 90 IS NOT PRIME
18507 506 162 309 404 303 802 080 124 727 734 182 742 372 579 294 121 546 883 983 018 516 388 806 764 205 037 9 IS NOT PRIME
40954 951 324 328 505 519 281 326 541 346 181 913 035 649 305 284 435 438 171 434 533 558 542 975 569 057 759 08 IS NOT PRIME
74251 415 661 999 743 303 316 490 362 826 482 174 390 123 025 427 821 755 210 764 911 865 035 806 894 967 938 95 IS NOT PRIME
71639 171 828 936 488 411 546 410 512 886 155 717 763 114 788 252 198 757 528 998 703 868 186 030 164 939 034 40 IS NOT PRIME
64532 763 215 360 226 682 966 204 873 848 472 747 462 791 404 840 797 430 699 923 791 626 997 994 541 282 842 04 IS NOT PRIME
51149 086 040 616 729 311 054 925 469 895 964 476 941 521 890 657 696 132 086 942 464 747 659 453 072 611 021 38 IS NOT PRIME
21908 357 260 443 622 704 169 320 320 564 506 529 846 783 901 830 083 472 701 513 328 815 109 745 909 100 370 49 IS NOT PRIME
83490 160 114 127 881 014 546 313 083 663 900 860 793 981 340 817 463 937 498 242 958 698 231 028 686 531 933 26 IS NOT PRIME
50741 823 680 277 167 710 856 356 301 469 567 523 383 770 302 266 148 137 192 208 106 034 357 538 232 289 399 11 IS NOT PRIME
26714 090 093 943 451 419 935 384 559 579 443 609 599 547 216 397 883 547 114 092 125 563 752 334 650 945 251 11 IS NOT PRIME
24943 980 271 298 006 761 762 067 503 665 773 863 833 646 710 101 417 729 590 549 130 519 472 189 999 552 430 59 IS NOT PRIME
92606 017 111 181 199 485 765 591 894 411 122 205 713 582 276 466 643 070 576 267 058 207 519 607 952 478 983 74 IS NOT PRIME
43052 233 074 718 607 924 827 381 676 681 957 735 084 832 393 521 114 486 223 005 933 801 855 280 503 640 015 88 IS NOT PRIME
67818 230 088 296 596 793 652 614 767 109 233 615 608 659 303 840 886 483 584 166 980 676 653 648 146 253 415 28 IS NOT PRIME
84063 160 028 959 219 989 139 885 862 572 653 636 220 274 746 556 321 071 869 023 736 489 077 880 451 184 641 12 IS NOT PRIME
16788 179 271 648 087 511 710 210 389 993 963 400 171 820 923 964 818 458 271 514 241 825 416 243 125 105 349 03 IS NOT PRIME
96515 953 074 350 689 273 418 258 965 202 443 798 197 306 351 239 901 226 593 827 639 206 012 332 505 898 323 53 IS NOT PRIME
83796 107 480 143 527 265 017 839 235 624 326 285 272 941 159 209 038 786 746 601 979 465 801 374 960 682 599 27 IS NOT PRIME
97592 141 184 494 194 877 809 898 174 992 706 707 081 002 888 047 892 895 577 577 544 621 559 598 825 079 655 83 IS NOT PRIME
68721 253 992 218 733 435 022 853 814 717 122 717 385 266 560 033 895 552 640 260 736 284 979 647 212 205 850 23 IS NOT PRIME
47301 599 832 465 928 266 088 519 064 764 875 431 750 443 305 169 363 739 799 257 594 268 328 400 713 329 298 87 IS NOT PRIME
27597 721 097 158 706 362 777 388 134 699 309 337 839 846 232 526 994 998 959 493 838 973 617 413 211 541 277 43 IS NOT PRIME
55904 694 668 483 972 836 286 593 310 082 468 692 324 774 227 845 533 358 754 008 923 030 861 548 765 441 646 50 IS NOT PRIME
75530 958 066 279 964 720 591 003 134 530 583 990 352 178 342 638 968 244 476 496 665 883 563 755 733 052 492 IS NOT PRIME
45250 954 149 019 002 828 851 667 270 571 470 010 648 255 212 168 514 382 407 680 532 837 171 903 272 192 893 75 IS NOT PRIME
