

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

Криптографія

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

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

```
Run: cp4_code
/usr/local/bin/python3.11 /Users/uliannabalasanan/Downloads/Balasanian_fb32_Dorohin_fb32_cp4/cp4_code.py
=== Генерація ключів RSA для абонентів A та B ===

n_A < 2 * n_B, перегенеруємо ключі A...
n_A < 2 * n_B, перегенеруємо ключі A...
n_A < 2 * n_B, перегенеруємо ключі A...
n_A < 2 * n_B, перегенеруємо ключі A...
n_A < 2 * n_B, перегенеруємо ключі A...
n_A < 2 * n_B, перегенеруємо ключі A...
n_A < 2 * n_B, перегенеруємо ключі A...
n_A < 2 * n_B, перегенеруємо ключі A...
Публічний ключ A: (n_A, e_A)
n_A = 952049124962062615375858653395088047684727624388678348959242601994182015799144120931653484529783690468541175144827945221077434776814161478839878644177163
e_A = 65537
Секретний ключ A: (d_A, p_A, q_A)
d_A = 3487762247465425840755449699579820805400043113568637235152088982273804355056181464026977559939545919362556166960128539045510095295049397268265549288680793

Публічний ключ B: (n_B, e_B)
n_B = 9105841921201677643145964818029950271697161398120680503963838778089085780258673178040676705818664890714671504896095543028121564335929968554040699592389223
e_B = 65537
Секретний ключ B: (d_B, p_B, q_B)
d_B = 6423010823402217893515901881500351574835838947652822497404572019370771586276288417478478372028827174146347368209613564086361933005311238165495219883543105

=== Перевірка операцій для A ===
M_A = 9483032661409105397871834302856349324691739735414185704679284425114722574183410267139528983480509004388026485093241068616462679511267343398716650210058202
C_A = 9136409668847025943085224654700747968354169675646245933111794504501166346279598399359062957029161783898715932066674660062291631491046807539126740921876391
M_A' = 9483032661409105397871834302856349324691739735414185704679284425114722574183410267139528983480509004388026485093241068616462679511267343398716650210058202
Підпис коректний для A: True

=== Перевірка операцій для B ===
M_B = 14254811332783880976356477875113234347757200597702178488564902136693085516643246334761363359108868504811103851174469513200107460116375663322951456420187
```

```
Run: cp4_code
e_B = 65537
Секретний ключ B: (d_B, p_B, q_B)
d_B = 6423010823402217893515901881500351574835838947652822497404572019370771586276288417478478372028827174146347368209613564086361933005311238165495219883543105

=== Перевірка операцій для A ===
M_A = 9483032661409105397871834302856349324691739735414185704679284425114722574183410267139528983480509004388026485093241068616462679511267343398716650210058202
C_A = 9136409668847025943085224654700747968354169675646245933111794504501166346279598399359062957029161783898715932066674660062291631491046807539126740921876391
M_A' = 9483032661409105397871834302856349324691739735414185704679284425114722574183410267139528983480509004388026485093241068616462679511267343398716650210058202
Підпис коректний для A: True

=== Перевірка операцій для B ===
M_B = 14254811332783880976356477875113234347757200597702178488564902136693085516643246334761363359108868504811103851174469513200107460116375663322951456420187
C_B = 229499192697925649418903396261435154985187212111035242958632431703243918149754264704794683959598835283693591334404978676863763841597637395047536770365498
M_B' = 14254811332783880976356477875113234347757200597702178488564902136693085516643246334761363359108868504811103851174469513200107460116375663322951456420187
Підпис коректний для B: True

=== Випадковий передаваний ключ k ===
k = 5289220917236594173989236973562702110541557221707513263814791048134132575631380374289003336962600064241387883436017710766533996092703199444920256386823082

=== Дані, які формує відправник A ===
Підпис s = 90110493671413845766925907139306198746673998227766940508689797929929334758596117791537189432331701140093877232821152406186593684496640031215803107477449
Зашифрований ключ C_k = 14137250004258369043330957257902192672035215999281901649591512246433525950975890785111720820856588750441746615402884800348889558843381989846650394
Зашифрований підпис C_s = 66816684571701854271941423809052163026487193993265996316288223668076867235111772051462204529652067248860780601792979165330115548833052446079127283

=== Дані, які отримує одержувач B ===
Отриманий ключ k' = 5289220917236594173989236973562702110541557221707513263814791048134132575631380374289003336962600064241387883436017710766533996092703199444920256386823082
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