

Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря
Сікорського"
Фізико-технічний інститут

Крипто́графія

Комп'ютерний практикум №4
Вивчення крипtosистеми RSA та алгоритму
електронного підпису, ознайомлення з методами
генерації параметрів асиметричних крипtosистем

Виконали:
Студенти 3 курсу
ФБ-32 Баласанян Юліана та
ФБ-32 Дорогін Артем

```

Run: cp4_code x
/usr/Local/bin/python3.11 /Users/uliannabalasanan/Downloads/Balasanian_fb32_Dorohin_fb32_cp4/cp4_code.py
== Генерація ключів RSA для абонентів А та В ==
n_A < 2 * n_B, перегенеруємо ключі А...
Публічний ключ А: (n_A, e_A)
n_A = 9528491249620626153758586653395088047684727624388678348959242601994182015799144120931653484529783690468541175144827945221077434776814161478839878644177163
e_A = 65537
Секретний ключ А: (d_A, p_A, q_A)
d_A = 3487762247465425840755449699579820085400043113568637235152088982273804355056181464026977559939545919362556166960128539045510095295849397268265549288680793

Публічний ключ В: (n_B, e_B)
n_B = 91058419212016776414596481802995027169716139812068563963838877808908578025867317804067670581866489071467150489690554302812156433592996855404699592389223
e_B = 65537
Секретний ключ В: (d_B, p_B, q_B)
d_B = 6423010823462217893515901881500351574835838947652822497404572019370771586276288417478478372028827174146347368209613564086361933005311238165495219883543105

== Перевірка операцій для А ==
M_A = 9483032661409105397871834302856349324691739735414185704679284425114722574183410267139528983480509004388026485093241068616462679511267343398716650210058202
C_A = 913640966884782594308522465708074796835619675646245933111794584501166346279598399359862957029161783898715932066746608622916314910680759126740921876391
M_A' = 9483032661409105397871834302856349324691739735414185704679284425114722574183410267139528983480509004388026485093241068616462679511267343398716650210058202
Підпис коректний для А: True

== Перевірка операцій для В ==
M_B = 14254811332783880976356477875113234347757720059770217848856490213669308551664324463347613633591088685048111038511744695132008107468116375663322951456420187

Run: cp4_code x
e_B = 65537
Секретний ключ В: (d_B, p_B, q_B)
d_B = 6423010823462217893515901881500351574835838947652822497404572019370771586276288417478478372028827174146347368209613564086361933005311238165495219883543105

== Перевірка операцій для А ==
M_A = 9483032661409105397871834302856349324691739735414185704679284425114722574183410267139528983480509004388026485093241068616462679511267343398716650210058202
C_A = 913640966884782594308522465708074796835619675646245933111794584501166346279598399359862957029161783898715932066746608622916314910680759126740921876391
M_A' = 9483032661409105397871834302856349324691739735414185704679284425114722574183410267139528983480509004388026485093241068616462679511267343398716650210058202
Підпис коректний для А: True

== Перевірка операцій для В ==
M_B = 14254811332783880976356477875113234347757720059770217848856490213669308551664324463347613633591088685048111038511744695132008107468116375663322951456420187
C_B = 229491926979255694189033956261435156985187212111035242958632431763243918149754264704794683959835283693591334484978676863763841597637395047536770365498
M_B' = 14254811332783880976356477875113234347757720059770217848856490213669308551664324463347613633591088685048111038511744695132008107468116375663322951456420187
Підпис коректний для В: True

== Випадковий передаваний ключ k ==
k = 52892209172365941739892369735627021105415572217875132638147910481341325756313803742890033369626008642413878834360177107665339969278319944920256386823082

== Дамі, які формує відправник А ==
Підпис s = 9811049371413847665987439861987466739982277769485808689797929929347585961177913731894323317611406938772328211524618659368496640031215883107477449
Зшифрований ключ C_K = 14137250004253836904333095725798219267203521599928198164959151224644335259589758978511172082085658875644174661540288480034888955884338198984665039
Зшифрований підпис C_s = 66816684571701854271414238890521630264871939932659963162882236688768672351117205146220452965208678086017929791653011554883305244607912728

== Дані, які отримує одержувач В ==
Отриманий ключ K' = 52892209172365941739892369735627021105415572217875132638147910481341325756313803742890033369626008642413878834360177107665339969278319944920256386823082
Підпис коректний: True

Протокол виконано успішно.

Process finished with exit code 0
|

