КРИПТОГРАФІЯ КОМП'ЮТЕРНИЙ ПРАКТИКУМ №4

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

Виконали: Медвецький Давид та Левашова Світлана

Група: ФБ-13

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:

Абонент А:

 $\begin{array}{lll} \textbf{p_A} &=& 67434069773723700423316764014229821814315609807542663121007590065672672455501 \\ \textbf{q_A} &=& 69300489368712328126289055783103480381950136620345764968554336794560106630243 \\ \textbf{A60HEHT} & \textbf{B:} \end{array}$

p_B = 83096649198860189408834193720986319302458639378116757478126020169608016661751 q_B = 107937475688991463934544371865817480325178374657786580984341088557059596106573

- наші випадкові прості числа.

Все кандидаты:

- всі кандидати (виводили суто для протоколу)

```
Ключи

Открытый ключ A (n, e): (46732140354429446515256425592749238449143103041090126549898186372144735547694396676223004

Секретный ключ A (n, d): (46732140354429446515256425592749238449143103041090126549898186372144735547694396676223004

Открытый ключ B (n, e): (89692425527386237023892712268568751321411195721400509300220856196756115307056602211929168

Секретный ключ B (n, d): (89692425527386237023892712268568751321411195721400509300220856196756115307056602211929168
```

- параметри криптосистеми RSA для абонентів A та B (так як числа занадто великі, на скріні не видно відкриті та секретні ключі повністю).

Абонент А:

Сообщение: 36145440483680697188271279333578939792379624557734109568456938326412176240950

Зашифрованное сообщение: 467827787360616382308175221901763727194312057659286483864462854972159504079054097
Подпись: 1745131766268541978982081517189550008971223380252667611066078327502375800418604360029566843566019

Абонент В

Разшифрованное сообщение: 36145440483680697188271279333578939792379624557734109568456938326412176240950 Проверка цифровой подписи: True

- згенероване відкрите повідомлення, зашифроване повідомлення, цифровий підпис та перевірка цифрового підпису.

Як в цілому працює код:

Спочатку для абонентів А і В генеруються два простих числа р і q.

Наступним кроком для абонентів А і В генеруються відкриті та секретні ключі з використанням простих чисел, що були згенеровані у попередньому кроці (р, q).

Далі генерується випадкове повідомлення для абонента А. Це повідомлення шифрується відкритим ключем абонента В. Отримане зашифроване повідомлення розшифровується секретним ключем абонента В.

Перевірка підпису:

Береться випадкове повідомлення для абонента А, що підписується секретним ключем абонента А. І підпис перевіряється відкритим ключем абонента А.

Перевірка операцій на тестовому середовищі:

89492425527386237823892712268568751321411195721480509380228856196756115307056680221192916878343502615602928812045615824291083583416124912579915872288789323

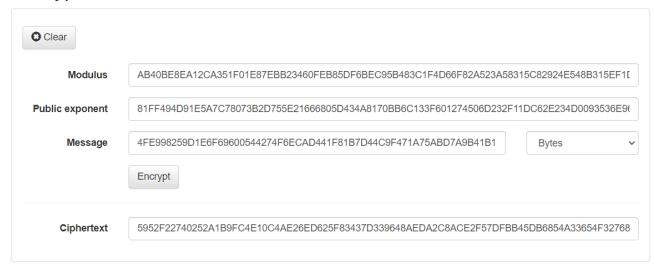
- наш модуль з публічного ключа В.

- публічна експонента.

36145440483680697188271279333578939792379624557734109568456938326412176240950

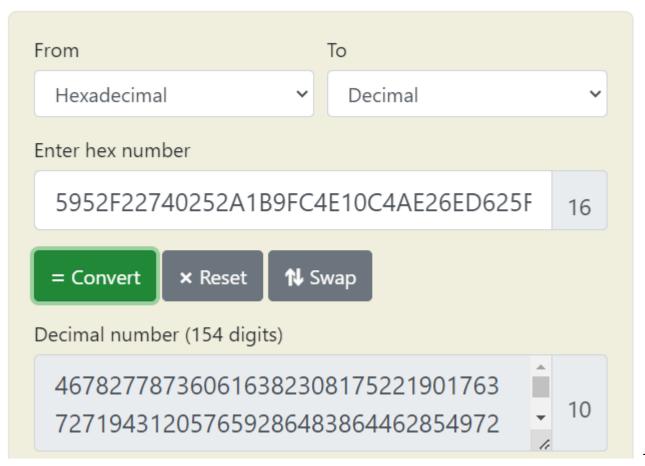
- згенероване повідомлення.

