

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
“КІЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №4

Вивчення крипtosистеми RSA та алгоритму електронного підпису; ознайомлення з методами генерації параметрів для асиметричних крипtosистем

Виконали:

ФБ-32 Рибчук Нікіта

ФБ-32 Луценко Євгеній

Мета роботи: Ознайомлення з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної крипtosистеми типу RSA; практичне ознайомлення з системою захисту інформації на основі крипtosхеми RSA, організація з використанням цієї системи засекреченого зв'язку й електронного підпису, вивчення протоколу розсилання ключів.

Порядок виконання роботи

1. Написати функцію пошуку випадкового простого числа з заданого інтервалу або заданої довжини, використовуючи датчик випадкових чисел та тести перевірки на простоту. В якості датчика випадкових чисел використовуйте вбудований генератор псевдовипадкових чисел вашої мови програмування. В якості тесту перевірки на простоту рекомендовано використовувати тест Міллера-Рабіна із попередніми пробними діленнями. Тести необхідно реалізовувати власноруч, використання готових реалізацій тестів не дозволяється.
2. За допомогою цієї функції згенерувати дві пари простих чисел $p, q \in \{1, p\}$, q довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб $pq \leq p_1q_1$; $p \neq q$ – прості числа для побудови ключів абонента А, $p \neq q_1$ – абонента В.
3. Написати функцію генерації ключових пар для RSA. Після генерування функція повинна повернати та/або зберігати секретний ключ (d, p, q) та відкритий ключ (n, e) . За допомогою цієї функції побудувати схеми RSA для абонентів А і В – тобто, створити та зберегти для подальшого використання відкриті ключі (e, n) , (d, n) та секретні d_1 і d_2 .
4. Написати програму шифрування, розшифрування і створення повідомлення з цифровим підписом для абонентів А і В. Кожна з операцій (шифрування, розшифрування, створення цифрового підпису, перевірка цифрового підпису) повинна бути реалізована окремою процедурою, на вхід до якої повинні подаватись лише ті ключові дані, які необхідні для її виконання. За допомогою датчика випадкових чисел вибрати відкрите повідомлення M і знайти криптограму для абонентів А и В, перевірити правильність розшифрування. Скласти для А і В повідомлення з цифровим підписом і перевірити його.
5. За допомогою раніше написаних на попередніх етапах програм організувати роботу протоколу конфіденційного розсилання ключів з підтвердженням справжності по відкритому каналу за допомогою алгоритму RSA. Протоколи роботи кожного учасника (відправника та приймаючого) повинні бути реалізовані у вигляді окремих процедур, на вхід до яких повинні подаватись лише ті ключові дані, які необхідні для виконання. Перевірити роботу програм для випадково обраного ключа $0 < k < n$. Кожна з наведених операцій повинна бути реалізована у вигляді окремої процедури, інтерфейс якої повинен приймати лише ті дані, які необхідні для її роботи; наприклад, функція Encrypt(), яка

шифрує повідомлення для абонента, повинна приймати на вхід повідомлення та відкритий ключ адресата (і тільки його), повертаючи в якості результату шифротекст. Відповідно, програмний код повинен містити сім високорівневих процедур: GenerateKeyPair(), Encrypt(), Decrypt(), Sign(), Verify(), SendKey(), ReceiveKey().

