Хмельницький національний університет
Факультет програмування та комп'ютерних і телекомунікаційних систем
Кафедра комп'ютерних наук та інформаційних технологій

ДИПЛОМНА РОБОТА

МАГІСТРА

на тему *Інформаційна технологія ідентифікації користувачів*

Галузь знань *12 – Інформаційні технології*
Шифр і назва галузі знань

Спеціальність *122 – Комп'ютерні науки*
Шифр і назва спеціальності

Виконав: студент 2 курсу, група *КНм-19-1* Підпис *В.В. Карпанасюк*
Ініціали, прізвище

Керівник: *к.т.н., доцент кафедри КНІТ* Підпис *О.А. Насічник*
Ініціали, прізвище

Нормоконтроль: *к.т.н., доцент кафедри КНІТ* Підпис *Р.О. Багрій*
Ініціали, прізвище

До захисту допускаю:
Зав. кафедри КНІТ, д.т.н., професор Підпис *О.В. Бармак*
Ініціали, прізвище

7 *12* 2020 р.

Хмельницький 2020

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет *програмування та комп'ютерних і телекомунікаційних систем*

Кафедра *комп'ютерних наук та інформаційних технологій*

Освітній ступінь *магістр*

Галузь знань *12 – Інформаційні технології*

Спеціальність *122 – Комп'ютерні науки*

ЗАТВЕРДЖУЮ
Завідувач кафедри *комп'ютерних наук та інформаційних технологій*

(підпис)
д.т.н., професор О.В. Бармак
«7» 9 *2020* року

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ МАГІСТРА

1. Тема дипломної роботи магістра: *«Інформаційна технологія ідентифікації користувачів»*
2. Завдання видано студенту *Карпанасюк Віктору Володимировичу*
(прізвище, ім'я, по батькові)
3. Керівник роботи *к.т.н., доцент Олександр Анатолійович Пасічник*
(прізвище, ім'я, по батькові)
4. Затверджені наказом університету від «9» 9 *2020* р. № 22
5. Зміст пояснювальної записки (перелік задач) та вхідні дани:
Мета роботи полягає у реалізації інформаційної технології ідентифікації користувачів на основі концепції «нульових знань» з достатнім рівнем обчислювальної здатності, дослідженні предметної області, огляді існуючих рішень щодо існуючих методів ідентифікації, що реалізують концепцію «нульових знань».

Реферат

Дипломна робота магістра присвячена розробці інформаційної технології віддаленої ідентифікації користувачів з використанням криптографічної концепції “нульових знань” з покращеною обчислювальною здатністю.

Актуальність теми. Загальносвітовим трендом технічного та технологічного прогресу людства в останні десятиліття є активна інтеграція інформаційних систем. Утворений внаслідок цього процесу інформаційний простір надає можливість використовувати великі обсяги інформації задля вирішення широкого кола питань, завдань та проблем й задоволення найрізноманітніших потреб. Отримуваний результат визначається широким спектром різнопланових чинників, у тому числі і суб’єктивних. Суб’єктивізм у цих питаннях пов'язаний з двома головними аспектами. По-перше, це належні виконавці, а по-друге, відповідні вигідоотримувачі. Обидва ці аспекти об’єднує питання розподілу прав доступу, яке, у свою чергу, об’єктивно та обов’язково включає задачу ідентифікації віддалених користувачів.

Особливої актуальності питання ідентифікації користувачів набуло останнього часу коли інформатизація та цифровізація охопили практично усі сфери життєдіяльності людини, а мережеві технології стають повсякденним інструментарієм практичного кожного пересічного громадянина.

Наявні значні за обсягом інформаційні ресурси стають доступними широкому колу користувачів створюючи, одночасно, нові можливості для протиправних дій, у тому числі, шляхом зламу існуючих механізмів захисту та контролю доступу. Потенціал мережевих технологій опосередковано впливає на зниження криптографічної стійкості існуючих методів та порушує баланс сил у світі інформаційної безпеки. Це вимагає пошуку адекватних рішень щодо вдосконалення існуючих криптографічних методів, в тому числі і методів ідентифікації користувачів.

Історична ретроспектива свідчить про постійний розвиток засобів захисту та несанкціонованого доступу. Перманентний характер цих процесів потребує генерації

все нових схем контролю доступу, оскільки, технології зламу об’єктивно відстають технічно, алгоритмічно та методологічно. Стратегічним напрямком дій у цій сфері є запровадження алгоритмів, що мають підвищену криптографічну складність та потребують суттєвих часових витрат.

Таким чином, проблема підвищення ефективності і захищеності схем ідентифікації залишається актуальною й на сучасному етапі розвитку комп’ютерних інформаційних технологій. Базовим підходом може бути запровадження нових, раніше невикористовуваних, алгоритмів з ускладненим шифруванням та потребують потенційно більший час задля їх зламу.

Мета і задачі роботи. Мета роботи полягає у реалізація інформаційної технології ідентифікації користувачів на основі концепції «нульових знань» з достатнім рівнем обчислювальної здатності.

Для досягнення поставленої мети визначені наступні задачі дослідження:

- провести аналіз існуючих методів, технологій та рішень методів ідентифікації користувачів, що реалізують концепцію «нульових знань»;

- удосконалення існуючих методів ідентифікації у напрямку покращення обчислювальної здатності;

- розробити інформаційну технологію ідентифікації користувачів за допомогою отриманих моделей та методів;

- виконати експериментальну перевірку інформаційної технології ідентифікації користувачів.

Об’єкт дослідження – процес ідентифікації користувачів з використанням інформаційних технологій.

Предмет дослідження – моделі, методи, підходи та засоби інформаційної технології ідентифікації користувачів.

Методи дослідження. Для розв’язання поставлених задач використовуються основні положення методів аналізу даних, криптографії, ідентифікації; для удосконалення методів ідентифікації методи експоненціонування з використанням поліноміальної та модулярної арифметики; для реалізації інформаційної технології –

методології проектування інформаційних систем та об’єктно-орієнтований підхід.

Наукова новизна одержаних результатів. В результаті проведеної роботи були отримані такі результати:

- удосконалено існуючі методи ідентифікації у напрямку покращення обчислювальної здатності;

- встановлено межі використання поліноміальної арифметики у порівнянні з модулярною в залежності від значення експоненти в частині покращення обчислювальної складності при ідентифікації користувачів.

Практичне значення одержаних результатів. У результаті виконання дипломної роботи магістра за інформаційною технологією розроблено відповідне експериментальне програмне забезпечення, яке підтвердило вірність запропонованих положень. Застосування інформаційної технології дає можливість ідентифікації віддалених користувачів із використанням концепції «нульових знань», яка унеможливлює розголошення персональних даних, а експоненціонування при використанні модулярної арифметики суттєво покращує обчислювальну складність.

Апробація результатів дипломної роботи. Основні наукові та практичні результати доповідалися на конференціях:

- доповідь на тему «Інформаційна технологія ідентифікації користувачів» на XI Міжнародній науково-практичній конференції «Eurasian scientific congress», 1-3 листопада 2020 р., Барселона, Іспанія

За темою дипломної роботи магістра автором виконано одну наукову публікацію [33].

Структура та обсяг роботи. Дипломна робота магістра складається з завдання, реферату, змісту, переліку скорочень, вступу, 4 розділів, висновків, переліку посилань із 33 найменувань та 2 додатків. Загальний обсяг дипломної роботи магістра становить 92 сторінок, з них 62 сторінка основного тексту та 3о сторінок додатків. У роботі наведено 13 рисунків.

Ключові слова: інформаційна технологія, ідентифікація користувачів, обчислювальна здатність, експоненціонування.

Зміст

Перелік скорочень

Скорочення, термін, позначення	Пояснення
ОС	Операційна система
ПЗ	Програмне забезпечення
Користувач	Одна з сторін-учасників протоколу ідентифікації, метою якої є доведення іншій стороні, а саме, Системі, знання деякої унікальної ідентифікаційної інформації для отримання доступу до інформаційних ресурсів Системи
Система	Сторона-учасник протоколу ідентифікації, що перевіряє наявність у Користувача секретної ідентифікаційної інформації і надає доступ до своїх інформаційних ресурсів лише тоді, коли
Зловмисник	Сторона, що має на меті отримання доступу до ресурсів Системи і при цьому не володіє ніякою секретною ідентифікаційною інформацією, має доступ до каналу передачі даних між Системою і Користувачем.
ZKP	Доказ з нульовим розголошенням (з англ. «Zero-Knowledge Proof»). Криптографічна концепція, згідно з якою, доводяча сторона доводить знання певної інформації перевіряючій стороні, не розкриваючи її.

Вступ

Актуальність теми. Загальносвітовим трендом технічного та технологічного прогресу людства в останні десятиліття є активна інтеграція інформаційних систем. Утворений внаслідок цього процесу інформаційний простір надає можливість використовувати великі обсяги інформації задля вирішення широкого кола питань, завдань та проблем й задоволення найрізноманітніших потреб. Отримуваний результат визначається широким спектром різнопланових чинників, у тому числі і суб'єктивних. Суб'єктивізм у цих питаннях пов'язаний з двома головними аспектами. По-перше, це належні виконавці, а по-друге, відповідні вигідоотримувачі. Обидва ці аспекти об'єднує питання розподілу прав доступу, яке, у свою чергу, об'єктивно та обов'язково включає задачу ідентифікації віддалених користувачів.

Особливої актуальності питання ідентифікації користувачів набуло останнього часу коли інформатизація та цифровізація охопили практично усі сфери життєдіяльності людини, а мережеві технології стають повсякденним інструментарієм практичного кожного пересічного громадянина.

Наявні значні за обсягом інформаційні ресурси стають доступними широкому колу користувачів створюючи, одночасно, нові можливості для протиправних дій, у тому числі, шляхом зламу існуючих механізмів захисту та контролю доступу. Потенціал мережевих технологій опосередковано впливає на зниження криптографічної стійкості існуючих методів та порушує баланс сил у світі інформаційної безпеки. Це вимагає пошуку адекватних рішень щодо вдосконалення існуючих криптографічних методів, в тому числі і методів ідентифікації користувачів.

Історична ретроспектива свідчить про постійний розвиток засобів захисту та несанкціонованого доступу. Перманентний характер цих процесів потребує генерації все нових схем контролю доступу, оскільки, технології зламу об'єктивно відстають технічно, алгоритмічно та методологічно. Стратегічним напрямком дій у цій сфері є запровадження алгоритмів, що мають підвищену криптографічну складність та

потребують суттєвих часових витрат.

Таким чином, проблема підвищення ефективності і захищеності схем ідентифікації залишається актуальною й на сучасному етапі розвитку комп'ютерних інформаційних технологій. Базовим підходом може бути запровадження нових, раніше невикористовуваних, алгоритмів з ускладненим шифруванням та потребують потенційно більший час задля їх зламу.

Мета і задачі роботи. Мета роботи полягає у реалізація інформаційної технології ідентифікації користувачів на основі концепції «нульових знань» з достатнім рівнем обчислювальної здатності.

Для досягнення поставленої мети визначені наступні задачі дослідження:

- провести аналіз існуючих методів, технологій та рішень методів ідентифікації користувачів, що реалізують концепцію «нульових знань»;

- удосконалення існуючих методів ідентифікації у напрямку покращення обчислювальної здатності;

- розробити інформаційну технологію ідентифікації користувачів за допомогою отриманих моделей та методів;

- виконати експериментальну перевірку інформаційної технології ідентифікації користувачів.

Об'єкт дослідження – процес ідентифікації користувачів з використанням інформаційних технологій.

Предмет дослідження – моделі, методи, підходи та засоби інформаційної технології ідентифікації користувачів.

Методи дослідження. Для розв'язання поставлених задач використовуються основні положення методів аналізу даних, криптографії, ідентифікації; для удосконалення методів ідентифікації методи експоненціонування з використанням поліноміальної та модулярної арифметики; для реалізації інформаційної технології – методології.

Наукова новизна одержаних результатів. В результаті проведеної роботи були отримані такі результати:

- удосконалено існуючі методи ідентифікації у напрямку покращення обчислювальної здатності;

- встановлено межі використання поліноміальної арифметики у порівнянні з модулярною в залежності від значення експоненти в частині покращення обчислювальної складності при ідентифікації користувачів.

Практичне значення одержаних результатів. У результаті виконання дипломної роботи магістра за інформаційною технологією розроблено відповідне експериментальне програмне забезпечення, яке підтвердило вірність запропонованих положень. Застосування інформаційної технології дає можливість ідентифікації віддалених користувачів із використанням концепції «нульових знань», яка унеможливлює розголошення персональних даних, а експоненціонування при використанні модулярної арифметики суттєво покращує обчислювальну складність.

Апробація результатів дипломної роботи. Основні наукові та практичні результати доповідалися та обговорювалися на міжнародній науково-практичній конференції [33] - XI Міжнародній нщуково-практичній конференції «Eurasian scientific congress», 1-3 листопада 2020 р., Барселона, Іспанія.

Структура та обсяг роботи. Дипломна робота магістра складається з завдання, реферату, змісту, переліку скорочень, вступу, 4 розділів, висновків, переліку посилань із 33 найменувань та 2 додатків. Загальний обсяг дипломної роботи магістра становить 96 сторінок, з них 60 сторінка основного тексту та 36 сторінок додатків. У роботі наведено 13 рисунків.

Розділ 1
Аналіз сучасного стану технологій ідентифікації користувачів

Створення єдиної, централізованої системи безпеки є необхідною умовою існування сучасної інформаційної інфраструктури [1, 2, 3], а управління доступом – ефективним методом захисту інформації, регулюючим використання ресурсів інформаційної системи, для якої розроблялася концепція інформаційної безпеки [1, 4].

Основою будь-яких систем захисту інформаційних систем є ідентифікація, оскільки всі механізми захисту інформації розраховані на роботу з пойменованими суб'єктами і об'єктами систем. Суб'єктами систем можуть виступати як користувачі, так і процеси, а як об'єкти систем - інформація та інші інформаційні ресурси системи.

Присвоєння суб'єктам і об'єктам доступу особистого ідентифікатора і порівняння його з заданим переліком називається ідентифікацією. Ідентифікація забезпечує виконання таких функцій:

- встановлення автентичності та визначення повноважень суб'єкта при його допуску в систему;
- контролювання встановлених повноважень в процесі сеансу роботи;
- реєстрація дій тощо.