Encryption



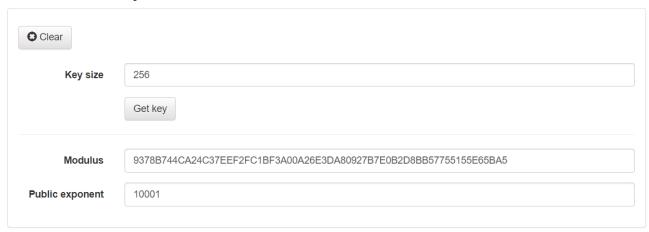
- перевели в шістнадцяткову систему числення та отримали шифртекст.

Hexadecimal to Decimal converter



перевели в десяткову систему числення та отримали правильне розшифрування.

Get server key



- згенерували модуль та експоненту.

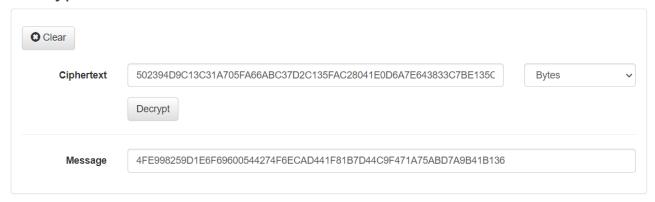
```
# <u>Шифруем</u> и <u>расшифровываем сообщение для абонента</u> A
message_A = 36145440483680697188271279333578939792379624557734109568456938326412176240950
encrypted_message_A = encrypt(message_A, n: 66703275263659607857607982718184123795922479827902579188919434789179921685413, e: <u>65537</u>)
decrypted_message_A = decrypt(encrypted_message_A, private_key_B)
```

- шифруємо нашою програмою.

Сообщение: 36145440483680697188271279333578939792379624557734109568456938326412176240950

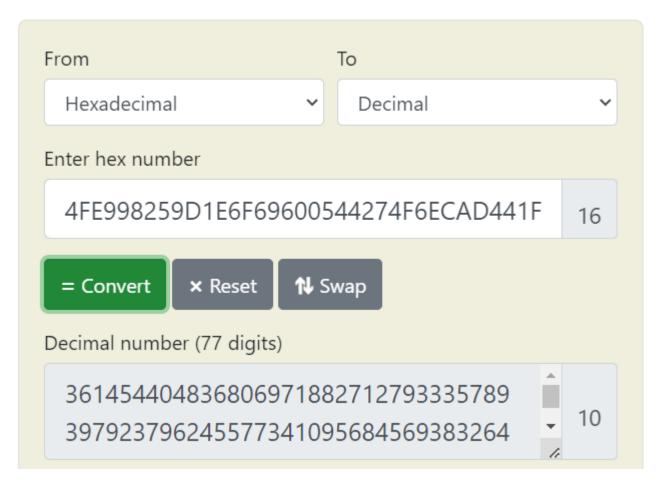
- отримуємо повідомлення.

Decryption



- переводимо наше повідомлення в hex та дешифуємо.

Hexadecimal to Decimal converter



- бачимо, що все співпадає.

- за допомогою згенерованих на сервері ключа та підпису проводимо перевірку та бачимо, що вона пройшла успішно.

Verify



- взяли наше повідомлення, згенерований нами підпис, наше значення публічного ключа для абонента А і бачимо, що верифікація пройшла успішно.

Висновки:

Робота дозволила освоїти криптосистему RSA та алгоритм електронного підпису. Досліджено методи генерації ключів, перевірку чисел на простоту та протокол розсилання ключів. Практично використано систему RSA для засекреченого зв'язку та електронного підпису, розвиваючи навички в області криптографії.