Комп’ютерний практикум №4

Вивчення криптосистеми RSA та алгоритму електронного підпису; ознайомлення з методами генерації параметрів для асиметричних криптосистем

ФБ-32 Будніков Дмитро та Кузьменко Вікторія

Результати

Генерація ключів

```
+------------------Генерація ключів-----------------+
Генерація ключів Аліси
public Key (e, n): (65537, 637584012146507338617524743022978500839252364863904756726675
private Key (d): 515635866942172848336146702316308444107634677243643741947714412723613

Генерація ключів Боба
+--> Згенеровано з 1-ї спроби (щоб n_B >= n_A)
public Key (e, n) (65537, 104406434337996560631248701995561585456516118450337479495158
private Key (d) 450844880260814908504255346823075952274197194278735778218866962097166 2
```

Шифрування та дешифрування

```
+------------------Шифрування та дешифрування------------------+
[Alice] Message: juicy
[Alice] Message Int: 457236374393

Аліса шифрує для Боба, використовуючи pub_B
Ciphertext (C) 27311895715728596145108743460783821378400269944403422093425670499201206490534419127 0

Боб дешифрує повідомлення, використовуючи priv_B
[Bob] Decrypted: 457236374393
[Bob] Decrypted text: juicy
```

Цифровий підпис

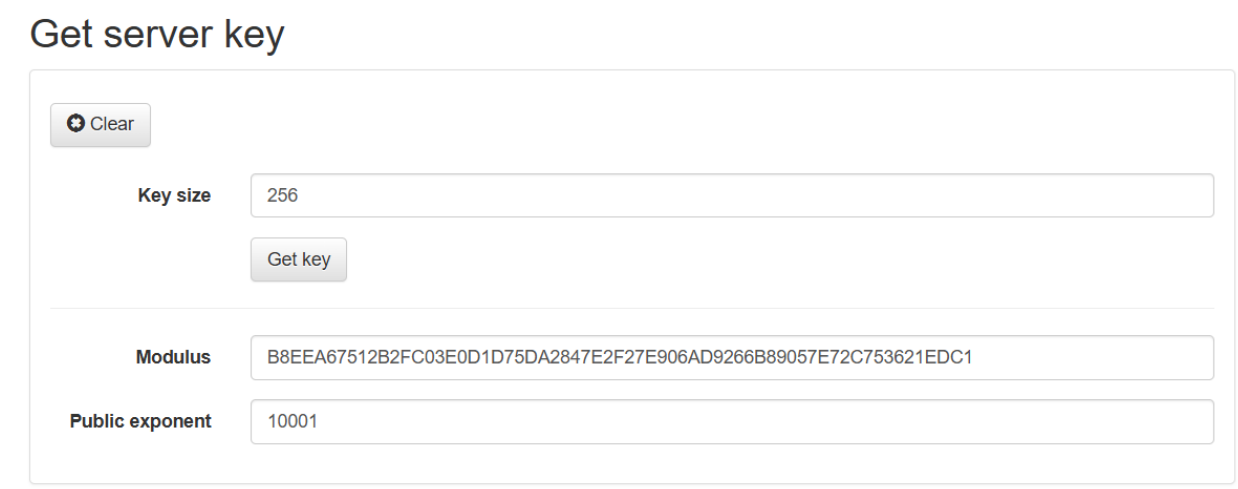
```
+------------------Цифровий підпис------------------+
Аліса створює підпис
sign (S): 508761232931392638072106942204588983534748162446855267359484477786787684346697293899251

Боб перевіряє підпис ключем Аліси
Check: Verify(S, pub_A) == M
successful
```