87673 588 124 490 473 206 724 846 353 800 103 866 326 585 232 637 209 353 861 989 515 836 828 349 243 037 267 69 IS NOT PRIME
52266 998 410 169 646 365 947 939 745 009 777 258 539 037 181 937 826 632 057 864 222 653 127 491 150 493 553 08 IS NOT PRIME
13367 007 129 382 094 479 506 346 799 116 537 199 357 619 359 997 488 913 587 607 669 118 823 081 278 434 037 51 IS NOT PRIME
28477 623 402 915 461 640 791 563 450 397 756 094 290 068 403 530 755 150 398 415 845 073 663 604 301 344 469 46 IS NOT PRIME
53968 867 747 531 637 377 378 560 066 545 074 003 225 144 987 605 048 866 002 947 007 144 855 066 324 584 248 74 IS NOT PRIME
83879 314 488 098 719 144 671 502 457 558 428 667 376 055 605 996 272 902 959 892 869 862 207 943 288 252 046 60 IS NOT PRIME
87398 616 924 508 563 913 021 693 570 998 729 092 756 950 394 216 150 224 846 972 450 139 646 921 053 330 584 62 IS NOT PRIME
70638 452 035 260 945 653 898 389 464 018 649 884 784 772 433 926 491 274 281 968 814 520 176 174 655 291 584 79 IS NOT PRIME
21551 832 621 833 704 371 328 357 162 627 623 879 427 450 637 929 678 010 867 860 083 551 903 518 327 294 529 34 IS NOT PRIME
42167 556 022 906 780 218 634 710 882 267 025 434 604 663 076 464 070 650 767 171 078 500 665 972 641 852 642 31 IS NOT PRIME
28760 754 610 710 476 055 500 876 150 534 438 715 629 738 022 966 144 325 447 421 338 461 885 391 169 002 386 32 IS NOT PRIME
66459 956 018 210 015 689 513 056 300 596 457 043 796 210 680 470 328 181 068 524 996 180 132 432 933 461 188 4 IS NOT PRIME
14554 929 269 074 422 030 285 921 341 682 372 320 704 761 226 009 370 065 708 020 639 893 586 933 839 436 205 77 IS NOT PRIME
24643 547 427 310 978 582 545 546 133 829 167 537 606 533 695 431 073 751 034 894 070 212 669 654 061 373 358 28 IS NOT PRIME
86113 595 697 728 817 640 496 163 760 141 461 030 442 597 858 068 591 938 306 835 238 490 757 267 767 096 000 86 IS NOT PRIME
52136 033 935 506 637 574 066 304 548 992 209 081 337 457 830 931 607 593 287 244 048 650 284 915 198 035 999 41 IS NOT PRIME
81928 157 440 032 833 367 502 536 277 888 877 368 548 658 996 033 685 035 862 741 007 972 938 413 122 266 424 35 IS NOT PRIME
31634 559 088 662 234 733 356 146 056 090 554 773 064 708 990 495 672 005 978 219 778 018 539 979 018 304 919 10 IS NOT PRIME
61307 955 659 077 648 389 108 804 662 222 600 040 249 500 488 248 467 393 016 458 704 005 963 883 534 348 639 71 IS NOT PRIME
64399 583 044 784 404 212 045 900 911 149 827 888 546 904 131 431 765 160 179 283 048 258 712 893 555 625 310 18 IS NOT PRIME
14316 249 765 239 606 342 775 766 932 301 471 522 879 070 538 415 537 255 546 962 851 862 083 364 288 803 350 43 IS NOT PRIME
70409 336 570 517 615 298 417 883 273 022 373 566 993 959 691 303 058 598 119 479 001 367 352 525 049 595 799 98 IS NOT PRIME
16727 337 588 301 340 457 882 559 323 668 751 962 227 255 115 573 784 224 507 859 070 309 855 265 300 919 775 3 IS NOT PRIME
55544 713 448 723 821 428 868 361 173 090 165 643 972 656 406 549 046 991 030 245 190 356 841 860 152 265 107 08 IS NOT PRIME
94380 714 741 384 411 103 365 846 503 275 640 841 027 164 332 630 050 482 649 192 475 454 159 495 338 476 224 16 IS NOT PRIME
36165 892 778 137 497 826 762 867 769 467 479 933 502 078 514 371 848 606 453 756 843 421 609 430 876 851 114 71 IS NOT PRIME