Авторизація полягає у керуванні рівнями та засобами доступу до певного захищеного фізичного або інформаційного ресурсу в залежності від ідентифікатора та пароля користувача або надання певних прав на виконання деяких дій у системі обробки даних. З позицій інформаційної безпеки авторизація є невід’ємною частиною процедури надання доступу для роботи у відповідній інформаційній системі, після ідентифікації та автентифікації.

На сьогоднішній десь існує велика кількість різноманітних технологій для ідентифікації користувачів, які умовно можна розділити на дві групи.

До першої групи відносяться технології, що передбачають використання певної наперед визначеної інформації для ідентифікації користувача системою. Це,

насамперед, ідентифікація за допомогою секретної інформації (пароля), технології з використанням спеціальних технологічних пристроїв (електронних карток), технології з використанням біометричних даних особи або з використанням радіочастот.

До другої групи відносять технології, що передбачаються імплементацію концепції «нульових знань». Згідно з цією концепцією, для кожного нового сеансу ідентифікації використовуються різні паролі, а секретна ідентифікаційна інформація зберігається лише у однієї зі сторін протоколу, найчастіше у користувача. Сутність цієї концепції полягає у можливості довести певне твердження, не розголошуючи при цьому сам доказ, навіть частково.

1.1. Технології з використанням наперед визначеної інформації

Технології, які передбачають використання наперед визначеної інформації поділяють групи, що передбачають використання паролів, спеціальних технічних засобів, біометричних показників.

1.1.1 Технології ідентифікації, що передбачають використання паролів

Одними з найпоширеніших технологій ідентифікації користувачів є технології, які ґрунтуються на знанні особою, яка має право на доступ до ресурсів системи, певної секретної інформації, наприклад, пароля. Такі методи ідентифікації є найбільш поширеними, простими, звичними й існували ще у докомп'ютерну епоху хоча й в дещо іншій технологічні реалізації. При введенні користувачем свого пароля система порівнює його з паролем, що зберігаються в базі даних в зашифрованому вигляді. У разі збігу паролів система надає доступ до своїх ресурсів.

Широке запровадження парольної ідентифікації в сучасних інформаційних системах обумовлює відповідний інтерес до ней науковців та дослідників [5, 6, 7].

Парольні методи класифікують за ступенем частоти зміни пароля:

- методи, які використовують постійні (багаторазові) паролі;

- методи, які використовують одноразові (динамічні) паролі.

Більш поширеним є використання багаторазових паролів. В цьому випадку пароль користувача не змінюється від сеансу до сеансу протягом встановленого адміністратором системи часу його дійсності. Це спрощує процедури адміністрування, але підвищує загрозу розсекречення пароля одним із багатьох відомих на тепер способом.

Більш надійний спосіб полягає у використанні одноразових або динамічно змінюваних паролів.

Існують такі методи парольного захисту, що ґрунтуються на використанні одноразових паролів - методи модифікації схеми простих паролів та методи «запит-відповідь».

До методів модифікації схеми простих паролів відносять випадкову вибірку символів пароля і одноразове використання паролів.

При використанні методу модифікації простих паролів, кожному користувачеві виділяється досить довгий пароль, причому щоразу для ідентифікації використовується не весь пароль, а тільки його деяка частина. Під час перевірки автентичності система запитує у користувача групу символів під заданим порядковим номерам. Кількість символів і їх порядкові номери для запиту визначаються, як правило, за допомогою датчика псевдовипадкових чисел.

При одноразовому використанні паролів кожному користувачеві виділяється список паролів. В процесі запиту номер пароля, який необхідно ввести, вибирається послідовно за списком або по схемі випадкової вибірки.

Значним недоліком методів модифікації схеми простих паролів є необхідність запам'ятовування користувачами довгі паролі або їх списки. Запис же паролів на папір або в записники призводить до появи ризику втрати або розкрадання носіїв інформації з записаними на них паролями.

При використанні методу «запит-відповідь» система задає користувачеві деякі питання загального характеру, правильні відповіді на які відомі тільки конкретному користувачу.

Методи ідентифікації, засновані на одноразових паролях, все ж не забезпечують абсолютного захисту, наприклад, у випадках коли є можливість перехоплення даних.

1.1.2 Технології, що передбачають використання спеціальних технічних засобів

Існую ряд технологій регулювання доступу, які передбачають використання різного роду технічних засобів таких, як зокрема, жетони, електронні картки тощо [1, 8].

Зазначені методи відносяться до категорії комбінованих методів ідентифікації, й потребують, окрім знання пароля, ще й наявності спеціального технічного пристрою, за допомогою якого підтверджується справжність суб'єкта.

Картки поділяють на такі два типи - пасивні (картки з пам'яттю) та активні (інтелектуальні картки). Перевагою використання карток є те, що обробка інформації виконується пристроєм читання, без передачі в пам'ять комп'ютера. Це виключає можливість електронного перехоплення по каналах зв'язку. Недоліки таких карток наступні. Вони є істотно дорожчими за паролі та вимагають спеціальних технічних пристроїв зчитування. Їх використання передбачає спеціальні процедури безпечного обліку і розподілу. Картки обов’язково необхідно оберігати від зловмисників та ні в якому разі не залишати в пристроях зчитування.

Також для ідентифікації користувачів використовуються спеціальні радіотехнічні системи та пристрої, зокрема так звані RFID.

RFID (Radio Frequency Identification) є способом забезпечення зберігання та передачі інформації зі зручного носія-мітки у необхідне місце з використанням відповідних спеціальних технічних пристроїв. Такі мітки-ідентифікатори полегшують ідентифікацію та визначення розташування широкого кола різноманітних об'єктів. Існують пасивні та активні RFID-мітки.

1.1.3 Технології, що використовують біометричні показники

Даний тип технологій ґрунтується на вимірюванні біометричних параметрів людини - фізіологічних або поведінкових. Такі технології характеризуються надзвичайно високим рівнем достовірності ідентифікації. Вони, фактично, унеможливлюють втрату пароля та/або особистого ідентифікатора. Разом із тим, ці методи потребують складного та дороговартісного спеціального обладнання.

Біометричній ідентифікації знаходить широке застосування в системах контролю доступом [1, 9, 10, 11, 12, 13].

Технологічно такі системи виконують ідентифікацію користувача за малюнком райдужної оболонки ока, відбитками пальців та долоні, формою вух, інфрачервоною картиною капілярних судин, тембром голосу, лінгвістичні характеристики та навіть ДНК.

Біометричні технології доцільно використовувати на особливо важливих об'єктах, хоча розвиток техніки та технологій, що супроводжуватиметься їх здешевленням, безумовно сприятиме більш широкому використанню. Так системи такого типу вже використовуються навіть у явно побутових випадках, зокрема, сканери відбитків пальця в ноутбуках.

Новим напрямком є використання біометричних характеристик в поєднані з електронними картками, жетонами та елементами стільникового зв'язку.

1.2 Технології, що реалізують концепцію «нульових знань»

Доказ з нульовим розголошення не видає ніякої інформації окрім вірності твердження; дозволяє довести твердження, не видаючи інформації про саме твердження [5, 14].

Базовими критеріями ефективності будь-якої системи захисту є рівень захищеності, що досягається при її використанні та об’єм ресурсів, що застосовується для реалізації функцій захисту. Складність проблеми визначається неможливістю

побудови адекватної формальної моделі дій сторони, що намагається реалізувати незаконний доступ до ресурсів системи.

Всі сучасні протоколи ідентифікації абонентів розділяють на два класи: з використанням паролів, що перевіряються системою шляхом порівняння (“слабка” ідентифікація) та на основі теоретичної концепції “нульових знань” (“строга” ідентифікація) [15].

Сутність цієї концепції полягає в тому, що для доведення своєї ідентичності абонент має неявним чином виявити знання певної інформації, якою система не володіє, але може перевірити її наявність у абонента. При цьому в системі не зберігається ніякої секретної інформації, яка дозволяє відновити ідентифікаційні дані абонента, що пояснює походження назви концепції "нульових знань”. При кожному зверненні до системи абонентом генерується нова ідентифікуюча інформація.

Таким чином, концепція “нульових знань” найбільш повною мірою відповідає вимогам забезпечення високого рівня захищеності від спроб несанкціонованого доступу до ресурсів розподілених систем. Концепція “нульових знань” базується на використанні незворотних математичних перетворень. В більшості існуючих схем строгої ідентифікації в якості таких перетворень використовуються аналітично нерозв’язувані задачі теорії чисел, зокрема відома задача дискретного логарифмування [15].

До найбільш відомих схем ідентифікації, що відповідають концепції “нульових знань” відносяться метод Feige Fiat Shamir Identification Scheme та його модифікації Joseph Kizza та Ohta Okamoto, Guillou-Quisquater та Schnorr.

1.2.1 Метод Feige Fiat Shamir Identification Scheme (FFSIS)

Суть методу FFSIS полягає в наступному. Користувач вибирає два простих числа p і q, та обчислює модуль $m=p\times q$. Для генерації відкритого та закритого ключів користувач вибирає число v, що є квадратичним лишком по модулю m. Іншими словами, користувач вибирає таке v, для якого існує таке x що $x^2 \bmod m = v$ і існує v^{-1}

таке, що $v \times v^{-1} \bmod m = 1$. Віднаходиться найменше s для якого має місце $s^2 \bmod m = v^{-1}$. Число v разом з модулем m утворюють відкритий ключ, а число s – закритий ключ [14].

Процедура методу згідно [14] є такою.

При реєстрації користувач посилає системі свій відкритий ключ: число v та модуль m.

В циклі ідентифікації користувач вибирає випадкове число r та обчислює значення $x = r^2 \bmod m$, після чого обчислене значення x відсилає в систему. Система ініціює виконання t циклів акредитації, в кожному з яких виконуються такі дії [14]:

Система посилає користувачу випадковий біт b.

Якщо b=0, то користувач посилає в систему число r, в протилежному випадку, тобто якщо b=1, користувач обчислює з використанням закритого ключа s значення $y = r \times s \bmod m$ і відсилає його системі.

Якщо b=0, то система перевіряє $x = r^2 \bmod m$, а якщо b=1, то система виконує перевірку $x = y^2 \times v \bmod m$, переконуючись, що абонент знає $s =$.

Для сторони, що здійснює спробу незаконного отримання доступу до ресурсів системи під виглядом користувача не відомі компоненти закритого ключа: число v та модуль m користувача. Відповідно сторонній зловмисник, перехоплюючи h циклів ідентифікації отримає дані з h_1 циклів при b=0 та h_2 циклів при b=1, $h=h_1+h_2$. Таким чином, зловмисник має в своєму розпорядженні сукупність пар чисел $<r_i, x_i>$, $\forall i \in \{1,2,\ldots,h_1\}: x_i = r^2 \bmod m <r_j, y_j>$, та $\forall i \in \{1,2,\ldots,h_2\}: y_j = r_j \cdot s \bmod m$. Сукупність пар $<r_i, x_i>$ потенційно може бути використана для підбору модуля m. Сукупність пар $<r_j, y_j>$ може бути використана для підбору закритого ключа s. Обидві вказані задачі в математичному сенсі еквівалентні розкладанню числа на два співмножника і при розрядностях більших за 1024 потребують ресурсів. що виходять за рамки практичної доцільності [14].

Якщо зловмисник знаходиться в самій системі, тобто знає відкритий ключ, тобто число v та модуль m користувача, то зловмисник може вибрати будь-яке g та обчислити $x = g^2 \bmod m$; послати системі x в якості x. Якщо зловмисник отримає від

системи біт запиту b=1, то він відсилає системі генероване ним число g. Система перевіряє той факт, що $x = g^2 \ mod \ m$ [14].

Проте, якщо зловмисник отримає від системи біт запиту b=1, то він має послати у відповідь системі обчислене з використанням закритого ключа s значення $y = g \times s \ mod \ m$. Очевидно, що не знаючи закритого ключа s, зловмисник не зможе обчислити коректне значення s. Підбор зловмисником закритого ключа s в математичному сенсі еквівалентно задачі віднаходження значення v^{-1} по відомому v. В свою чергу, ця задача може бути розв'язана лише за умови, що зловмисник знає складові співмножники p і q, такі, що $m=p \times q$. Проте, система не знає цих співмножників і, відповідно, задача підбору сеансового паролю зловмисником, що знаходиться в системі, практично не може бути реалізована [14].

Як зазначено в роботі [14] найбільш значимими для практики недоліками схеми ідентифікації FFSIS є необхідність в декількох циклах акредитації, що, в свою чергу, потребує відповідності кількості сеансів передачі даних. Час, потрібний для здійснення сеансу передачі даних між користувачем та системою суттєвим чином залежить від поточного трафіку в комп'ютерній мережі і на порядки перевищує час виконання системою обчислень, пов'язаних з ідентифікацією користувача. Проведення декількох коротких сеансів передачі даних при ідентифікації кожного користувача значно впливає на пропускну здатність мережевого інтерфейсу систем колективного доступу. Крім того, наявність прогнозованих декількох сеансів передачі даних з конкретним користувачем відкриває потенціальні можливості для зловмисників ефективно завадити успішному проведенню циклу ідентифікації. Таким чином, необхідність в декількох сеансах передачі даних суттєвим чином сповільнює процес ідентифікації користувача.

Метод FFSIS має потенціал для покращення. Можливі модифікації Метод FFSIS наведені в роботах [17, 18, 19].

1.2.2 FFSIS - модифікація Joseph Kizza

Хоча схема ідентифікації Feige-Fiat-Shamir є найвідомішою, класичною, практичною та широко використовуваною модульної арифметичною схемою, що реалізує концепцію нульових знань, вона страждає від так званої проблеми «пінг-понгу» (*ping-pong problem*). Проблема "пінг-понгу" в рішеннях концепції нульових знань обумовлена багаторазовими, іноді неконтрольованими обмінами «запит-відповідь» між Системою та Користувачем. Оскільки система намагається отримати від користувача якомога більше інформації, щоб завершити процес автентифікації в найкоротший термін та, в той самий час, найпевнішим способом, і, оскільки користувач намагається надати необхідну інформацію для процесу автентифікації, не розкриваючи інформації про свою ідентичність, проблема «пінг-понгу» призводить до високої ресурсомісткості процедури. В багатьох системах, наприклад, в системах реального часу, процедура автентифікації має виконуватися за короткий час, для дотримання часових нормативів. В методі FFSIS не має можливості зробити процес автентифікації коротким [20].