```

перевірка коректності власної реалізації RSA шляхом взаємодії з тестовим сервером:

The screenshot shows a web browser window with the URL asymcryptwebservice.appspot.com/?section=rsa. The title bar says "Не захищено". The top navigation bar includes links for "Asym Crypto Lab Environment", "RSA" (which is selected), "Rabin", "Zero Knowledge Protocol", and "Documentation". On the left, a sidebar menu lists "Server Key", "Encryption" (selected), "Decryption", "Signature", "Verification", "Send Key", "Receive Key", and "Oleh Chornyi © 2025". The main content area is titled "RSA Testing Environment" and "Get server key". It contains fields for "Key size" (set to 256), a "Get key" button, and pre-filled values for "Modulus" (89DB05AF612336714971B5396EB441B5AD9D7EA1766732F091471A37762BFDFD) and "Public exponent" (10001). A "Clear" button is also present.

The screenshot shows a web browser window with the same URL and title bar. The top navigation bar and sidebar menu are identical to the previous screenshot. The main content area is titled "RSA Testing Environment" and "Encryption". It contains fields for "Modulus" (89DB05AF612336714971B5396EB441B5AD9D7EA1766732F091471A37762BFDFD), "Public exponent" (10001), "Message" (123), a dropdown for "Bytes", and an "Encrypt" button. Below these, a "Ciphertext" field contains the value 3A0D34F6AA470D751DA5CD1087A1C1EC24ECA8504085EBD66D120464CFC63996. A "Clear" button is also present.

The screenshot shows the RSA Testing Environment interface. On the left, a sidebar lists options: Server Key, Encryption, Decryption, Signature, Verification, Send Key, and Receive Key. The 'Decryption' option is selected. The main area is titled 'Decryption'. It contains a 'Ciphertext' input field with the value '3A0034F6AA470D751DA5CD1087A1C1EC24ECA8504085EBD66D120464CFC63t', a dropdown menu set to 'Bytes', and a 'Decrypt' button. Below this is a 'Message' input field with the value '0123'.

RSA Testing Environment

Server Key
Encryption
Decryption
Signature
Verification
Send Key
Receive Key

Decryption

Clear

Ciphertext

Bytes

Decrypt

Message

Oleh Chomyl © 2025

Asym Crypto Lab Environment RSA Rabin Zero Knowledge Protocol Documentation

RSA Testing Environment

Server Key
Encryption
Decryption
Signature
Verification
Send Key
Receive Key

Sign

Clear

Message

Bytes

Sign

Signature

Oleh Chomyl © 2025

Asym Crypto Lab Environment RSA Rabin Zero Knowledge Protocol Documentation

RSA Testing Environment

Server Key
Encryption
Decryption
Signature
Verification
Send Key
Receive Key

Verify

Clear

Message

Bytes

Signature

Modulus

Public exponent

Verify

Verification

Oleh Chomyl © 2025

Висновок: Для перевірки коректності реалізації RSA ми використали тестовий сервер з методичних рекомендацій. Отримали відкритий ключ сервера, зашифрували повідомлення та перевірили, що сервер коректно його розшифровує. Також ми створили цифровий підпис і перевірили його на сервері. Отримані результати збігаються з

результатами нашої програми, що підтверджує правильність реалізації алгоритмів RSA. Ще у ході роботи було реалізовано повну схему RSA: генерацію випадкових простих чисел, побудову відкритих і закритих ключів, шифрування та розшифрування, формування і перевірку цифрового підпису, а також протокол конфіденційного передавання сесійного ключа