57399 889 359 772 011 220 673 388 196 045 290 699 417 796 037 750 019 677 514 014 193 175 113 743 762 652 768 98 IS NOT PRIME
22804 798 705 138 828 296 209 826 287 265 709 460 205 676 421 025 021 153 564 700 934 630 795 749 272 641 541 60 IS NOT PRIME
39180 616 487 755 801 477 645 329 289 132 797 064 610 409 107 260 853 806 247 781 361 145 832 283 583 754 611 63 IS NOT PRIME
59388 803 083 530 674 468 608 241 194 168 212 962 870 818 335 163 214 234 144 388 432 924 377 791 034 000 843 18 IS NOT PRIME
69906 043 193 070 784 044 069 071 131 623 262 254 284 439 340 569 099 163 399 620 592 202 066 876 582 445 989 5 IS NOT PRIME
81243 421 407 070 621 120 506 619 060 144 677 235 082 269 315 220 252 583 469 482 977 464 716 777 562 461 780 16 IS NOT PRIME
49428 163 892 649 632 764 438 241 999 360 706 988 737 725 287 687 822 374 676 425 705 168 579 923 026 711 123 42 IS NOT PRIME
22862 689 111 867 720 254 659 244 340 227 620 006 060 607 924 518 034 905 839 517 449 715 498 755 193 141 198 36 IS NOT PRIME
66540 339 797 726 876 774 351 395 459 158 487 836 893 047 293 185 460 517 946 309 778 809 470 455 665 544 276 9 IS NOT PRIME
23093 791 082 485 252 143 754 062 955 401 331 336 163 817 232 410 014 211 257 914 087 190 679 199 101 048 229 58 IS NOT PRIME
59886 023 954 928 704 452 443 462 982 737 489 025 036 773 597 427 036 650 610 025 316 296 358 775 108 073 018 19 IS NOT PRIME
29006 163 427 315 367 112 197 074 816 311 657 470 075 209 126 569 291 879 894 097 667 198 574 294 976 127 988 52 IS NOT PRIME
24772 469 348 346 628 271 954 109 433 784 239 948 048 573 197 309 752 189 531 621 216 456 361 540 144 273 934 71 IS NOT PRIME
20744 492 163 424 774 957 362 640 762 923 390 399 001 757 759 187 019 832 758 421 413 936 217 964 711 251 249 55 IS NOT PRIME
87720 360 994 294 106 488 548 011 031 197 962 813 306 225 955 582 069 683 526 016 003 937 502 393 235 233 374 85 IS NOT PRIME
99471 897 674 502 634 605 703 938 375 135 920 236 502 152 700 624 807 563 622 802 181 151 498 672 965 794 677 54 IS NOT PRIME
54119 803 799 633 901 446 733 885 077 927 617 515 354 863 936 519 468 295 517 450 186 410 709 602 362 208 872 40 IS NOT PRIME
72517 722 271 654 349 057 982 325 251 244 313 073 540 134 736 320 846 676 032 818 402 873 087 882 296 417 808 59 IS NOT PRIME
90864 805 550 888 888 138 011 686 773 537 683 357 447 852 768 779 079 535 374 810 137 398 054 801 375 692 367 40 IS NOT PRIME
31039 503 268 299 245 264 334 542 877 326 966 924 440 424 890 020 728 006 572 522 320 791 180 617 194 074 142 32 IS NOT PRIME
96200 462 229 904 710 278 591 921 575 012 048 489 117 387 292 629 876 966 727 959 408 714 935 896 947 951 501 96 IS NOT PRIME
29831 919 090 802 122 789 200 845 221 043 597 909 279 327 207 880 163 976 634 577 989 162 371 902 105 445 355 57 IS NOT PRIME
95076 006 471 252 912 395 483 848 432 684 429 521 224 159 294 109 547 555 128 699 665 277 136 993 251 963 946 39 IS NOT PRIME
88230 687 501 025 123 452 881 623 972 864 017 328 943 516 542 644 466 163 505 468 894 917 459 625 150 017 166 28 IS NOT PRIME
79063 498 856 865 490 078 742 916 496 099 978 385 893 631 082 347 102 361 489 671 679 749 947 842 479 646 991 32 IS NOT PRIME