1.2.3 FFSIS - модифікація Ohta Okamoto

Один з недоліків FFSIS полягає в тому, що при виконанні протоколу розмір інформації, що передається та розмір пам’яті не можуть бути одночасно малими. Класичний метод представлений у послідовному та паралельному варіантах. Хоча послідовний варіант повністю реалізує концепцію «нульових знань», кількість раундів акредитації має складати $O(\log_2 n)$, що має наслідком низьку комунікаційну продуктивність. Паралельна версія, з цієї точки зору, є більш ефективною, адже не видає ніякої корисної інформації. Продуктивність протоколу – це завжди компроміс між розміром необхідної пам’яті та розміром інформації, що передається при взаємодії Користувача з Системою. Рівень захищеності складає 2^{-kt}, де k – кількість секретних чисел, що використовуються для обчислення вектору s, а t – кількість

раундів акредитації. Наприклад, для того, щоб досягти рівня безпеки 2^{20}, тобто $t \cdot k = 20$, якщо ми зменшимо кількість раундів до $t = 1$, ми повинні зберігати двадцять $(k = 20)$ секретних цілих чисел. Якщо ми зберігаємо лише одне секретне ціле число, тобто k = 1, ми повинні виконати двадцять (t = 20) раундів акредитації. З цієї причини, ефективні з точки зору чисельної обробки параметри ($t = k = 1$) не можуть використовуватися.

В [21] запропоновано рішення цієї проблеми. В цій схемі вводиться третій параметр L, в додаток до t і k. Рівень захищеності визначається як L^{kt}. Тоді параметри $t = k = 1$ можуть використовуватися при правильно підібраним значенні L. Дана модифікація є повільнішою за класичний метод FFSIS, але потребує значно менших ресурсів пам'яті і може ефективно застосовуватись в системах, що працюють з малопотужними термінальними пристроями або смарт-картками.

1.2.4 Метод Guillou-Quisquater

Крім методу FFSIS та його модифікацій, широкого розповсюдження в системах колективного доступу набув метод Guillou-Quisquater, який також реалізує теоретичну концепцію строгої ідентифікації "нульових знань" [22].

Протокол Guillou-Quisquater - це інтерактивний протокол, який дозволяє довести, що твердження, що доводиться, вірне, і сторона, що його доводить, знає цей доказ, в той же час не надаючи ніякої інформації про сам доказ цього твердження. Даний криптографічний протокол має три властивості – повнота, коректність, нульове розголошення [22, 23].

Згідно протоколу передбачається тільки один цикл обміну повідомленнями між системою та користувачем за один цикл акредитації. При цьому задля досягнення того ж рівня захищеності, що й в FFSIS, зазначений протокол потребує більш ні на три порядки більше обчислень, аніж при використані FFSIS. Також протокол Guillou-Quisquater в порівнянні з FFSIS, має меншу кількість повідомлень обміну задля ідентифікації.

Як недолік зазначеного методу є потреба у декількох сеансах обміну даними з одночасною потребою у виконанні операції модулярного експоненціювання користувачем безпосередньо в процесі ідентифікації, що призводить до значного збільшення часу ідентифікації користувача.

Безпека протоколу базується на складності обчислення квадратного кореня по модулю для достатньо великого числа із заданим модулем n [24].

Якщо припустити, що на початку протоколу зловмисник не знає *B*, то його можливості полягають в наступному. Якщо зловмисник вгадує *d,* він може вибрати будь-яке випадкове число *G* і вивести відповідне число *P* так само, як і система. Це очевидно виграшна стратегія для будь-кого, хто вгадав *d* [15].

При кожному використанні процедури, Зловмисник має 1 шанс з *v,* обманути систему. Система має *v-1* шансів виявити обман. Після виконання процедури, система не дізналася фактично нічого про автентифікаційне число *B*. Протокол не потребує повторення, якщо розрядність експоненти *v* достатня для досягнення цільового рівня захисту системи. Це досить просто вказати: від десяти до шістнадцяти бітів для локальної автентифікації, від двадцяти до тридцяти для віддаленої автентифікації та як мінімум шістдесят для схем підпису, що базуються на неінтерактивних технологіях «нульових знань» [18].

1.2.5 Метод Schnorr

Метод Schnorr [25] також передбачає вибір користувачем двох простих чисел *p* та *q* причому, *q* має бути подільником *p*-1. Вибирається число *a* таке, що $a^q \bmod p = 1$. Вибирається випадкове число *s* менше за *q* : $s < q$, яке являє собою секретний ключ користувача. Далі користувачем обчислюється відкритий ключ у вигляді: $v = a^{-s} \bmod p$, який передається системі під час реєстрації.

Особливістю розглянутого методу ідентифікації, що реалізує концепцію “нульових знань” є використання групи чисел менших за *q* відносно невеликої розрядності, що дозволяє суттєво зменшити обчислювальну складність операцій,

пов’язаних з процесом ідентифікації. З іншого боку відносно невелика розрядність закритого ключа s меншого за q : $s < q$ відкриває можливості для його підбору. Суттєвою вадою методу є те, що цикл ідентифікації віддаленого користувача потребує трьох сеансів обміну даними між користувачем та системою, що помітним чином уповільнює процес ідентифікації [25].

В [26] запропоновано модифікацію описаного вище методу, що є підходящою для використання в смарт-картках. Вона потребує обсягів обчислень, більші у 3.6 рази ніж при використання методу Schnorr. Перевагою цього методу є підвищена захищеність, що базується на одразу двох обчислювально складних задачах: обчислення дискретного логарифму в підгрупі Z^*_p та факторизації великих чисел. Очевидним недоліком даного методу є збільшена, у порівнянні з методом Schnorr, кількість бітів, що мають бути передані під час взаємодій між Системою та Користувачем. Якщо в оригінальному методі це 1404 біти, то в даній модифікації це 1776 бітів. Попри збільшення обсягів необхідних обчислень, метод вирішує одну важливу проблему: на відміну від стандартних методів ідентифікації, в яких Зловмисник теоретично може одночасно видавати себе за Систему перед легітимним Користувачем і видавати себе за Користувача перед справжньою Системою, передаючи запити від неї легітимному Користувачу, а відповіді на них – від легітимного користувача справжній Системі, модифікований метод передбачає використання довіреного центру, що верифікує публічні ключі Користувачів і формує цифрові підписи на пари *<Ідентифікатор, публічний ключ>*, які кожна зі сторін перевіряє перед тим, як розпочати виконання протоколу.

1.2.6 Використання алгебри полів Галуа для реалізації концепції «нульових знань» при ідентифікації та автентифікації віддалених користувачів

В роботах [27, 28, 29, 30, 31, 32] представлені теоретичні та практичні аспекти реалізації строгої ідентифікації з використанням незворотних перетворень на полях Галуа. Досліджено циклічні властивості операції експоненціювання на полях Галуа,

утворюючий поліном яких є поліноміальним добутком двох простих поліномів з різними степенями. Аналогічно тому, як у традиційній алгебрі як базові операції механізмів криптографічного захисту використовується модулярне експоненціювання, в алгебрі полів Галуа застосовується експонентціювання полях. Що дозволяє значно прискорити час виконання програм та спростити апаратну реалізацію

1.3 Висновки до розділу та постановка задачі

Проведений аналіз літературних джерел засвідчує суттєву та зростаючу потребу у засобах ідентифікації віддалених користувачів. Це обумовлено стрімким розвитком та широким запровадженням інформаційних технологій у найрізноманітніші сфери життєдіяльності людини. Процес інформатизації та цифровізації суспільства створює як можливості для піднесення рівня життя людей на якісно новий рівень, так, й формує цілий спектр викликів та загроз пов’язаних із різного роду зловживаннями при неналежному використанні даних. Передумовою зловживань в інформаційній сфері є отримання зловмисниками несанкціонованого доступу, що визначає питання ідентифікації віддалених користувачів як першочергове.

В сучасних системах реалізовані різноманітні системи контролю доступу від апаратних, апаратно-програмних, програмно-апаратних до суто програмних які реалізують різноманітні технічні рішення та програмні алгоритми.

У випадку інформаційних систем та інформаційних технологій базовим інструментарієм згаданих питань є використання належних алгоритмів ідентифікації віддалених користувачів. Ці алгоритми повинні забезпечувати надійних захист від зловмисного проникнення, а з іншого – забезпечити комфортні умови доступу належним користувачам. Одними з найбільш ефективними є технології, які реалізують концепцію «нульових знань». Разом із тим, застосування цієї технології потребує вирішення питання щодо рівня обчислювальної здатності.

В результаті проведеного аналізу існуючих підходів сформульовані такі

завдання дослідження метою якого є реалізація інформаційної технології ідентифікації користувачів на основі концепції «нульових знань» з достатнім рівнем обчислювальної здатності:

1) провести аналіз існуючих методів, технологій та рішень методів ідентифікації користувачів, що реалізують концепцію «нульових знань»;

2) вдосконалення існуючих методів ідентифікації у напрямку покращення обчислювальної здатності;

3) розробити інформаційну технологію ідентифікації користувачів за допомогою отриманих моделей та методів;

4) виконати експериментальну перевірку інформаційної технології ідентифікації користувачів.

Розділ 2
Розробка технології ідентифікації користувачів

2.1 Ідентифікація та автентифікація

Задля забезпечення належного доступу, захисту від зловмисного проникнення використовується комплекс засобів та методів, що забезпечують перевірку однією стороною у достовірності та правомірності іншої.

Процедура ідентифікації полягає у визначенні користувача за його ідентифікатором, здійснення якої відбувається при спробі користувача отримати доступ до ресурсів інформаційної системи. Під час цієї процедури, користувачем, за відповідним запитом системи, повідомляється власний ідентифікатор, наявність якого система перевіряє.

В цей же час, процедура автентифікації полягає у відповідній та належній перевірці справжності користувача (фізичної особи або технічного пристрою). Подібного роду перевірки мають за мету визначити, що користувач є саме тим, хто заявлений. Під час процедури автентифікації сторона, яка виконує перевірку, пересвідчується, що сторона, яка перевіряється, є справжньою.

Процедури ідентифікації та автентифікації взаємопов’язані між собою, й, по суті, полягають у розпізнаванні та перевірці справжності. Зазначені процедури визначають, чи отримає користувач доступ до ресурсів інформаційної системи або отримає відмову (рис. 2.1)

З процедурної точки зору проста автентифікація полягає у введенні користувачем ідентифікатора та пароля при спробі входу в систему. Далі відповідний сервер по власній базі даних знаходить або ні відповідний запис. У разі їх відмінності, користувач отримує відмову в доступі, в іншому випадку користувач отримує доступ до відповідних ресурсів з відповідними правами (рис. 2.2).

З точки зору повного унеможливлення розголошення або отримання доступу до певного роду приватної інформації, є використовується концепція «нульових

знань» щодо якої потрібно забезпечити прийнятний рівень обчислювальної складності.

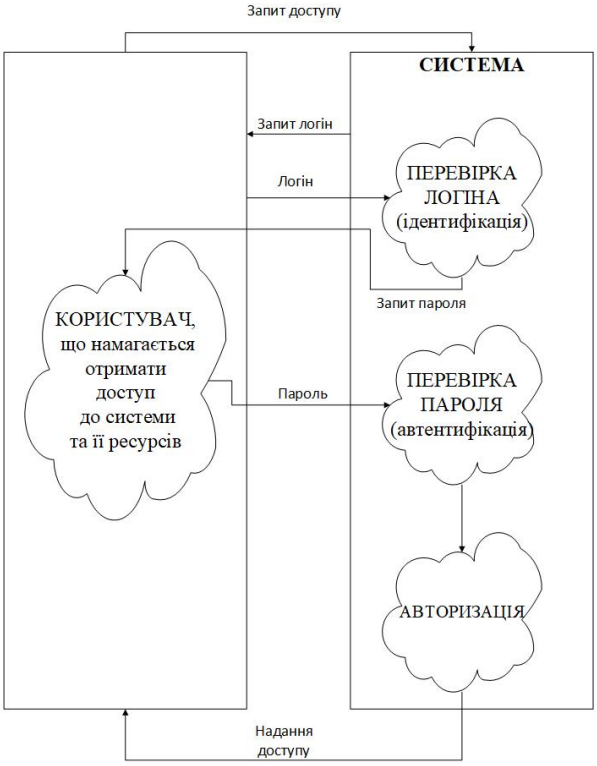


Рисунок 2.1 –Процедури ідентифікації та автентифікації

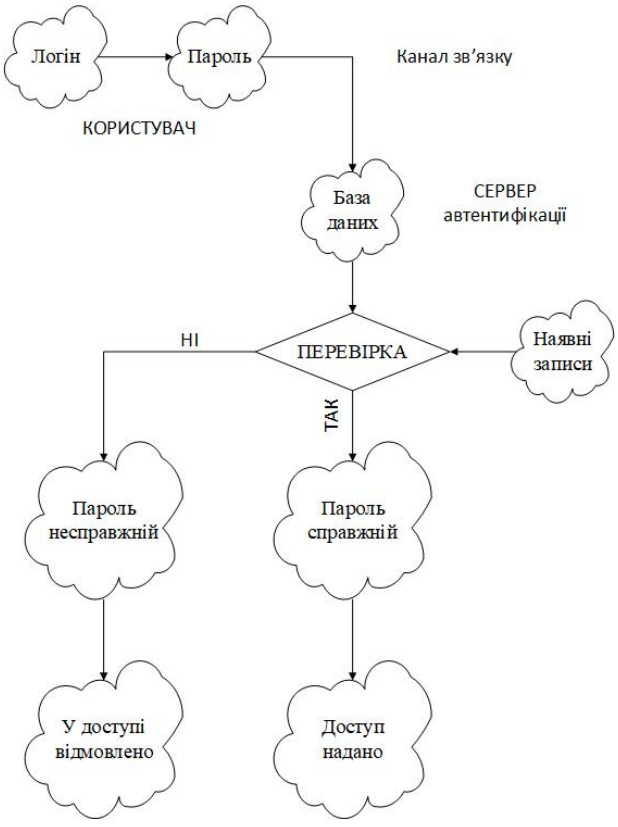


Рисунок 2.2. – Проста ідентифікація з паролем

2.2 Організація ефективного експоненціювання на полях Галуа

Поле Галуа або скінченне поле містить скінчену множину елементів. Найменше за розмірами поле Галуа складається з усього з двох елементів. Арифметичні операції над елементами полів Галуа виконуються майже як звичайно, за деякими винятками.