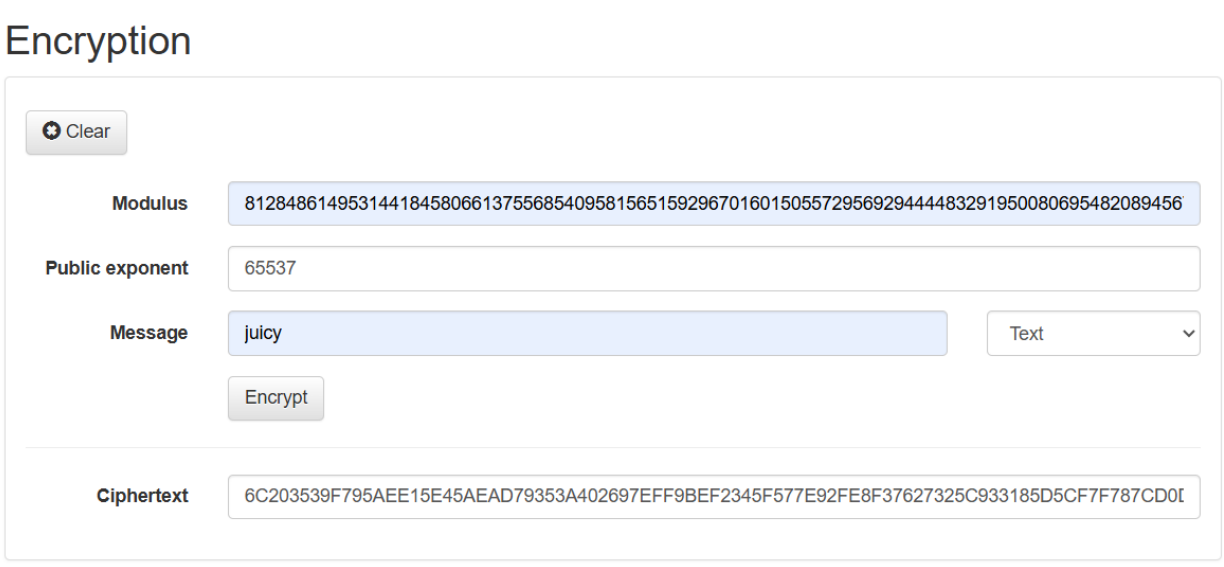
Обмін сесійним ключем

```
+------------------Key Exchange------------------+
[Alice] Генерує сесійний ключ k: 93112050010883188184361044221143758778752950965054502249688244855016889718342072820947715301
1. Аліса надсилає пакет (SendKey)
Дії: 1. S = k^d_A (mod n_A)  -> Підпис
     2. k1 = k^e_B (mod n_B) -> Шифрування ключа
     3. S1 = S^e_B (mod n_B) -> Шифрування підпису
Encrypted key (k1): 68354973310603353229041350218272739898577480756233949313299797162228693862396422496 48
Encrypted sign (S1): 68483039562846197813039122669628787923547137113364684826361132516633986365498678846 9
2. Боб отримує пакет (ReceiveKey)
Дії: 1. k = k1^d_B (mod n_B) -> Розшифровка ключа
     2. S = S1^d_B (mod n_B) -> Розшифровка підпису
     3. Verify(k, S, pub_A)  -> Перевірка підпису
Decrypted k: 93112050010883188184361044221143758778752950965054502249688244855016889718342072820947715301
Конфіденційність: successful
Цілісність: successful
```

GenerateKeyPair()



Encrypt()



Decrypt()

```python
n_srv = int("B8EEA67512B2FC03E0D1D75DA2847E2F27E906AD9266B89057E72C753621EDC1", 16)
e_srv = 65537

msg = "juicy"

msg_bytes = msg.encode("utf-8")
msg_int = int.from_bytes(msg_bytes, byteorder="big")

print("Message integer =", msg_int)

C = pow(msg_int, e_srv, n_srv)

C_hex = hex(C)[2:]
print("Ciphertext for server:", C_hex)
```

```
PS D:\KPI\Крип.Лаби> & C:/Users/vikto/AppData/Local/Microsoft/WindowsApps/python3.13.exe d:/KPI/Крип.Лаби/s_1.py
Message integer = 457236374393
Ciphertext for server: 147bdc7837cf6d4b2cfdac9c6b174b03de48038060703d144a24969a74dbc1bd
```

Decryption

Clear

Ciphertext 147bdc7837cf6d4b2cfdac9c6b174b03de48038060703d144a24969a74dbc1bd Text

Decrypt

Message juicy

Decryption

Clear

Ciphertext 147bdc7837cf6d4b2cfdac9c6b174b03de48038060703d144a24969a74dbc1bd Bytes

Decrypt

Message 6A75696379

Sign()

Sign

Clear

Message juicy Text

Sign

Signature 6EF35F7C34CE7D578BB12FF812FFF741DEB9896030401578B15E77CBD35EBCA6

Verify()

Verify

Clear

Message juicy Text

Signature 6EF35F7C34CE7D578BB12FF812FFF741DEB9896030401578B15E77CBD35EBCA6

Modulus B8EEA67512B2FC03E0D1D75DA2847E2F27E906AD9266B89057E72C753621EDC1

Public exponent 10001

Verify

Verification true

SendKey()

Send key

Clear

Modulus B8EEA67512B2FC03E0D1D75DA2847E2F27E906AD9266B89057E72C753621EDC1

Public exponent 10001

Send

Key 5B453F13E1BA23C0B68D756006A5DA6387348264AB5FF531F9CE0928C97BA7FE

Signature 45F2264DAA8A0FCF

ReceiveKey()

Receive key

Clear

Key 5B453F13E1BA23C0B68D756006A5DA6387348264AB5FF531F9CE0928C97BA7FE

Signature 45F2264DAA8A0FCF

Modulus B8EEA67512B2FC03E0D1D75DA2847E2F27E906AD9266B89057E72C753621EDC1

Public exponent 10001

Receive

Key 45F2264DAA8A0FCF

Verification true ✔