1630223481195430597744463168834784071728462899196317964114508647833890230015527416430 IS NOT PRIME
540924028597997968939928609065116169038028464520317538668639396166868052891769079237 7 IS NOT PRIME
634833155781967924873781569465343786700706311121812217884075639163461463293896769622 7 IS NOT PRIME
509403026514855220271289641728957891408513754746682809389860526355846957011188595186 7 IS NOT PRIME
668457459076888489070909560210714816950136317585016941756056718653070712418291739705 3 IS NOT PRIME
824192038553854783469300035533746205497842577211189487207589599641013829807540384898 0 IS NOT PRIME
932883389743054477999724371096768035203074804050163052717156000564042634688760986207 8 IS NOT PRIME
918962275273543789447692640987554634755831360919213101696120134514182465585133229771 9 IS NOT PRIME
769064677965858950872768478748014182291025215485474008769887379497392507308783295492 5 IS NOT PRIME
123142457554237427733596928039868250650483122221243450895344597441253537437932903429 IS NOT PRIME
653003167667849196979384772191232656677448879121803503903887450489059059245217866120 IS NOT PRIME
525277771062155073616947632313366825585477044368190265026846315294279490430390147602 IS NOT PRIME
363193712449054813092414896994995438203137822032112862705811334162384089771935564789 4 IS NOT PRIME
262492470627016804068233262435896681984556548334078133544983484449998827657712305442 5 IS NOT PRIME
514609175304809287535371561197360059577724050193972103747762888173343734261918634046 8 IS NOT PRIME
424940849390392871782815204567194286434233686375590374863147338118837089414276264254 1 IS NOT PRIME
372133503986838920149761138050669530559982828019335112626515819197194799268941893037 5 IS NOT PRIME
393389895568073868914829127127147842771200331911697994365608578835955914043223739668 6 IS NOT PRIME
900410999256038279310906316096378199605766274241325692400435161913220173601704572982 0 IS NOT PRIME
916153168622514611466259473777125769095300792954482154655466254873375431325852813336 IS NOT PRIME
627937506250771992039363124940042194659147298700063223778479042351780120389778671583 8 IS NOT PRIME
147279796278274395056015961266516662942390448914424009587352452441452691033432446772 6 IS NOT PRIME
188625087142819116571486438214120413740373700795247371474465145274609982338541022927 7 IS NOT PRIME
558938991163096341006032580883771283682695801115958740809050319004759770598917975012 4 IS NOT PRIME
998057413285093523607743540392871060540178472866191858133548764907382024228998568967 6 IS NOT PRIME
495082813965087076884182931430584386246019492460740207009473644565799316022875749299 6 IS NOT PRIME
346178460876828725311359645754154220079778534762220183997077729015071398037986270231 IS NOT PRIME
161526062831419196629583220909063211088495752891140775051916238344369297399642695440 0 IS NOT PRIME
216804875364587516554612851874025059146683510979774183266850574190605087557306102110 3 IS NOT PRIME
59897928309335178503283336100806527044971144891022232768841047437917525088431587390 IS NOT PRIME
685524289654270304880483045903036886439960419637416471606609514442063399784912457735 0 IS NOT PRIME
642861372707044795209045423319073309594795350448092322104117681203801302841507904043 IS NOT PRIME
945243154191921353895328285703556472009082406315476582910395942435882577398573778102 3 IS NOT PRIME
743401408143811177030561486679454755928137005095565891303840767820698344777688045075 2 IS NOT PRIME
651356910425007400891554122420257684356416121822877741078527685412204122126346545235 IS NOT PRIME
538773576772657574054417748853996309833356108269349222858381268107187473659281557536 IS NOT PRIME
234966747711017510107292918974372260350610361675795068726043072813849448562755957257 7 IS NOT PRIME
268980079596344247586847543310508042809164474690979332804261678631273984190580299596 1 IS NOT PRIME
348565041568914683256930574560972782432479165799629878959288688977261115195580344621 9 IS NOT PRIME
782179903343229487461156923802759993914144469379166468767537364664641611606713182939 2 IS NOT PRIME
371772783308437858937823068681251808886595275384561445859102356972930857077553370389 5 IS NOT PRIME
571354879937164625491902631668410997806284697976418127974035097019657582182127885350 9 IS NOT PRIME
398002049506062895452125405070907636312670332931340395173219020020886176273243778481 IS NOT PRIME
528634017335089791701962791084963686522033833631993595941404598399973417238910899502 8 IS NOT PRIME
188914643953507539463966651816277179828611284955202019927988516766103131324791294042 8 IS NOT PRIME
108632998544734622995868459333809980544123491693436897428742730173792119684368209810 8 IS NOT PRIME
893756499164082207372545722920862455525990299570587307553956945767273729307992052215 IS NOT PRIME
700714248285200551251702474489253457292751424720133270220379995256866455379994161502 3 IS NOT PRIME