Базова ідея щодо використання застосування полів Галуа полягає у розгляді послідовності одиниць та нулів, як елементів певної алгебраїчної структури,операції в якій призводять до деяких важливих конструкцій.

Надважлива передумова ефективної та безпечної взаємодії відповідних віддалених користувачів та інформаційних систем полягає у наявності необхідних механізмів контролю та регулювання доступу до наявних інформаційних ресурсів. Як основа сучасних методів ідентифікації використовуються операції модулярної арифметики над числами розрядність яких суттєво перевищує розрядність процесорів, та, відповідно, потребують великих обчислювальних ресурсів та витрат, як апаратних так й часових.

Задля підвищення швидкодії в методах ідентифікації доцільним є використання алгебри кінцевих полів Галуа зі зменшеними часовими потребами на реалізацію операції експоненціювання. Можливості щодо реалізації такого підходу обумовлені наступною властивістю поліноміального квадрату - двійкові розряди поліноміального квадрату числа на парних позиціях дорівнюють нулю, а на непарних - співпадають з двійковими розрядами числа.

Задля обчислення на кінцевих полях попередньо виконується формування двох таблиць W та T, перша з яких не залежить від числа, й потреба у її попередньому формуванні визначається зміною M - числа, що відповідає утворюючому поліном кінцевого поля.

Формування першої W виконується в такому порядку.

1. $W[0] = 2^n \operatorname{rem} \mathrm{M},\ i = 0.$
2. $W[i] = 2W[i-1] \operatorname{rem} \mathrm{M},\ i = i + 1.$

3. Якщо $i < \frac{n}{2}$, виконується повернення до п.2.

Порядок формування першої таблиці наведений на рис. 2.3.

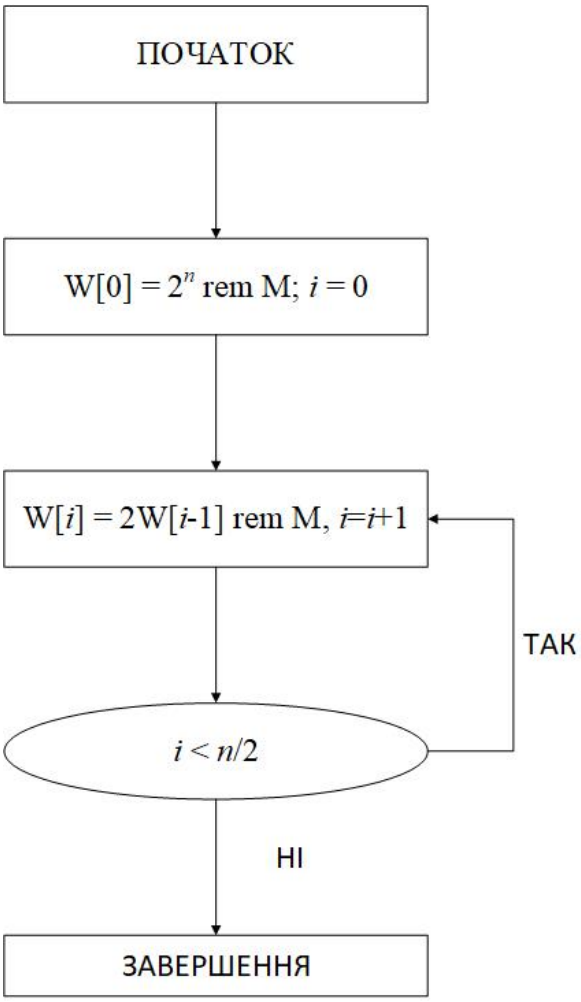


Рисунок 2.3 - Порядок формування першої таблиці

Друга таблиця T заповнюється перед початком обчислення $A^E \text{ rem M}$ у такій послідовності.

1. $T[0] = A;\ j = 0$.

2. $T[j] = 2T[j-1] \text{rem M},\ j = j+1$.

3. Якщо $j < n$, виконується повернення до п. 2.

Порядок формування другої таблиці наведений на рис. 2.4.

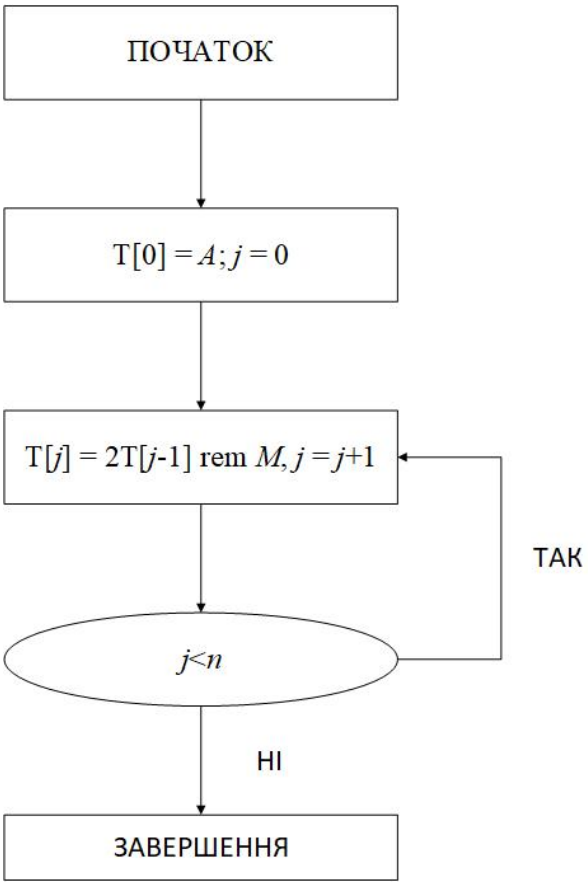


Рисунок 2.4 - Порядок формування другої таблиці

Процес експоненціювання організовується у вигляді n раз повторюваного циклу з такою послідовністю дій (рис. 2.5).

1. $R = 1,\ j = n - 1.$

2. Якщо $e_j = 0$, виконуються пп. 2.1 - 2.7.

2.1. $i = 0,\ D = 1,\ S = 0.$

2.2. Якщо $r_i = 0$, виконується перехід на п. 2.5.

2.3. Якщо $i < \frac{n}{2}$, тоді $S = S + D.$

2.4. Якщо $i > \frac{n}{2}$, тоді $S = S + W\left[i - \frac{n}{2}\right].$

2.5. $D = 2D,\ i = i + 1.$

2.6. Якщо $i < n$, виконується повернення до п. 2.2.

2.7. Якщо $i > n$, виконується перехід до п. 4.

3. Якщо $e_j = 1$, виконуються пп. 3.1 - 3.6.

3.1. $i = 0,\ S = 0$.

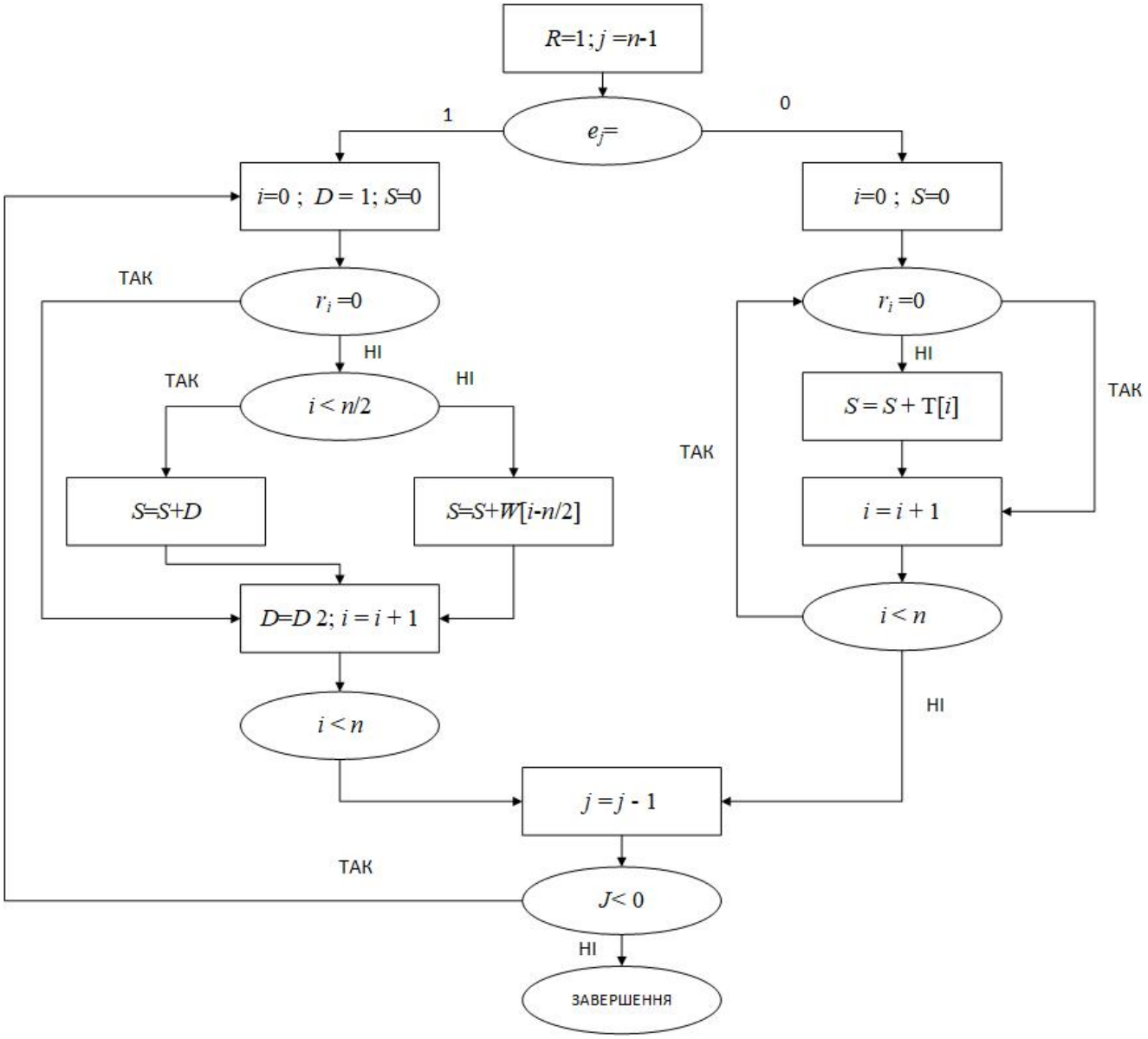


Рисунок 2.5 - Організація процесу експоненціювання

3.2. Якщо $r_i = 0$, виконується перехід до п. 3.4.

3.3. $S = S + T[i]$.

3.4. $i = i + 1$.

3.5. Якщо $i < n$, виконується повернення до п. 3.2.

3.6. Якщо $i > n$, виконується перехід до п. 4.

4. $j = j - 1$, якщо $j \geq 0$, виконується повернення до п. 2.

2.3 Метод строгої ідентифікації користувачів

Метод ідентифікації віддалених користувачів з реалізацією концепції «нульових знань» містить дві базові процедури (рис. 2.6):

- реєстрації користувача,
- ідентифікації користувача системою.

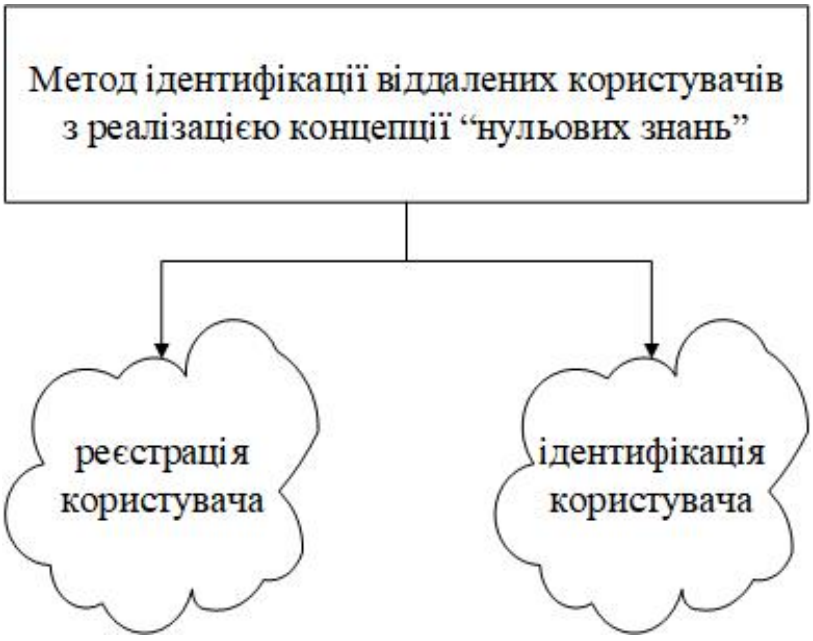


Рисунок 2.6. –Базові процедури методу ідентифікації віддалених користувачів з реалізацією концепції «нульових знань»

Використання різноманітних криптографічних алгоритмів визначають сутність процедур строгої ідентифікації (рис. 2.7)

Процедура реєстрації виглядає наступним чином.

1. Системою надсилається користувачеві її публічний ключ $K\text{п}$.

2. Користувачем довільним чином обирається пара простих поліномів $p(x)$ та $g(x)$ з різними ступенями.

3. Користувачем здійснюється формування поліному $M(x)$ у вигляді поліноміального добутку обраних поліномів $p(x)$ та $g(x)$ - $M(x) = p(x) \otimes g(x)$.

4. Число m, яке відповідає поліному $M(x)$ є відкритим ключем Користувача.

5. Відкритий ключ користувача шифрується публічним ключем *К*п та надсилається системі.

6. Система, використовуючи секретний ключ Kc, відновлює значення *m* ключа Користувача, та заносить його в базу даних.

