

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

Криптографія
Лабораторна робота №4
<<Вивчення криптосистеми RSA та алгоритму
електронного підпису; ознайомлення з
методами генерації параметрів для
асиметричних криптосистем>>

Виконали:
Студенти групи ФБ-92
Рога Владислав та Томич Олег

Київ-2021

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.

Хід роботи:

- 1) Спочатку написали функцію перевірки простоти числа тест Міллера-Рабіна
 - 2) Згенерували дві пари простих чисел
 - 3) Написали функцію генерації відкритого та закритого ключів для двох абонентів для RSA
 - 4) Написали функції: шифрування та розшифрування і створення цифрового підпису
 - 5) Організували обмін повідомленнями між абонентами А і В
- Скріншоти

```
m = 3079013521140198604418523158549033194067204198695096048278722898275893465169544386540799894201330928495609478041256031243034931154627153555561140108917026

m = 0x3ac9e793484b3ad43c6dd566df2f6edad09201dd34320f0fa1cabf96bcb670ab031d3dab41b3169f1a40d2d668f41a9c1e29495ff63a12e8df63be635d7f922


podpisOtpravitel = 2203850269963316321262359782852912956668634795486088115812822414934452381777540678357188163362818757321930419417384545715237212927263558962688070326616129

podpisOtpravitel = 0x2a14321b2b58c0f1a0818c85b6b3ff3df185e31c8edb3a35467ef64672d8cd1923c0b516cd324d09be0d0572c86e2e33e26795445871c9b11095856feab0041
verificirovano

podpisPoluchatel = 1973263347489511614843486355933647966607139127817861146077712942277203383698577922347824696943488661037965744053347754795652433837352480656309886596507000

podpisPoluchatel = 0x25ad1c3e74dda32ad4e48f156f5437921892836f5bf733437476ceadf647a469e278e8d41e426955e85afad1a628e007c0a7711a13e3251a1672b48619a96578
verificirovano
A otpravil kluch
k1 = 1357901356032858136533136430444907067328731265655017371409946606799836374875606075961844317393625348007814274103885050515921937706626884803229500721170482
s1 = 1015166054056612262395261787924735545018600296202588436518807955924635923339555636497913599889199403694865338226512142229755976709590387035330309664716595
B poluchil kluch!
Soobshenie Verificirovano
k1 = 0x5b49e0893d82df997c6449ea0a8daaa50356adf8336fedca4ba056327d5fe7cc7643e069b8484e787422637a425cde21e7d91ab68cc8220194bf9a29d37f4f71
s1 = 0x2c26006ce1dcf3601d0851a5bc74989743292f94677e80e0b7b8d858439182a04115d6c84e7a9e19587bec9da5c1e5ee7498c8cdf09972e2038592c0b7b096e4
s = 0x6408ccb568199ebf2f44794f534513781084d8e6f833a41f3bcf073a9e86225069c3399595a1c8a959e5e0a6762340f9b96468254354ce80341096b8b1769ff8
```

Receive key

 Clear

Key

5b49e0893d82df997c6449ea0a8daaa50356adf8336fedca4ba056327d5fe7cc7643d

Signature

2c26006ce1dcf3601d0851a5bc74989743292f94677e80e0b7b8d858439182a0411f

Modulus

656ab755c9b29595b8ad6d4bd75a018d5fce7407d5103a2bf71835f2d434434e4a1c

Public exponent

5329f731391e9e4796fae7733534cf3c5b7a4ef56d40b45d17c3cbad8fb676de2de4f

Receive

Key

05F04F69DF4387E966CDE1314C946ECB249D2C212D06E278C5F9F82615723f

Verification

true