BOB:

133380942536715462687465592852529689122398754355361623408958729865088217421659668972 3 IS NOT PRIME
904433795236456895296284512718198977127185392523323499028752208321284723376643277123 6 IS NOT PRIME
358207035043910819135695098070264072545150740272735863872115661944513413452290445941 3 IS NOT PRIME
559547978839629421516871121285318232778821864532469447709660023264927568106741837181 1 IS NOT PRIME
231050837087813342612232176196793156243434007184104282211056090670749193841330075144 3 IS NOT PRIME
145806554908733713768634487075612917390753124363792749410933379918910367799334105240 6 IS NOT PRIME
140429383218432252098751999195477349351550016774318396694836614952539486707453749995 2 IS NOT PRIME
167826284777406574851302597541648618138690982840835637796128659928604888650058160062 9 IS NOT PRIME
831096286811317591376630768250126297660244995400635241739991999942758821642383411161 9 IS NOT PRIME
259689167822049308641811114252923468319508653950560351145277023066840335100233823340 0 IS NOT PRIME
108823893744056824531595126015940317929317188344117657853576403217030138815771566566 5 IS NOT PRIME
100621794536225473360848824095797596507249122550301805692916978825572857448930114597 5 IS NOT PRIME
394351086147871625642856850935529204806638297456911226983159325757120548015058474512 4 IS NOT PRIME
121033273137307919226169973595459267922650263412395119673243029795021654442983107154 7 IS NOT PRIME
654753218076511657653934165034557792653696039058576671666071222249895495703997419394 4 IS NOT PRIME
621723719435544067903596245011161702054567689736450954704938579454910078058274372723 5 IS NOT PRIME
887021850582228516378594223340301663578787793817687180309191976990854161215387790782 5 IS NOT PRIME
681105632097308257486921953818643750253286505012344759746113963585079575343006957074 0 IS NOT PRIME
908924383631663869404084810225543825887925916756435735445186709477257419722768764299 7 IS NOT PRIME
364615864399287292731423523208811441450417934689561620832714663986272063230097368968 1 IS NOT PRIME
474195573427751627630473450178820425269468152904666570633595008667973451211070689395 5 IS NOT PRIME
235872548097489121491035936600817581879977613298500705134379373815073001096121479868 IS NOT PRIME
439871923161685144132104077299742265700506935770583752522850002205498890460532526978 1 IS NOT PRIME
775686676470603714678994973048649380038358089883239161756984496615021170725955256234 0 IS NOT PRIME
380147774730137279700366488211517529729823626325571925878285902013168041466122848409 0 IS NOT PRIME
179587487927670161100101845907985459628204259305254418032089834983281665936499947822 2 IS NOT PRIME
749156902951842626277619068972395386464395777435879936612390531099695766324086895451 IS NOT PRIME
129353020275357783660741508845746690178822134407358001588544816597312353971484367533 4 IS NOT PRIME
633862474469151118859897047692336232365706538201117808365719878418171677408335720368 2 IS NOT PRIME
854085428567046401759427572011910871179071777719958001376604353886684602867506922617 2 IS NOT PRIME
100353825595494280366203828059522896902452145288362825620769082670038798687611163005 2 IS NOT PRIME
510059030167912238211506944707284667189299139254663173751198884628249794579349439195 IS NOT PRIME
537707974859943878425620309885761217320529334373287951999171090601485664138497454757 4 IS NOT PRIME
256700970413640532200318930034378100320542711679845872739366848283177486104484705434 1 IS NOT PRIME
916875499817904711585822961373846377190800168940821996205668282140901006241360406653 8 IS NOT PRIME
724065595229806377060841551995282050275755501487831073540921567679709867907306553541 9 IS NOT PRIME
686297860535808156151020017406597545963098210048403269470934996692683741686742255012 7 IS NOT PRIME
801212148220022754309522469817260128266240964239286421345702976371892316463212827438 9 IS NOT PRIME
246135279643643529055287901621489769280092344408341511976762803724853749856028186053 6 IS NOT PRIME
401955737408209358021773383709031489698984952536392362422944778336899990392438081719 2 IS NOT PRIME
535181272942910971611166605832389645843450967641081578459870786507947207934954642273 0 IS NOT PRIME
707335718480989301911687453145238343434809649842635527307289379261057113803282630891 6 IS NOT PRIME
488741638308143717337214405205967513212094654388793430548542999588547538486667699605 8 IS NOT PRIME
285614992636159005297533028784229025647958026071165711878371511677374241412618599284 1 IS NOT PRIME
380710323364237561006005916827782929100307300939746986639895429028302790997791749678 9 IS NOT PRIME
485579498564702897753404360981242561808641382831470790200350259978559315510950504910 3 IS NOT PRIME
759382017912164374273267348707181926207595682902793207962081167056754835021676846529 2 IS NOT PRIME
422051995369630636614886118455191621663100356292305968088394054918066995251434946295 9 IS NOT PRIME
993021841452727793948522577731876535996889766180802673223426892444400075029905411088 2 IS NOT PRIME
780050854662629991709875391440215147830102486778076213509569520548336578210641856634 8 IS NOT PRIME
607038819964360361540659454783474057828010860555789764979061649356160420768730820690 8 IS NOT PRIME
290952971606171711033527103267777677966797705234186760007898740534070353967410117132 IS NOT PRIME
443715364970533080256251264512682046325243200041697313967519620006042357744387779409 3 IS NOT PRIME
462751980210258243122748828432033230692621022802172630024624537145381032607820117801 IS NOT PRIME
890838231243519735448913764929416192597836132820875831732009069154752577147565851413 5 IS NOT PRIME
736310790422547285571197912392907205108309711271115742636318493035759557885715723467 8 IS NOT PRIME
884079744879173546460767002955230272536543260303595891302586181692584313465764689260 8 IS NOT PRIME
961025658244025023439585606427039373130852903387397245733460780302491446190091786391 8 IS NOT PRIME
384554040254237002587533159215167478952297317720962283310234791172552323281677975517 7 IS NOT PRIME
410527533685418260666331241482714904354660749390882538910976958990007851570751878569 2 IS NOT PRIME
638589075399803084248055291249275121344832763707373387095089559577742263719787084993 0 IS NOT PRIME
631263118574867127142488074284116923519362095597146681416555992408971265476564111096 0 IS NOT PRIME
700178699736680992004313932173619332430955533655514683094548365293756470085484677754 2 IS NOT PRIME
151718109505099119022234870582727868194854940208743593404188811092970230823292762235 IS NOT PRIME
967699079196375476301469874999057538157414042140952363489104022776543002293165127235 6 IS NOT PRIME
366431337491816973674939943145603038066383696107097083760992910818664449732262631278 4 IS NOT PRIME
194255733513383701083455557862345468318436877410332801494397727786659149199168991693 4 IS NOT PRIME
721556391232551656242872831741032260901459045957296903727277538158649818461134059360 5 IS NOT PRIME
688435262585249392996725352849618836149601392438757090650767778741965984408659001564 9 IS NOT PRIME
225673457650932046890717252055012221417345519698853442468363800550885792957685336860 3 IS NOT PRIME
293688143251424417512548640257312286358021721779711060147736700785797978702440352229 6 IS NOT PRIME