Процедура реєстрації передбачає послідовність дій представлену на рис. 2.8.

Рисунок 2.7 - Протоколи строгої автентифікації

Процедура одного циклу ідентифікації передбачає такий порядок дій та представлена на рис. 2.9.

1. Користувачем генерується випадкове число k, яке має бути меншим ніж 2^d та виконується поліноміальне множення поліному $k(x)$, який відповідає числу k, на поліном $p(x)$ - $q(x) = k(x) \otimes p(x)$.

2. Користувачем генерується випадкове число $U < 2^d$ та виконується експоненціювання на полі Галуа з базовим поліномом $M(x)$ - $R = q^{U} \text{ rem M}$.

3. Користувачем обчислюється значення виразу $E = 2^d - U$.

4. В систему надсилається сеансовий пароль користувача, який складається із таких чисел $< q, R, E >$.

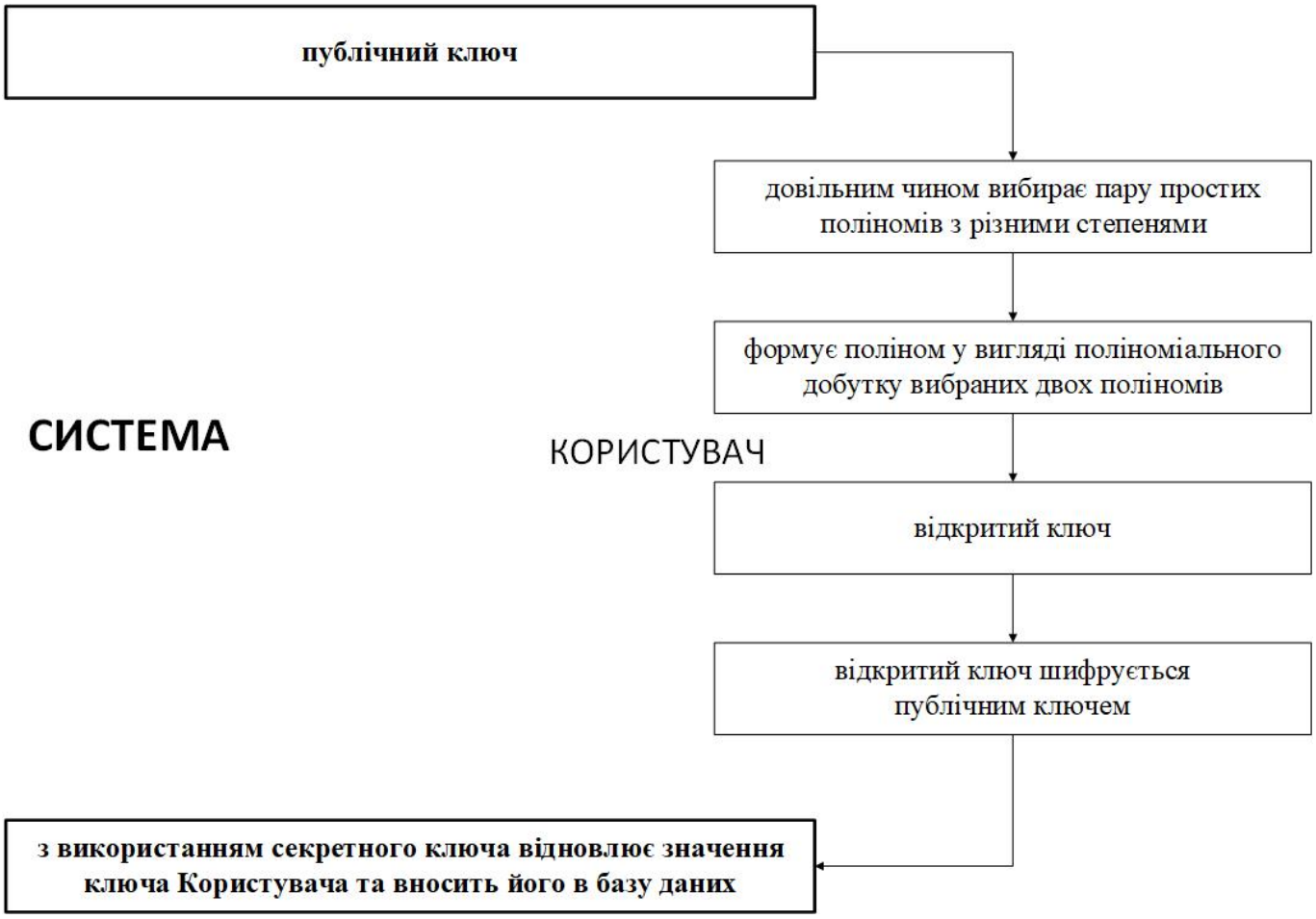


Рисунок 2.8 - Послідовність дій при реєстрації користувача

5. Система отримує від користувача сеансовий пароль $< q, R, E >$ та шляхом піднесення q до степені E в полі Галуа з базовим поліномом $M(x)$ обчислює $\rho = q^{U} \operatorname{rem} M$.

6. Система обчислюється добуток в полі Галуа - $\eta = \rho \otimes R \operatorname{rem} M$.

7. Результат η порівнюється з q.

8. Ідентифікація користувача вважається успішною, якщо $\eta = q$.

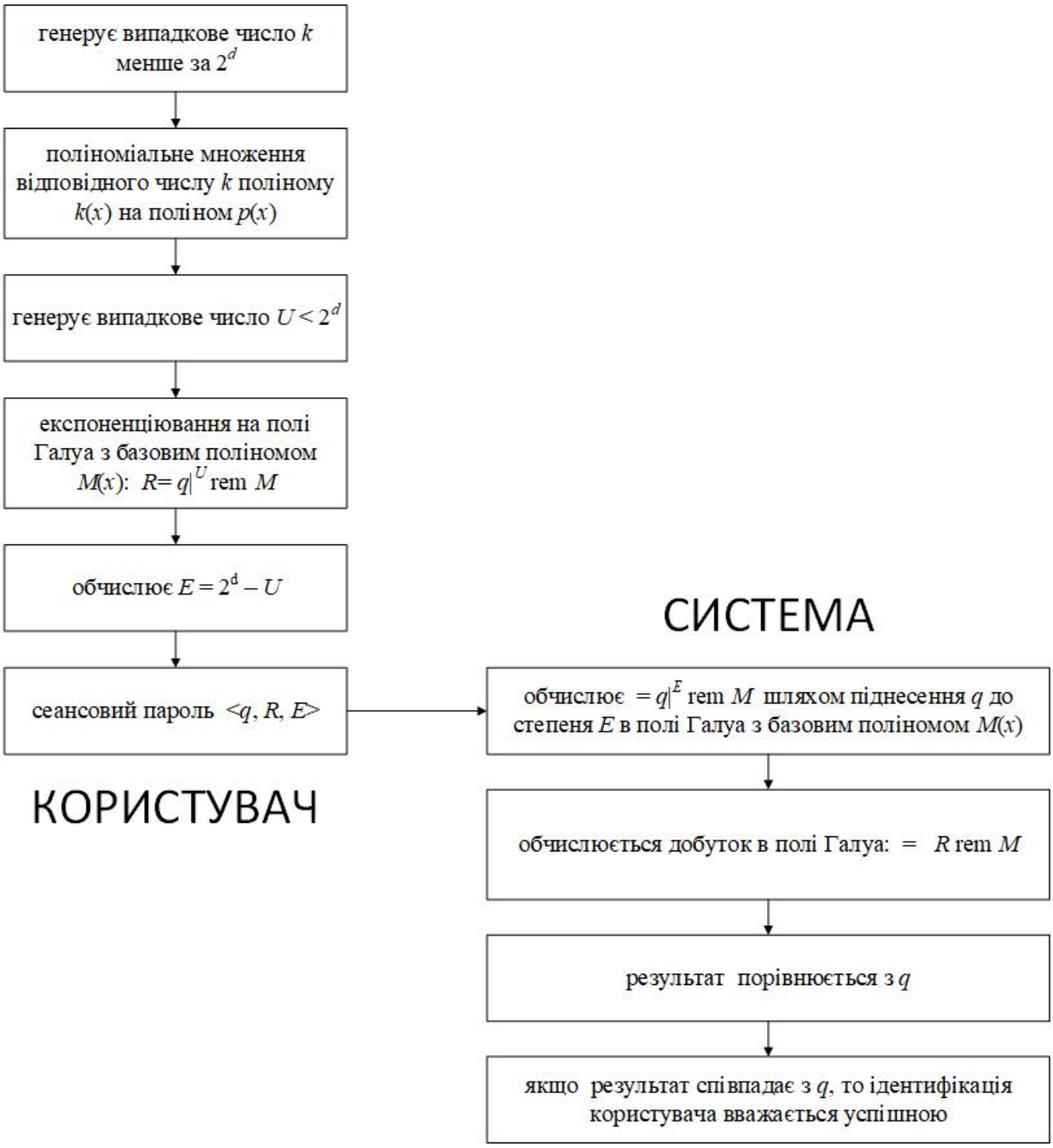


Рисунок 2.9 - Процедура одного циклу ідентифікації

Висновки до розділу 2

Задля підвищення швидкодії в методах ідентифікації використано алгебру кінцевих полів Галуа зі зменшеними часовими потребами на реалізацію операції експоненціювання. Суть процедури полягає в обчисленні на кінцевих полях з

використанням попередньо сформованих двох таблиць.

Процес експоненціювання організовується у вигляді n раз повторюваного циклу з реалізацією наведеної послідовністю дій

Метод ідентифікації віддалених користувачів за концепцією “нульових знань” представлений як двохпрцедурний. Представлена послідовність дій при реєстрації віддаленого користувача та наведена процедура одного циклу ідентифікації.

Розділ 3
Інформаційна модель технології ідентифікації користувачів

3.1 Вибір технологій та їх обґрунтування

3.1.1 Обґрунтування вибору мови програмування

Створювана інформаційна технологія ґрунтується на реалізації криптографічних методів, які, у свою чергу, базуються на математичних операціях, й тому доцільним є використання мову програмування та відповідних засобів розробки, що мають розширений набір вбудованих методів та зовнішніх бібліотек призначених для роботи з числами. Серед мов програмування, які є найбільш придатними для розв'язання такого класі математичних задач відносяться, в першу чергу, R, Ruby, Python, Haskell та C. Основні особливості використання зазначених мов програмування з точки зору зручності виконання потрібних математичних операцій та роботи із числами полягають у наступному.

Мова R пропонує розробнику комплекс графічних інструментів для розробки та реалізації зображень. В більшості випадків мову програмування R використовують за її статистичну обчислювальну потужність. У наявності є велика кількість бібліотек для мови R, що пов'язано її з відкритим кодом. Головною перевагою мову програмування R є значний потенціал для візуалізації даних, хоча робота з пам'яттю є повільною у поєднанні з невисокою загальною ефективністю.

Мова програмування Ruby надає широкий набір засобів задля роботи з математичними операціями. Суттєвою мови програмування Ruby є значна кількість шаблонів для проектування різнопланових застосувань та роботи з ними, зокрема, великий вибір інструментів задля проведення тестів, стандартні шаблони для веб-додатків тощо, у поєднанні зі швидкістю й значною кількість бібліотек. Недоліками слід вважати скромну документацію для сторонніх модулів й невелику швидкість виконання.

Мова C є однією з найбільш поширених мов програмування, яка працює

достатньо швидко, оскільки виконує багато функцій, вбудованих в інші мови програмування високого рівня, такі як - перевірка індексування масиву, алокація та звільнення пам’яті тощо. Як наслідок, мова програмування C є складною із громіздкими написаними на ній програми що ускладняється достатньо невеликим набором вбудованих методів для роботи з числами.

Python - мова програмування високого рівня з широким вибором вбудованих методів для математичних операцій, які доповнюються відповідними модулями та відкритими бібліотекам у загальному доступі. Швидкість runtime є високою, що обумовлює її ефективність при написанні програмного забезпечення із жорсткими часовими нормативами на виконання.

Як підсумок, найбільш раціональною мовою програмування задля реалізації інформаційної технології ідентифікації користувачів слід вважати Python, яка пропонує значну кількість бібліотек задля оптимальної роботи з математичними алгоритмами та є задовільною з точки зору вимог щодо швидкості виконання реалізованих програм (рис. 3.1).

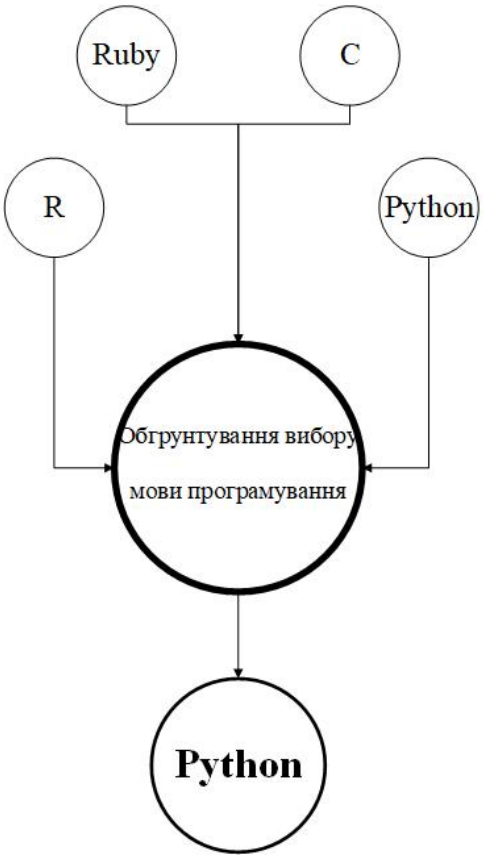


Рисунок 3.1 - Обґрунтування вибору мови програмування

3.1.2 Вибір модулів та бібліотек

Реалізація інформаційної технології ідентифікації користувачів передбачає використання певних криптографічних алгоритмів на етапі реєстрації користувача в системі. На цьому етапі система надсилає користувачеві публічний ключ по незахищеному каналу передачі даних, що обумовлює необхідність імпорту бібліотеки, яка реалізує криптографічні методи захисту даних. Потрібний функціонал містить бібліотека pycryptodome.

