МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Криптографія

Комп’ютерний практикум №4

Виконали:
студенти III курсу
групи ФБ-82
Боднар А. В.,
Казміді І.Д.

Перевірив:
Чорний О.М.

_____

Київ 2020

Робота №4. Вивчення криптосистеми RSA та алгоритму електронного підпису; ознайомлення з методами генерації параметрів для асиметричних криптосистем

- 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.
- Дата: 23.11.2020

Завдання до виконання:

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) , (e1, n1) 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 $0 < k < n$.

Виконання роботи:

1. Значення вибраних чисел p, q, l p , l q із зазначенням кандидатів, що не пройшли тест перевірки простоти, і параметрів криптосистеми RSA для абонентів A і B. Довжина: 256.

```
Not prime:
791751593661124782413964976548298500472472187376333875569741822827255871197 23
169706607243638928963906975774390031399988352546716834534693156377838074405 21
Not prime:
169706607243638928963906975774390031399988352546716834534693156377838074405 21
122268843560308722062977861450267232590150840687867161251962392342637871327 21
Not prime:
122268843560308722062977861450267232590150840687867161251962392342637871327 21
389431305070093121153689005634730624555261355091340820119860958369521919167 7
Not prime:
389431305070093121153689005634730624555261355091340820119860958369521919167 7
261352962458267667306521552445605468517950896965825870853602443933292091500 59
Not prime:
261352962458267667306521552445605468517950896965825870853602443933292091500 59
308375180235050078766359905744857544627029113480782535819848031406034609269 59
Not prime:
308375180235050078766359905744857544627029113480782535819848031406034609269 59
891504931100376856181311096206542811258580066877284871242965521835233259385 65
……
```

Перша пара

```
q:  74278233820186835633367661071763032575742635783780423104404959312327819426 87
p:  74715597100194796603875329066225831279404564510104748719487417255157181034 303
e:
28421796643601362966002480097492353842591119778552424700442323224031233375441155696210 2
80596638307343608907025685403736688660906436791822472396145374372 7
n:
55497425914231426055966514862646284057861722060672207665890414438800740022419344188259 7
29026905312739232675000708612720281227897447849669179660432699216 1
d:
48398988913527345523919726174065489310500743230779856002970045869820698988740335894793 7
81386702266974465420670279635046366293727544572517496674178046246 7
```

Друга пара

```
q1:  59676746269868460623604059519564159516541652067848736270280456785466791955011
P1:  52124791003149659466249589849481617729045303587250286776422606080037147024071
e1:
82172120828193919447807913870780191771622338188146877017217864346557537881843417956819 6
00446116392558697430552280085314790951562243058210763037179281320 9
n1:
31106379270648845363009573669058741763444319469139394951749811282283328397828955020406
40003965539957408770682197810762120740010429493452706039427660697 81
d1:
72449660071368310016150811905769651532066682048104218822291805402103403066855003869501 2
85355234465301473744266468936656976635954837113105023115325456978 9
```

2. Чисельні значення прикладів ВТ, ШТ, цифрового підпису.

Приклад відкритого тексту:

0d1150d1110d1090d1010d320d1160d1010d1200d116

Приклад шифротексту:

0d48215065789865508658869466584871301783749122633657251901390763933959131969279561093885666377060645439922487274646871820870397175279062238072812832402009300d2356649884778264662928764433579847495319073001532128469315504142297647308199819817853095177088443449932793130769769679821544195355279070353699459221127820d899493213000523083483671230467282621697692138197511699125970207703522053215972133560801704717508272357178885949514167054716083442303567715468127051049287 0d6968113164744092661224927455327034352408058975449474825973332817279882447911842730372111647428723427200609372038345773428666135323630724600091820210012360d153792413703619478381416976024102658894452727728902476037958989913831156633243783385464715873942815730968155837988068308607666055034834379957225551947133 0d1236404046477915729068444646304259904841410616660236899159102751522864961420097906821437580433200d6968113164744092661224927455327034352408058975449474825973332817279882447911842730372111647428723427200609372038345773428666135323630724600091820210012360d153792413703619478381416976024102658894452727728902476037958989913831156633243783385464715873942815730968155837988068308607666055034834379957225551947133 0d1236404046477915729068444646304259904841410616660236880609197576252275332135741845090391849206614330737753034889815910275152286496142009790682143758043320 0d4730239523548978423532550403682317802160346409035082866936806437787432962549344628811903447153079399691131048583784057236680767652542588925887622954481950d2670767583766988528770594132404849678707376950313193089372824872254013929502868215352005749776988627584648653234274659612873694967236121345436529623603260d534675672640887750143812663746688132554683266046155439104148656116265958152104955681627386417387538926928692699721087489207539623414796842663890484435877 0d1360802949272704849125304174021665403163704936403827202970175011403406836634674331708366901084819488068418864390436443112418566411421231275724361500200946 0d8741479983552260445903662740143451270129877888885379124927298294162093484853152190016656808575470387262869975601403028099327066390442722356468449722377300d534872924446304432612131959677320024153406447092519720855696704706681340430991932228213816838838857332443834961624059921469961308133392972439446983673297 0d4821506578986550865886946658487130178374912263365725190139076393395913196927956109388566637706064543992248727464687182087039717527906223807281283240200930d2356649884778264662928764433579847495319073001532128469315504142297647308199819817853095177088443449932793130769769679821544195355279070353699459221127820d899493213000523083483671230467282621697692138197511699125970207703522053215972133560801704717508272357178885949514167054716083442303567715468127051049287 0d6968113164744092661224927455327034352408058975449474825973332817279882447911842730372111647428723427200609372038345773428666135323630724600091820210012360d153792413703619478381416976024102658894452727728902476037958989913831156633243783385464715873942815730968155837988068308607666055034834379957225551947133 0d1236404046477915729068444646304259904841410616660236880609197576252275332135741845090391849206614330737753034889815910275152286496142009790682143758043320 0d4730239523548978423532550403682317802160346409035082866936806437787432962549344628811903447153079399691131048583784057236680767652542588925887622954481950d2670767583766988528770594132404849678707376950313193089372824872254013929502868215352005749776988627584648653234274659612873694967236121345436529623603260d534675672640887750143812663746688132554683266046155439104148656116265958152104955681627386417387538926928692699721087489207539623414796842663890484435877 0d1360802949272704849125304174021665403163704936403827202970175011403406836634674331708366901084819488068418864390436443112418566411421231275724361500200946 0d8741479983552260445903662740143451270129877888885379124927298294162093484853152190016656808575470387262869975601403028099327066390442722356468449722377300d534872924446304432612131959677320024153406447092519720855696704706681340430991932228213816838838857332443834961624059921469961308133392972439446983673297

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

- Згенеруємо пару ключів (e, n), d довжиною 256:
  e:
  `612891351365653694691120075076430751002903924824185164782982829339783256847593560227884520705671412116210044976118517150942875728318966990837865545188413`
  n:
  `103194935976356400386365555840062364528693673925624299880703884834650688417910319677614305110504836879167883237085558451466760260316115895429873326698256 9`
  d:
  `375062526353822190350363842347330970538455887944872663072946095325963309582132874023917373306828127442856837718214903866521719484305504015885250619850877`
- Надішлемо сайту запит на отримання його вікритого ключа. Дані запиту:
  keySize=512

  Відповідь:
  n1:
  `795325432370452665300505292516508793853358995475677447478600349998041370771022413280605672599993215198209417258068925541822378009214894825085891959129 3167`
  e1:
  `65537`
- Створимо цифровий підпис ключа k = 123456, за допомогою свого закритого ключа d. S = (k^d) mod(n)
  S:
  `776235773954037234459136391298028228307666926243876613751625336675372962282426817728348420479734977462709665395946619399104078329372257563105957469155578`
  Зашифруємо S та k відкритим ключем сайту. S1 = (S^e1) mod(n1).
  k1 = k^e1 mod(n1)
  S1:
  `750175049709455477729844428563728576031927360938015252296375582842311764924839871675860309080040240925623328343300246601277031625956769656331555221808 8612`
  k1:
  `155891776173943207508245855638152365082572096777461731772156296861192634824267834862082314871783416023592338794077109023277572724228120096549322697934 6927`

- Відправимо пару (k1, S1) та свій відкритий ключ (e, n) сайту. Дані запиту:
  key=1dc3d4cf9c064b6132786b911979eedc8e9d5c54ef2a99827ce37a6c0573ff0d7bafea9465269f34e668d885f4f6a7bb11228f8885da7f18d4aabf7668e649ef
  signature=8f3bcae8b8e940a088ddf62ed40a364f3d401687065276b944804faaa43f85ed25014d0a42b158b6fd2f69159f1d0d8a418360ab55f0e0c4087a20f689a984a4
  modulus=13b4103aec3e40883455c99df15079e7defb4d2a79646f7be8947c15b2b2488d4accd7eaa0ea5179ceb7caa43ed7d8ea4862663007591ad0cc789e532b53d6a9
  publicExponent=bb3c0223353b87435bc4f5c8943004a89a50f02ef969002fef949f8a4cddad7f573d6b39e81ba7b8431fc14f2692eed43ccd9e80437d99c700c29907bebc43d

Відповідь:

```
key: 01E240,
verified: True
```

Висновок

Під час виконання цієї роботи ми зрозуміли принципи шифрування та розшифрування алгоритму RSA, запрограмували та розібрали тест Міллера-Рабіна на псевдопростість числа, розробили функції створення та підтвердження цифрового підпису, створення ключів з простих чисел.