89629657951645624722497208750382770802117870895196813801195126181397769691325867891 13 IS NOT PRIME
60460443818263037730948106527488529769475804039535652259974498405215275649141884797 80 IS NOT PRIME
95994463490282060293798747351060421141122266105607468309165001522178477301170400084 14 IS NOT PRIME
77839857767968966327203243266536410129282673974947150604341323739678944893518686749 84 IS NOT PRIME
43467270735058204937448762631449975678234460289960156280447465976857158914576107452 3 IS NOT PRIME
73662895353336546811603677832213712510347187884938718706733212767060089945722324559 39 IS NOT PRIME
41993979815518968524070288935061686938487882145550812213593806010466903834851224926 6 IS NOT PRIME
78022090803884226368669513951385749268526871798950935243843545802858545516334777294 77 IS NOT PRIME
21734879511646232853370381707275017953761288464399757961893834001277679826871451435 61 IS NOT PRIME
95356215862960641099564752716460504583610099803198941476993174475613608043524931360 08 IS NOT PRIME
77135393840233694906193872333640269276001888031323395557295208631647927137509767153 3 IS NOT PRIME
48702624523903521922636680581362267801164274079170397666034694888155165596113433548 77 IS NOT PRIME
44214899974423922456146317323415171501412091241715354081435369898692131921865443170 92 IS NOT PRIME
22263252832747995141811948325179362198096043337159239075565246019464211237602747441 07 IS NOT PRIME
28333288683570115562553825217983450586820538247399808826238999733977139409233172334 59 IS NOT PRIME
81250111653073698493235775131906866628582281394051841553367877049137839481748029758 73 IS NOT PRIME
79567155020620401310084693430015981653422346493608653016824720492840270434065848994 43 IS NOT PRIME
55717710408523890560278968222864863193553209300814710872673357166627342645057571778 39 IS NOT PRIME
94211818980624229699274795386897119104659196099552142552512745356736040372963809043 45 IS NOT PRIME
22199017500301956766764120697803131137461085812353428258220424580285696478263565356 0 IS NOT PRIME
96543967190124945492631073190798223553526651649930212269054205753268788485500795421 87 IS NOT PRIME
46469567443140486715954828953976129710032218129198994798795173654274898928670654705 02 IS NOT PRIME
26501334182682189413452984303911870388149944451485150894573702957224989848960099150 62 IS NOT PRIME
94189266148990891689667960544892584171581867095108464368091396916434125960090754732 70 IS NOT PRIME
42560416461751854328040167859561248925669675696779297749159110717950369895456264719 51 IS NOT PRIME
43388705695857072508550266346445830521411062564625949139184222847642470229315368309 97 IS NOT PRIME
58673304680761436928846745839871165545317864998757425771636085152807273235231871520 70 IS NOT PRIME
88502679910249777478778151297420353524483283555285287662664479013036810265591388712 16 IS NOT PRIME
44091771469043379829023213713111305164801755732679736783739777975435093851915148338 46 IS NOT PRIME
36894202334336790273171880135417070341864381917145970217843294624144730109628974603 29 IS NOT PRIME
88024880207326821928439233480394676935292584883254073367414112814343564967278943969 62 IS NOT PRIME
55946527528737573725323148346245196564170136585319152785301377874071068020352745942 6 IS NOT PRIME
63361024971078911829453265053360914726465499921415780575656414290980932769596498380 63 IS NOT PRIME
22697228662465643566697379865333040995090791985824704713321825837885153737903522202 16 IS NOT PRIME
13969093305070288093460137073929045079739174330893446074758299100166726190114590768 19 IS NOT PRIME
73761632948368635389948311395688214087461318654973862494793848604379655262858165971 58 IS NOT PRIME
36497680957934271066751550723704919390741121441084164691020815642390709998124257352 47 IS NOT PRIME
12087471207487683803978109527763125285199332046413360429884629297655462067464682656 21 IS NOT PRIME
16392484358554345664985583955236805750916191544014408003511523138082026102725904563 IS NOT PRIME
95528513832383709702098812740560250890233825711063610806798849264185018748369257028 12 IS NOT PRIME
86285514304916844774629311189782744087222979729218286076326969245760698507885299059 47 IS NOT PRIME
75082660517390734502110386138835399734031802079794838528029227150942420808300881273 89 IS NOT PRIME
37869735676316664166464792553114534163115482992783577982407652551229042866908444260 40 IS NOT PRIME
31156584502334712587523951414594262580642827961366691905756862323619106864301482116 4 IS NOT PRIME
41238761084367895095875766524015862594655000156640959221827345399054510358005092044 04 IS NOT PRIME
84530398523126823776493618738808606839577988888648958559390229484822097508935068687 16 IS NOT PRIME
59197359096615059931892137355563915474063742705144811404360078247882520045480707324 4 IS NOT PRIME
23364468618112127384049023812111786868098719434503315887610008836557361159825220077 86 IS NOT PRIME
46403062472242208471766000041385403150608752428881274024892195974116702842880699045 91 IS NOT PRIME
82766253933472764609411951892336943772543667866801327496123954100540891846044860463 25 IS NOT PRIME
44409708885083628098835363466298980211266311524594327414212723252897598249076115839 70 IS NOT PRIME
20914381755280363548613800681961058342130324754845099819893428043084233094426491319 32 IS NOT PRIME
29682653969674508950619952770410555087357617144531479975838908173020650443758420004 44 IS NOT PRIME
85181281942614728944573040131314183561017401087398346492614808296538877104006286747 03 IS NOT PRIME
50157739291851465268417642189173244222805805829538655338187237295520640695690161057 30 IS NOT PRIME
34984342310280905669386943807742842080200757516384476407113554429782479404555744076 1 IS NOT PRIME
71101413364784697415126753592593671940312884062876842183469227867223282493459286518 15 IS NOT PRIME
93816438622374818151465652029550735666270906683483039866517133626115263662651547915 25 IS NOT PRIME
78811118742727214808367628104126762026337272868732199126090623737676717489984674184 73 IS NOT PRIME
33706941476734152070637626818588029778394048475676407853023662126972312000329831495 76 IS NOT PRIME
66687576801871652288605025882793267197739910876215115944875184665584548375960956055 05 IS NOT PRIME
66018962080222244667311035245334430500939808869680419498440259767074464646809775531 69 IS NOT PRIME
47730756326866021197735413684625795558872067655406416222332692504323263452305917446 90 IS NOT PRIME
65045545484652822527419262711006470971101823271285401936954117260953053612103410614 71 IS NOT PRIME
57466775779946150352489611841137405599461175229447381214040707443650271584094894478 34 IS NOT PRIME
55329166992780201409487320828537476829197526032953828278871933124597059682399864020 8 IS NOT PRIME