Задля досягнення потрібного рівня захищеності щодо запропонованого методу розрядності операндів мають сягати 2048, що суттєво ускладнює реалізацію таких операцій, як поліноміальне множення, поліноміальне ділення з остатком та експоненціювання вбудованими засобами мови Python. Без залучення сторонніх бібліотек достатній рівень захисту не може бути досягнуто, оскільки ресурсів, які виділяються операційною системою компілятору Python за замовчуванням не вистачає. Зазначена обставина потребує бібліотеки, яка полегшує роботу з числами великих розрядностей, але, разом із тим, зберігає швидкість виконання на високому рівні. Заданим вимогам задовольняє бібліотека gmpy.

Для реалізації певних функцій є потреба в операціях з випадковими числами, що обумовлює використання модуля random, який входить до стандартного пакету модулів Python.

Ще одним модулем, який пропонує широкий арсенал методів для роботи з числами є модуль math.

Взаємодія системи та користувача здійснюється через канал передачі даних поетапно й кожна зі сторін повідомляє іншу щодо виконання своєї частини методу. Доцільно реалізувати це за допомогою сигналів, кожен з яких має унікальний ідентифікатор. Це дозволяє розпізнати, який саме етап виконання було пройдено іншою стороною та/або сповістити іншу сторону про виконання певного етапу. Це обумовлює використання модуля є enum, що дозволяє задіяти типи даних найбільш придатних для реалізації сигналів.

Ілюстрація використовуваних бібліотек та модулів представлена на рис. 3.2

Рисунок 3.2 - Бібліотеки та модулі, які використовуються при реалізації інформаційної технології ідентифікації користувачів

3.2 Структура програми

Реалізовану програму умовно можна поділити на декілька структурних

модулів (рис. 3.3):

- модуль для знаходження простих поліномів,
- модуль для шифрування повідомлень,
- модуль з реалізацією методу ідентифікації.

Рисунок 3.3 - Основні модулі системи

Функціонал першого модуля полягає у генерації двох простих поліномів великої розрядності користувачем задля формування модулю *m*.

Необхідність другого модуля обумовлена незахищеністю каналу передачі даних між системою та користувачем. Уразі спроби несанкціонованого доступу зловмисник може напочатку стежити за обміном повідомленнями між сторонами протоколу, читаючи незашифровані повідомлення й спотворюючи деякі, потрібні, з них. З цієї причини в запропонованому методі ідентифікації віддалених користувачів передбачається обмін зашифрованими повідомленнями на тому етапі, коли користувач обчислює модуль й надсилає його системі. Уразі використання алгоритму шифрування на цьому етапі, зловмисник не зможе відтворити модуль користувача, принаймні у прийнятний для нього період час. Без інформації про модуль, передаванні дані, а саме, значення *q, R, E,* не матимуть жодного практичного сенсу, оскільки відомості лише про них не дозволяють відтворити секретну інформацію щодо ідентифікації користувача. Як алгоритм шифрування було обрано RSA, який на поточний є одним з найбільш надійних алгоритмів шифрування із високим рівнем захищеності за відносно невелику кількість обчислень.

В третьому модулі зосереджена основна логіка програми, реалізована за допомогою чотирьох класів та трьох методів.

Клас DataTransferChanel імітує канал передачі даних (обмін повідомленнями та сигналами) між системою та користувачем й користувачем та системою. Процедура реєстрації відбувається таким чином. На початку користувач надсилає системі сигнал сповіщення про ініціалізацію процедури реєстрації по незахищеному каналу передачі даних. Система отримує та опрацьовує триманий сигнал. Надалі система звертається до модуля RSA та генерує пару ключів відповідної розрядності. Приватний ключ система зберігає у себе в пам’яті, а публічний пересилає користувачеві разом із відповідним сигналом, який дозволяє користувачеві розпізнати надіслане повідомлення. Користувач отримує публічний ключ системи й починає виконувати свою частину обчислень для протоколу реєстрації, а саме, генерує два простих неприводимих поліномів різної розрядності та обчислення їх добутку. На першому етапі відбувається звернення до модуля Prime_gen.py, який з використанням розширеного алгоритму Евкліда за поліноміальний час знаходить

прості поліноми *p* і *g* заданої розрядності. Потім викликається процедура mul(a,b) обчислення модуля *m* як добутку двох простих поліномів *p* і *g*. Після закінчення обчислень користувач використовує публічний ключ системи $К_с$, який був отриманий на початку, задля шифрування отриманого значення модуля *m* та надсилає його по незахищеному каналу передачі даних системі, завершуючи свою частину протоколу реєстрації. Далі система, отримавши повідомлення користувача разом з відповідним сигналом-ідентифікатором, за допомогою свого приватного ключа відтворює справжній модуль *m*. Потім у відповідь система надсилає користувачеві сигнал про підтвердження отримання ключа та завершення процедури реєстрації.

Процедура ідентифікації користувача є такою. На початку, користувач ініціює початок протоколу ідентифікації, через надсилання системі по каналу передачі даних спеціального сигналу. Далі система, після отримання сигналу та його обробки, переходить у стан готовності до отримання значень <*q,R,E*> та їх подальшої обробки. Програма користувача з використанням бібліотеки random генерує випадкове значення *k*. завдяки процедуру *mul(a,b)* обчислює добуток *k* на *p* та генерує випадкове значення *U* й обчислює з $R = q|^{U} rem\ m$. На цьому етапі використовуються процедури *mod(A,e)* та *exp(A,E)*. Перша з цих процедур виконує ділення із залишком, й фактично приводить число в поле Галуа, а друга – використовуючи прискорений алгоритм, виконує експоненціювання на полях Галуа. Як результат обчислень користувач отримує другу компоненту кортежу. На наступному кроці програма користувача обчислює $E = 2^d - U$ за тими самими процедурами. Після обчислень, користувач надсилає системі <*q, R, E*> в сукупності з відповідним сигналом. Після цього програма користувача переходить в режим очікування й, фактично, припиняє участь в протоколі ідентифікації.

Система після отримання відповідного сигналу й інформаційного повідомлення від користувача здійснює обробку цього сигналу та зчитування відповідного інформаційного повідомлення. Потім згідно протоколу виконується передбачена послідовність ряду дій. А саме. Система обчислює значення $\varphi = q|^{E} rem\ m$ та $\eta = \varphi \cdot R\ rem\ m$ та порівнює їх значення. Якщо вказані значення не співпадають,

систему передає сигнал про невдалу спробу ідентифікації, в іншому випадку сповіщає користувача про вдалу спробу ідентифікації й, відповідно, надає йому доступ до своїх ресурсів.

Послідовність дій представлена на рис. 3.4.

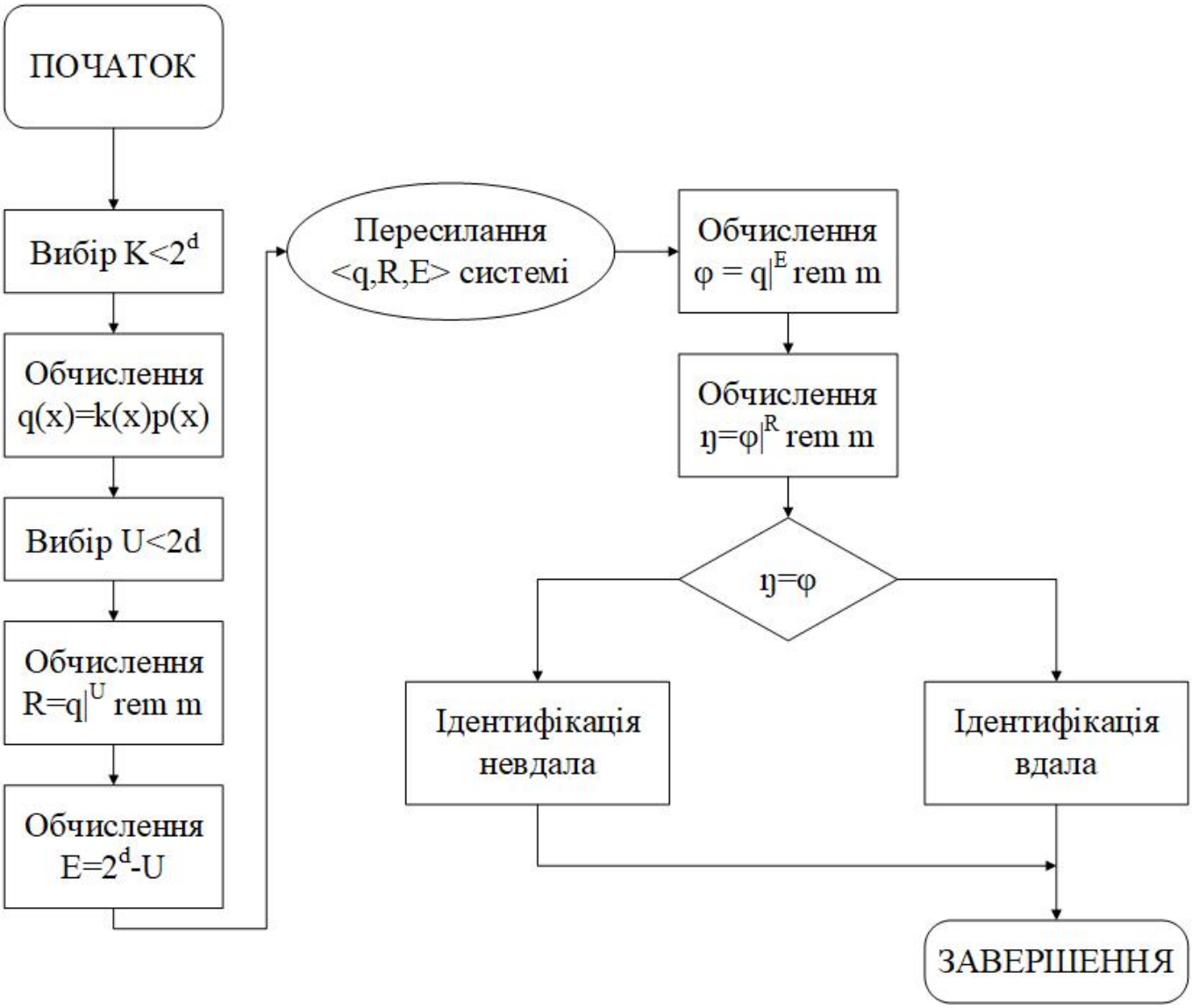


Рисунок 3.4 - Послідовність дій при ідентифікації користувача

3.3 Основні рішення з реалізації програми

До складу програми входять три файли (рис. 3.5):

- Rsa.py,

- Ident.py,

- Prime_gen.py.

У файлі Rsa.py реалізовано криптографічний алгоритм шифрування RSA, який використовується системою для генерації ключів шифрування та для шифрування користувачем свого модуля, який він надіслає системі.

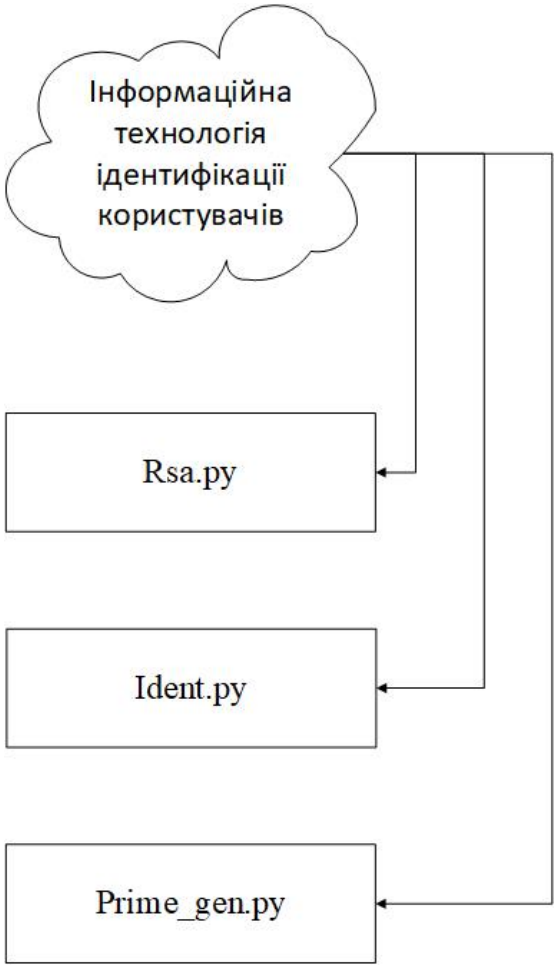


Рисунок 3.5 - Файли програмної реалізації інформаційної технології ідентифікації користувачів

У файлі ident.py реалізовано метод ідентифікації віддалених користувачів. Цефайл складається з таких чотирьох класів та процедур (рис. 3.6):

- класи – *Signal*, *User*, *System*, *DataTransferChanel*;

- процедури - *Mul(a,b)*, *Exp(A, E, m)*, *Mod(A,m)*.

Рисунок 3.6 – Класи та процедури файлу ident.py

Клас *Signal* зберігає різні типи сигналів, якими на відповідних стадіях ідентифікації та реєстрації обмінюються один з одним користувач та система.