Хід роботи

Генерація ключів для А і В:

```
>>> 1. Генерація ключів...
[Абонент А]
Public Key (e) (Dec): 65537
Public Key (e) (Hex): 10001
-----
Modulus (n) (Dec): 779720952101839452750960222691716935783889547104698495970780907151493221578392285224416476739982876488449997841836463216425803358694741345522987932893961
Modulus (n) (Hex): 940FF75875605AF7C04F9C4E7878058D36A8917900A72BCE35CD8E565632FABADF0AE048C55EAF301D7D936E1CBD827D2539451FAADCFF221F115FD5ACC309
-----
Private Key (d) (Dec): 569053407067652120559049505643298000191394817962398868459469384910899065853008049270507842966090774190021283540662923703496076934443363161440370388598189
Private Key (d) (Hex): ADD79A10C24F71EA3C36BA5F276D0F8E167560E90B495A6DC185F6DFFA682D3E9887A7C03400748BE390F57E291E384E3C7C819E1E11CC65C690460391770AD
-----
[Абонент В]
Public Key (e1) (Dec): 65537
Public Key (e1) (Hex): 10001
-----
Modulus (n1) (Dec): 8695013373964033401099152168039626288725997791178302889281123346052655347086332387443047430458457921714083058475079297557664410303547450730630646918083997
Modulus (n1) (Hex): A604570E2508001D6AEC40D22211C2EC0040AC73B36E9566761490BC465A5CCC9270A2AF1CAB991477E192CEF58A5440DCBC2760957EB3B247D07FD838F59D
-----
Private Key (d1) (Dec): 95922832436272581122033157199612123669208178632252199681862950382166864762550672054146349392870059976829304741227785223470515282109163092508989767121153
Private Key (d1) (Hex): 1D4DC6D00859088B5894D482A28586FAFDDBA94D998C1173DEEB9D2926918A90FDEEB138C5850E2EABC128BA85A1F7228BAED2052E84F5E6E133B492657901
```

Шифрування та дешифрування повідомлення:

```
>>> 2. Шифрування тексту (A -> B)
Вхідний текст: Hello IPT
Текст як число (Dec): 1335473908826942034004
Текст як число (Hex): 48656C6C6F20495054
-----
Зшифроване повідомлення (Ciphertext) (Dec): 4220158576372890102559659854729526857791254201761302755022312004591116296072405697544667666392761296813003886979446041118955043179824973170143532566439
Зшифроване повідомлення (Ciphertext) (Hex): 5093B49728E24E14E183315E499BC774E62B8E6A2165F8EB09235613CAC026872C73E85743D289CEDA764522C74C03003E90E9F7F9A74741FF24931E0647A7
-----
Розшифроване число (Dec): 1335473908826942034004
Розшифроване число (Hex): 48656C6C6F20495054
-----
Результат: "Hello IPT"
```

Цифровий підпис та його перевірка:

```
>>> 3. Цифровий підпис повідомлення
Цифровий підпис S (Dec): 11010464684788662488854686449659446075337047864378686696815812402947745912596468198917714461202072846539043615556486576901900417944827992927447558401155
Цифровий підпис S (Hex): 1505CD9372CB4C374866C485423B8FFF6D0D011F843884F1DC088077BDC202A1A3770955AA4A6355D8E918759078253655F0E4C79D918E0923CC37001CB42C83
-----
Перевірка підпису: УСПІХ
```

Протокол обміну сесовим ключем k:

```
>>> 4. Протокол обміну сесовим ключем k
Згенерований ключ k (Dec): 201082509578672194218977850544758725332997983347071354368451222773832904626893054234062405594228880187773308704829052265908067239137188011214551485268695
Згенерований ключ k (Hex): 2664855510290198F89730FF4305EB3D58AF4FB4E989827EA25D8800496284133889904EB1802C4385626A553D8B096BAE37576ACA735659BF82555A84207
-----
A відривав пакет (k1, S1)
k1 (Encrypted k) (Dec): 60245764559275803602220820850860178874787909412859930856511595804858211105424150328722265719076869414963201667029652336152079374205573770174131040852893
k1 (Encrypted k) (Hex): 7307842C7CF3939CDF3463EAEB416AFF20B84268CF78158A390237FBB68F400784F9CA6E76E6D0D958FCFC712AACD895B7F75613EFC85C0984666D6989D
-----
S1 (Encrypted Signature) (Dec): 7050824477288549878276741469970112925355895594676443451236018906640154359483985221627503473278955967487752113491202087319970303458265973778901201014630833
S1 (Encrypted Signature) (Hex): 86C2E7AE9E6E5FBFA5A9124E79B30C03AF05F3028D76556ECD6E481CF3CE84499E379E90C47155171A270234AD3A2D880266C48C95E9BC34A4D10DFC64E2981
-----
В отримав та обробив пакет
Отримане k (Dec): 20108250957867219421897785054475872533299798334707135436845122277383290462405594228880187773308704829052265908067239137188011214551485268695
Отримане k (Hex): 2664855510290198F89730FF4305EB3D58AF4FB4E989827EA25D8800496284133889904EB1802C4385626A553D8B096BAE37576ACA735659BF82555A84207
-----
Автентичність відправника (A): ПІДТВЕРДЖЕНО
```

