

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 = 952849124962062615375858653395088047684727624388678348959242601994182015799144120931653484529783690468541175144827945221077434776814161478839878644177163
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 = 91364096688470259430885246570807479838516967564624593311179458450116634279598399359862957029161783898715932066746608229163149106480759126740921876391
M_A' = 9483032661409105397871834302856349324691739735414185704679284425114722574183410267139528983480509004388026485093241068616462679511267343398716650210058202
Підпис коректний для А: True

== Перевірка операцій для В ==
M_B = 1425481133278388097635647787511323434775772005977021784885649021366930855166432446334761363359108868504811103851174469513200107460116375663322951456420187

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 = 91364096688470259430885246570807479838516967564624593311179458450116634279598399359862957029161783898715932066746608229163149106480759126740921876391
M_A' = 9483032661409105397871834302856349324691739735414185704679284425114722574183410267139528983480509004388026485093241068616462679511267343398716650210058202
Підпис коректний для А: True

== Перевірка операцій для В ==
M_B = 1425481133278388097635647787511323434775772005977021784885649021366930855166432446334761363359108868504811103851174469513200107460116375663322951456420187
C_B = 22949191269792556941890339562614351569851872121103524295863243176324391814975426470479468395959835283693591334484978676863763841597637395047536770365498
M_B' = 1425481133278388097635647787511323434775772005977021784885649021366930855166432446334761363359108868504811103851174469513200107460116375663322951456420187
Підпис коректний для В: True

== Випадковий передаваний ключ k ==
k = 52892209172365941739892369735627021105415572217875132638147910481341325756313803742890033369626008642413878834360177107665339969278319944920256386823082

== Дані, які формує відправник А ==
Підпис s = 9811049367141384576692598713986198746673998227776948580868979792992934758596117791373189432317611406938772328211524618659368496640031215883107477449
Зшифрований ключ C_k = 141372500042538369043330957257982192672035215999281981649591512246443352595987589878511172082085658875644174661540288480034888955884338198984665039
Зшифрований підпис C_s = 6681668457170185427194142380985216302648719399326599631628822366887686723511177205146220452965286724886078060179297916533011554883305244697912728

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

Протокол виконано успішно.

Process finished with exit code 0
|

```

Висновок: 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