Зміст класу *Signal* наступний:

Призначення сигналів є таким (рис. 3.7):

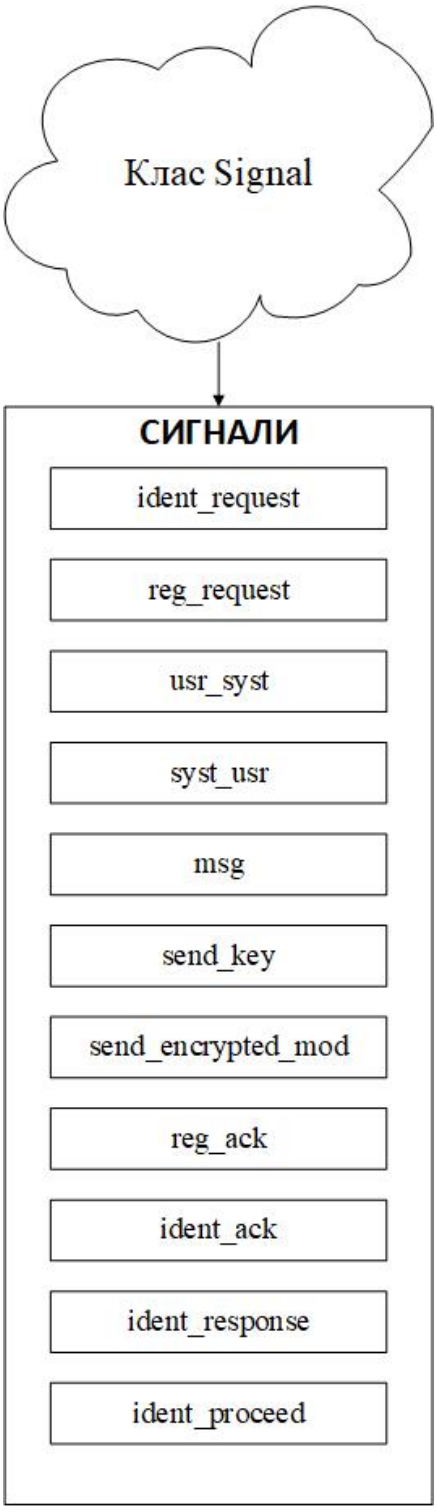


Рисунок 3.7 - Типи сигналі у класі *Signal*

- сигнал ident_request є сигналом про ініціацію процедури ідентифікації,

- сигнал reg_request є ініціацію процедури реєстрації,

- сигнал usr_syst позначає інформаційне повідомлення від користувача до системи,

- сигнал syst_usr позначає інформаційне повідомлення від системи до

користува,

- сигнал msg є силналом про інформаційний характер прикріпленого повідомлення,

- сигнал send_key надсилає системний публічний ключ користувачеві,

- сигнал send_encrypted_mod надсилає системі свій зашифрований модуль користувача,

- сигнал reg_ack про успішну реєстрацію користувача системою,

- сигнал ident_ack про успішне завершення системою процедури ідентифікації користувача,

- сигнал ident_response про надсилання ідентифікаційної інформації користувача системі,

- сигнал ident_proceed про підтвердження надходження повідомлень від іншої сторони на проміжних етапах протоколу ідентифікації.

В класі *System* міститься процедури виконувані системою у протоколах ідентифікації та реєстрації користувача (рис. 3.8). Це клас складається з таких процедур.

- процедура registrationRequest() здійснює обробку сигналу reg_req, що надсилається користувачем задля ініціалізації протоколу реєстрації. У відповідь система починає процедуру генерації пари ключів за алгоритмом RSA й відсилає сигнал send_key, а далі слідує повідомлення зі згенерованим публічним ключем системи.

- процедура receiveEncMod(msg) викликається після надходженні відповідного сигналу send_enc_mod за яким система викликає процедуру, яка у поєднанні алгоритму шифрування RSA та раніше згенерованого приватного ключа виконує дешифрування повідомлення та відновлення модуля, який надіслав користувач. Надалі системою зберігається у пам’ять модуль й, у відповідь, надсилається сигнал reg_ack, який сповіщає про успішну реєстрацію.

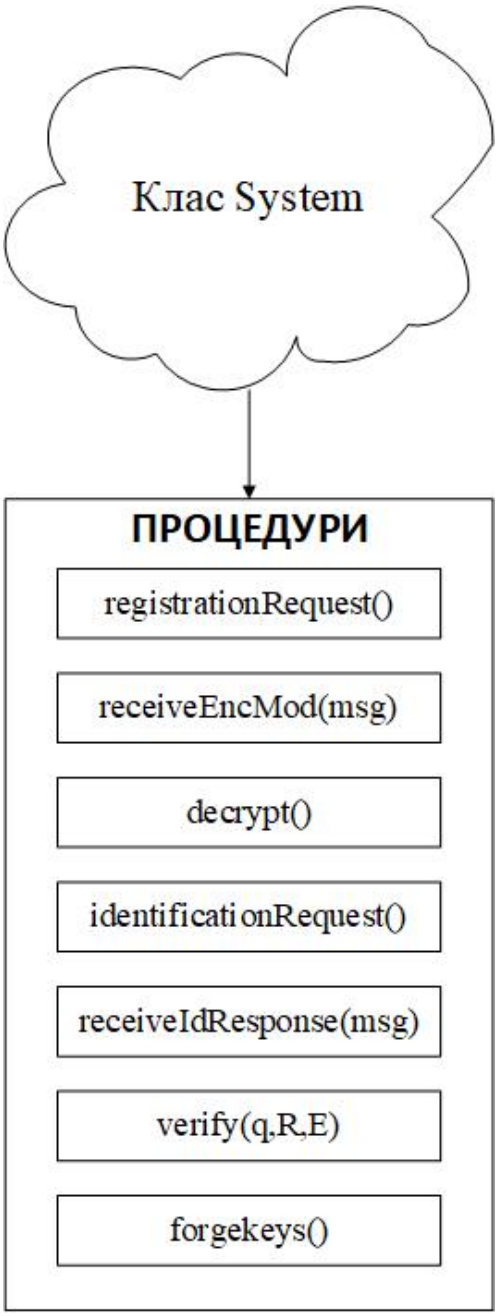


Рисунок 3.8 - Процедури в класі *Signal*

- процедура decrypt() ініціюється у разі потреби системи у розшифруванні повідомлення, яке отримано від користувача з використанням незахищеного каналу передачі даних, задля відтворення модуля користувача, із використанням раніше згенерованого за допомогою криптографічного алгоритму RSA приватного ключа.

- процедура identificationRequest() викликається після надходження сигналу ident_req, який надсилається користувачем задля ініціалізації протоколу ідентифікації. На початку система перевіряє наявність в системі запису з

ідентифікаційною інформацією користувача. У разі виявлення помилки протокол одразу припиняється. Якщо має місце збіг з одним із записів, системою надсилається сигнал ident_proceed і протокол, відповідно, продовжується.

- процедура - receiveIdResponse(msg) ініціалізується у разі надходження сигналу ident_response, після якого, у відповідності до протоколу, має слідувати повідомлення, яке містить у вигляді масиву набір значень <q, R, E>. Ця процедура здійснює розпаковку отриманого повідомлення та присвоює відповідним змінним відповідні числові значення з масиву. Надалі за параметрами розпакованих значень виконується процедура верифікації ідентичності користувача,

- процедура verify(q,R,E) реалізує відповідний алгоритм верифікації ідентичності користувача,

- процедура forgekeys() генерує пару ключів за криптографічним алгоритмом RSA.

У класі *User* реалізовано алгоритм користувача, який складається з таких процедури (рис. 3.9).

- процедура initiate_registration() ініціює протокол реєстрації надсилаючи системі сигнал reg_request та після отримання у відповідь визначеного сигналу й публічного ключа системи, забезпечує виконання тієї частини протоколу, яка передбачена для виконання користувачем, тобто здійснює виклик процедури генерації випадкових простих поліномів заданої розрядності та обчислення модуля через множення поліномів. Потім пересилає модуль системі.

- процедура initiate_identification() здійснює ініціалізацію протоколу ідентифікації. На початку система сповіщається через відповідний сигнал ident_request, а потім, згідно протоколу користувача, виконується відповідна частина обчислень. Після цього здійснюється виклик процедури id_compute(), яка обчислює *q, R, E.* Після сигналу ident_response виконується пересилка набору значень *q, R, E*.

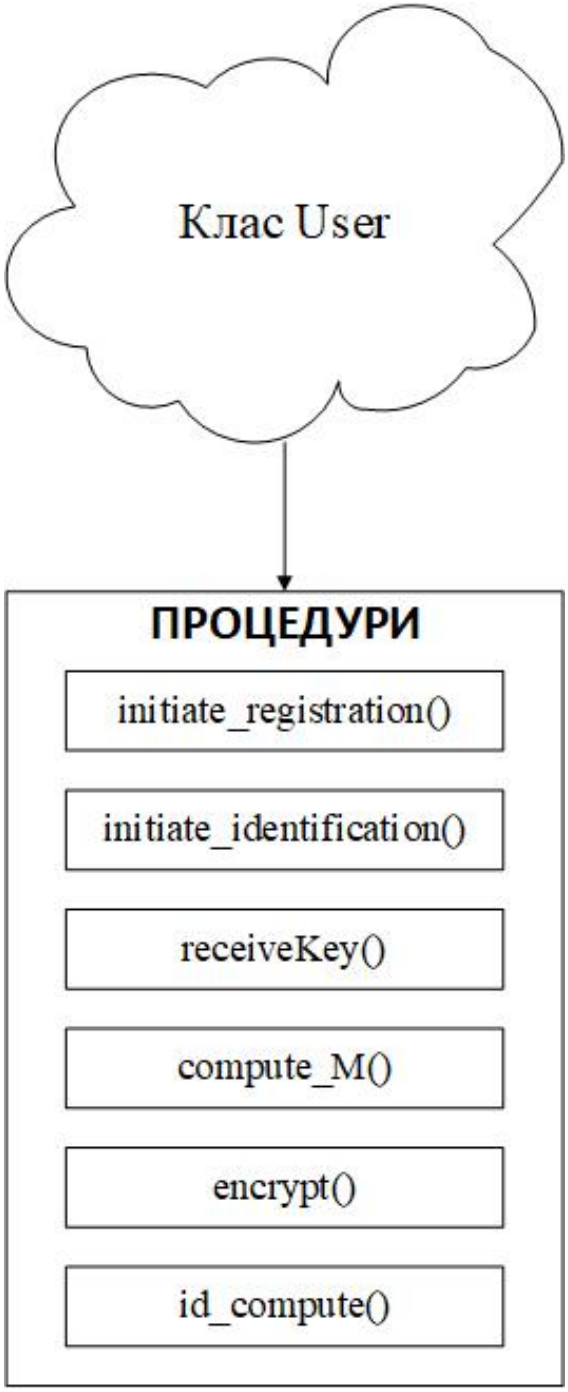


Рисунок 3.9 - Процедури класу *User*

- процедура receiveKey() викликається після сигналу send_key й забезпечує обробку повідомлення, розпаковку публічного ключа системи та його зберігання.

- процедура compute_M() забезпечує обчислення модуль *m* за раніше обраними двома простими поліномами заданої розрядності, використовуючи модуль Prime_gen.py. Отримавши поліноми, забезпечує виклик процедури множення та

зберігання розрядності обох операндів.

- процедура encrypt() шифрує значення модуля *m*, використовуючи алгоритм RSA й публічний ключ системи, та надсилає його системі.

- процедура id_compute() забезпечує реалізацію частину протоколу користувача по визначенню значень *q, R, E*.

Клас *DataTransferChanel* симулює каналу передачі даних, яким здійснюється взаємодія користувача і системи. Цей клас включає метод send() (рис.3.10).

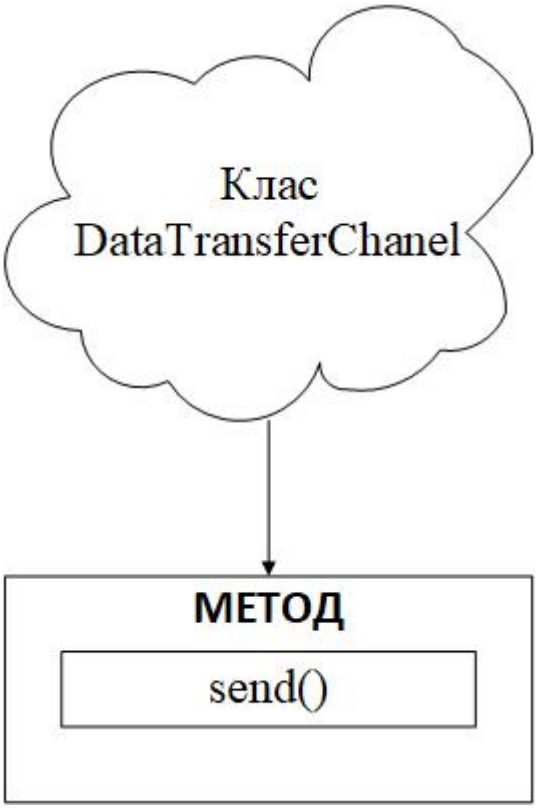


Рисунок 3.10 – Метод класу *DataTransferChanel*

Цей метод викликається користувачем або системою при потребі у передачі даних. Як параметри методу приймаються екземпляр класу відправника повідомлення, код сигналу та повідомлення, що по замовчуванню є нульовим та може не завжди використовуватися. Код сигналу визначає перелік виконуваних інструкцій та викликає відповідний метод користувача або системи з інструкціями щодо обробки повідомлення або подальшого виконання.

До файлу ident.py входять такі обчислювальні процедури (рис. 3.11):

- mul(a,b) – процедура поліноміального множення двох поліномів
- mod(a, b) – процедура приведення числа довільної розрядності до поля Галуа
- exp(A, E, m) – процедура обчислення значення $A|^{E}$ *rem m.*

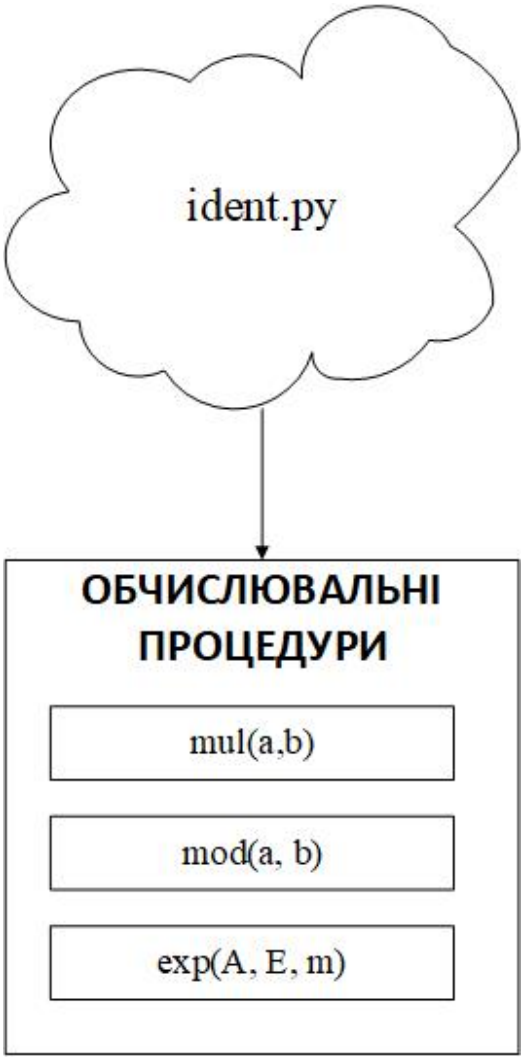


Рисунок 3.11 – Обчислювальні процедури у файлі ident.py

Процедура модулярного експоненціювання $A|^{E}$ *rem m* на полі Галуа полягає у послідовному виконання n циклів, в кожному з яких отримане на попередньому циклі значення піднесится до квадрату і в залежності від поточного біту експоненти E, додатково операція множення ($R \cdot A$) без переносів. Аналіз розрядів експоненти здійснюється від старших розрядів, тобто модулярне експоненціювання вивчається зліва направо.