Перевірка на сайті

Генерація ключа:
RSA Testing Environment

Server Key

Get server key

Key size: 256

Modulus: C212EBB1BFFA7487D068F59EA6AE15B82D8058598FF4B99375495AB16F65AA6B

Public exponent: 10001

Сигнатуря з сайту:
RSA Testing Environment

Server Key

Sign

Message: Hello IPT

Type: Text

Signature: 68B253CF9A1AF839211F3318F39CF59006C631451B93E3C4E01A647E01B49A78

Шифротекст згенерований нашим ключем із коду:

RSA Testing Environment

Server Key

Encryption

Modulus: 69DBB96494277D97714069C82222FB5E3A7F8D6AC43AD33BA983F9F5E587925F80D19DC86766DC26188BE

Public exponent: 10001

Message: Hello IPT

Type: Text

Ciphertext: 19373CD60F5D854F3FF284165473CE00AE26B84E69341688C45EDFF075825DB6812AF84C33967E352F5B1E

Верифікація на сайті для ключа згенерованого кодом:

RSA Testing Environment

Server Key
Encryption
Decryption
Signature
Verification
Send Key
Receive Key

Verify

Clear

Message

Text

Signature

Modulus

Public exponent

Verify

Verification



Шифрування на сайті ключем із сайту:

RSA Testing Environment

Server Key
Encryption
Decryption
Signature
Verification
Send Key
Receive Key

Encryption

Clear

Modulus

Public exponent

Message

Text

Encrypt

Ciphertext

Перевірка шифрування кодом для ключа із сайту:

>>> Тест 1: Шифрування 'Hello IPT' (для Сайту)
860E6A65BDCDF89BF7BCC718B1466E31F74A37EA9EB39B378D63DDD139A63B5C

Перевірка підпису для ключа із сайту:

>>> Тест 2: Перевірка підпису сайту
Результат: УСПІХ

Перевірка дешифрування шифротексту отримано із сайту ключем із коду:

```
>>> Тест 3: Дешифрування шифротексту з сайту
Результат:
HEX: 48656C6C6F20495054
TEXT: 'Hello IPT'
```

Генерація підпису і перевірка його на сайті для нашого ключа із коду:

```
>>> Тест 4: Генерація вашого підпису
34BC3640C024EC319AE5060727E104FAE3A9EBABE1855E84D926BF046952001A06B5AA161EAFCF8AA016C5496590E13480EBF775929246E8AD0F408E068BA3C8
```

RSA Testing Environment

Server Key
Encryption
Decryption
Signature
Verification
Send Key
Receive Key

Verify

Message: Hello IPT
Signature: 34BC3640C024EC319AE5060727E104FAE3A9EBABE1855E84D926BF046952001A06B5AA161EAFCF8AA016C5496590E13480EBF775929246E8AD0F408E068BA3C8
Modulus: 69DBB96494277D97714069C82222FB5E3A7F8D6AC43AD33BA983F9F5E587925F80D19DC86766DC26188BE
Public exponent: 10001
Verify

Verification: true

Висновки

У ході виконання комп’ютерного практикуму було досліджено, а також програмно реалізовано асиметричну криптосистему RSA, включаючи алгоритм генерації великих простих чисел на основі ймовірнісного тесту Міллера-Рабіна. Було розроблено функції шифрування, дешифрування та цифрового підпису, а також реалізовано протокол конфіденційного обміну сесійними ключами.

Практична робота дозволила глибше зрозуміти математичні основи та принципи роботи RSA, які забезпечують високий рівень безпеки.