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_message (), Sign().*

  k1:0x1359e19abe666342a75fc3757c669218c78faba8be678c1d6583c43cf12c24103ad967bdf3fc630ef9e59307e42ae1ad3a16c6db32336536d9e005864af4ed21f3082eb5894fd
  S:0x67f495cf669295ec9e87fc0ad31030d89376a8411c3ebae53b9dbdf057c62ebd3d50431fe1e2830ed9ebe0ca4cced739f07d8aa68de0d3b73ebeee19b882e0668cfa86130a8bd
  S1:0x3f03377b51e89deb6060dcf159e1dde4d3c6bfdc4e9e96efa7a795bb7b6bdc6cd995fb0cf98ae598f0111c56cb797725c0889d900fb3840086f8a4d958d07ec58f27949ac8e5a

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

k: 0x75bcd15

S:0x67f495cf669295ec9e87fc0ad31030d89376a8411c3ebae53b9dbdf057c62ebd3d504
31fe1e2830ed9ebe0ca4cced739f07d8aa68de0d3b73ebeee19b882e0668cfa86130a8bd
S^emod(n): 0x75bcd15

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

Параметри криптосистеми RSA для абонентів Alice і Bob

Alice:

N=0x796647a24decdb8364c76cd32c205805c57d4785d09e1e063c0aff53534bbe2e2292afed9bea28281531f
08f39b36f2beb0454c134369ed4e2d31a8b938a1f3c51a7211b05143

E = 0x29

D=0x67a23d26a66c89702a52d3888fd0af0b2bb5df65be93774a014e1227e9729c1ae551831d5d0f213f4a346
79819b628fab72b03dcc7bdd40dbb829f4d4cd3b758562010751f731

P = 0x19f1c85ecf6e463bfb938464dfa9b3169f50d091ead4fe9d1afdd0e42b60141e6de445f

Q = 0x4ade08bfa81ccb92febb43b5b8d876a00200bae14efef9a592604c31172d9955cc27d9d

Bob:

N=0x6e759628e33b938a3158f63c8199bcd8b8096c706db0d5cb92a88a58cb4ab7e10781d21935bb23d76b3b
bf9ffc802619ba82d944932dbcf94573c574074a8e503c95bb6b9fa03

E = 0x25

D=0x35bca9ea60b53304f5698c8c235f8c4dc150b14b73a222d1bcf80bf3d88536dc2d2a66052e376c8c5c441f
f933894228b3ce74c4429e0774d0883ee87ba34eecbc530ab6f0fdd

P = 0x4ceabfc4049c134e8e4260d5a2050e5b051edb54f20da579fdcd2a4e08cdf41181d6877

Q = 0x16fa341d24117ff675091364eb27688e3a40b83c41c40b91430317ac445d4c4cc7129d5

4. **Чисельні значення прикладів ВТ, ШТ**

ВТ	ШТ
0x75bcd15	0x1359e19abe666342a75fc3757c669218c78faba8be678c1d6583c43cf12c24103ad967bdf3fc630ef9e59307e42ae1ad3a16c6db32336536d9e005864af4ed21f3082eb5894fd

Цифровий підпис для Alice і Bob

Alice	Bob
0x67f495cf669295ec9e87fc0ad31030d89376a8411c3ebae53b9dbdf057c62ebd3d50431fe1e2830ed9ebe0ca4cced739f07d8aa68de0d3b73ebeee19b882e0668cfa86130a8bd	0x67f495cf669295ec9e87fc0ad31030d89376a8411c3ebae53b9dbdf057c62ebd3d50431fe1e2830ed9ebe0ca4cced739f07d8aa68de0d3b73ebeee19b882e0668cfa86130a8bd

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 = 0x29

N =0x5945cdc433c4c91b2086e06e3b1cb986e33a203ee80c0cdcd21c821e5218778702f50935682933f75a8327c9725c127348062737c0722d7de80b3a78d15a96e1a59851e63f2d7

D = 0xae30c9b0c8ea1e416b2ca32e7fd425521f45b58d79d912da93babf735b80e939636db9dcf1883975202f9456a0e395516185c87d8d536d911cc47f92caa91126b99090ad2d19

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

keySize=512

Відповідь:

n1:B8A898327F08B561AC75004CE612ACB966B677C0DC647EC654B124665EBF80A73CB11F2461813C17B122395BD68620DFFDBE30FF66C770BF96CF312452404A2F

e1: 10001

- *Функція SendKey неверне нам значення:*

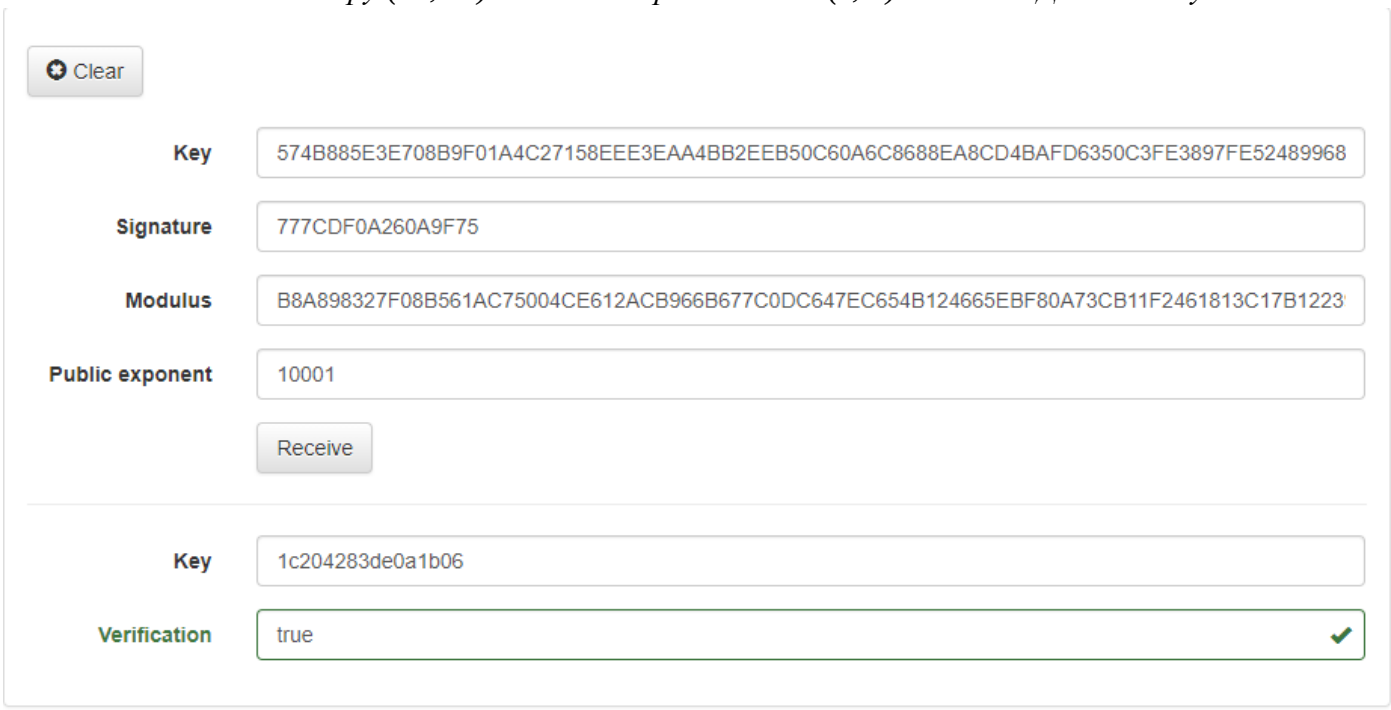
X = 1c204283de0a1b06

S =0x49d48c0339f2b2d042b430a2ff8e963f992bdac6652f2049a89aad41791995f1ef9e8dd905fc155e2f370dff5bd688f26d67f6ff2c0e4581517dbd439d5562cb1a87f9f736e

K = 574b885e3e708b9f01a4c27158eee3eaa4bb2eeb50c60a6c8688ea8cd4bafd6350c3fe3897fe524899685e2ba88571e9dcb93e29e888220e230a415d15748ed1

S = 777cdf0a260a9f75

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



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.