У файлі prime_gen.py реалізується алгоритм знаходження простих поліномів необхідних користувачу задля формування модуля.

У файлі RSA.py реалізовано криптографічний алгоритм шифрування RSA, що вже мав використання раніше в основній програмі для генерування пари ключів, шифрування та розшифрування повідомлень.

Загальна структура представлена на рис. 3.12.

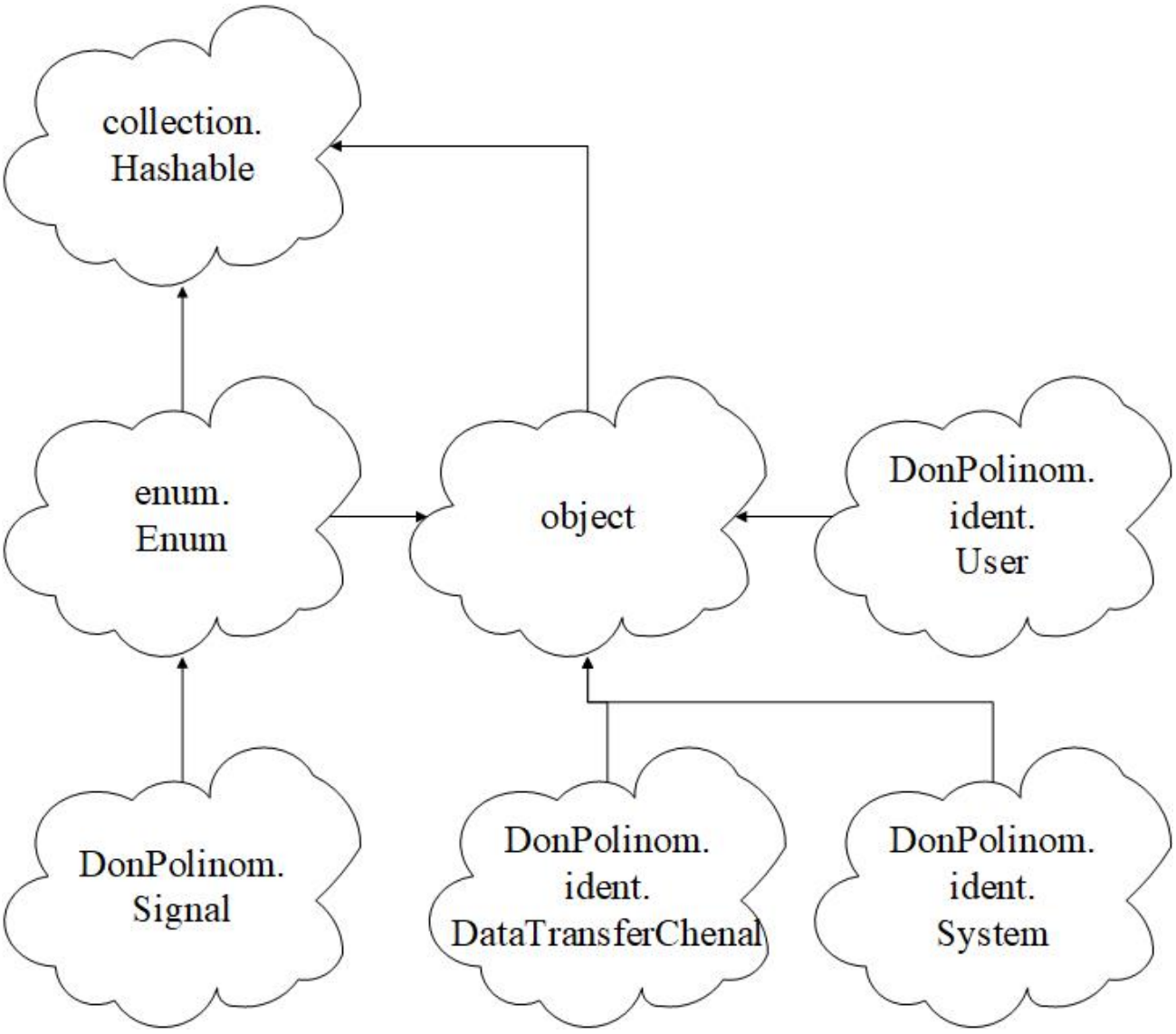


Рисунок 3.12 – Загальна структура програми

Висновки до розділу 3

Представлена інформаційна модель технології ідентифікації користувачів.

Інформаційна технологія реалізована з використанням мови Python. При програмній реалізації інформаційної технології ідентифікації користувачів було використано дві бібліотеки та три модуля мови програмування Python.

Реалізована інформаційна технологія ідентифікації користувачів складається з трьох структурних модулів та реалізована як сукупність трьох файлів з відповідними класами та процедурами з використанням процедури модулярного експоненціонування на полях Галуа та криптографічного алгоритму RSA.

Розділ 4
Апробація інформаційної технології ідентифікації користувачів

Одним із базових показників за яким виконується оцінювання ефективності криптографічного алгоритму виступає його обчислювальна складність. При визначенні згаданої обчислювальної складності користуються функцією, яка відбиває осяг потрібних для розв'язку задачі обчислювальних ресурсів щодо об'єму початкових даних.

З практичної точки зору обчислювальна складність відповідає часу виконання алгоритму.

Задля демонстрації ефективності запропонованої інформаційної технології ідентифікації користувачів проаналізуємо його ефективності з позиції часу виконання.

Обчислювальна складність методу ідентифікації в рамках реалізованої інформаційної технології визначається обчислювальною складністю його відповідних обчислювальних процедур, тобто загальний об'єм обчислень перебуває в прямій залежності від об'єм обсягу обчислень, які необхідні для виконання згаданих процедур й, відповідно, зменшення часу їх виконання безумовно призводитиме до зменшення загального часу реалізації методу. Також виконання порівняння швидкості виконання реалізованих методів ідентифікації можна виконувати шляхом порівняльної оцінки швидкості виконання базової операцій, якою є операція експоненціювання.

При виконанні порівняння реалізованого в рамках інформаційної технології ідентифікації користувачів методу з існуючими, здійснено оцінювання часу виконання операції експоненціювання $A^E mod\ m$ в модулярній та в поліноміальній арифметиках за різними значеннями параметрів A і E.

Обрахунки здіснювалися за такими початковими даними - $p = 10^{303} + 237$, $g = 10^{143} + 3^4$, $m = p \cdot g$, $A = 10^{143} + 3^4$, $E = \{200, \ldots, 200 \cdot 10^{10}\}$

Вимірювання періодів часу на здійснення виконання операцій

експоненціювання виконувалося з використання вбудованих інструментів мови Python призначених для роботи з системним часом. Таким інструментарієм є модуль time із методом time() для отримання потрібного актуальне значення системного годинника з високо точністю.

Під час проведення експерименту виконувалися послідовні заміри періоду часу на виконання операцій експоненціювання в модулярній арифметиці та на полях Галуа з подальшим збільшенням величини значення експоненти E на один порядок на кожній наступній ітерації циклу.

Результати обчислювального експерименту свідчать про відносно менший час виконання операції експоненціювання з використанням модулярної арифметики ніж з використанням полів Галуа при невеликих значеннях експоненти E. Але при перевищення значенням експоненти величини 10^4 час експоненціювання з використанням модулярної арифметики починає стрімко зростати й сягає величини 35с при значенні експоненти 10^7. При виконанні операцій експоненціонування на полях Галуа спостерігає суттєво повільніше зростання часу виконання. Як результат, до прикладу, при значенні експоненти 10^8 час експоненціонування на полях Галуа менший за час експоненціонування в модульній арифметиці відрізняється більше ніж у 4000 разів (0,082с до 350,771с).

Результати порівняння представлені на рис. 4.1, 4.2.

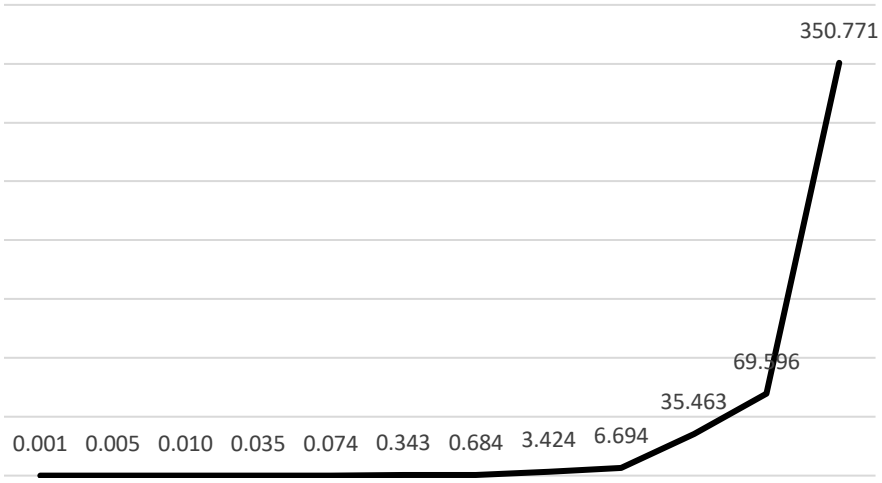


Рисунок 4.1 – Час на виконання операцій експоненціонування в модулярній арифметиці

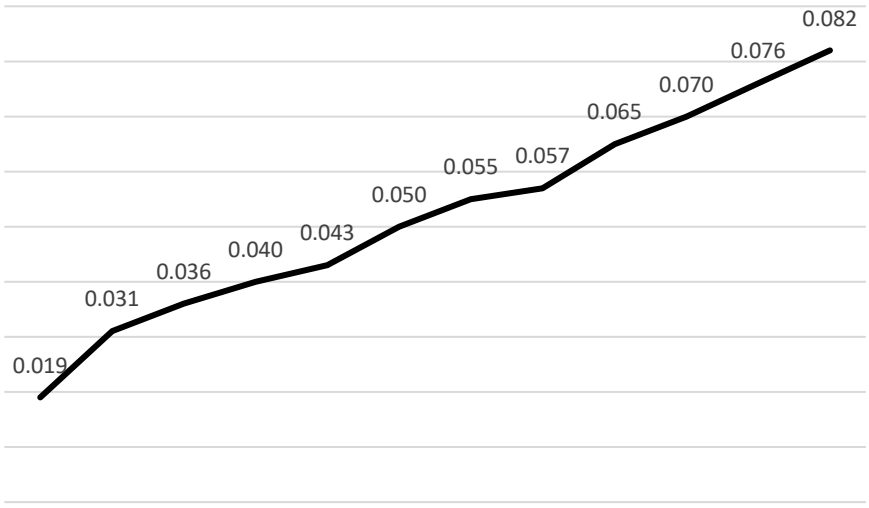


Рисунок 4.2 – Час на виконання операцій експоненціонування на полях Галуа

Тобто, операція експоненціювання як базова обчислювальна процедурою для методів ідентифікації, виконується за менший проміжок часу при використанні поліноміальної арифметики у порівнянні при використанні модулярної при значеннях експоненти більше ніж 10^4. При значеннях експоненти менше за 10^4 використання як поліноміальної так й модулярної арифметики є однаково ефективними.

Висновок до розділу 4

Поредена апробація запропонованих для реалізації інформаційної технології ідентифікації користувачів підходів та процедур.

Отримані результати дозволили довести, що обслювальна складність при використанні поліноміальної арифметики є порівняною з випадком використання модулярної арифметики при невеликих (до 10^4) значеннях експоненти. Але зі збільшенням експоненти (вже до 10^8) обчсилювальна складність при використанні модулярної арифметики сутєво перевищує обчислювальну складність у разі використання поліноміальної арифметики.

Отримані результати чисельного експерименту підтверджують вірність підходів закладених в реалізованій інформаційній технології ідентифікації користувачів.

Загальні висновки

Дана робота є закінченим дослідженням, розв’язує науково-технічну задачу створення інформаційної технології ідентифікації користувачів. У рамках роботи поставлені та вирішені такі завдання:

1. За результатами аналізу існуючих методів, технологій та рішень методів ідентифікації користувачів обґрунтовано потребу у створення інформаційної технології, яка реалізує концепцію «нульових знань».

2. Удосконалено існуючих методів ідентифікації у напрямку покращення обчислювальної здатності, яка використовує метод експоненціонування з використанням поліноміальної арифметики.

3. Розроблено нову інформаційну технологію ідентифікації користувачів, яка має покращену обчислювальну здатність.

Виконано експериментальну перевірку інформаційної технології ідентифікації користувачів. Результати експериментального тестування запропонованої інформаційної технології довели її спроможність розв’язувати поставлені задачі.

Перелік посилань

1. Н.А. Кошева, Н.І. Мазниченко. Ідентифікація користувачів інформаційно-комп'ютерних систем: аналіз і прогнозування підходів / Системи обробки інформації, 2013, випуск 6 (113). – С. 215 – 223.

2. Галатенко В.А. Основы информационной безопасности: учебное пособие / В. А. Галатенко; под ред. академика РАН В.Б. Бетелина, 4-е изд. – М.: Интернет университет информационных технологий; БИНОМ. Лаборатория знаний, 2008. – 205 с.

3. Schneier B. Applied Cryptography. Protocols. Algorithms and Source codes in C./ Schneier B. / Ed. John Wiley. NY, - 1996, - P.758

4. Воронова В.А. Системы контроля и управления доступом / В.А. Воронова, В.А. Тихонов. – М.: «Горячая линия – Телеком», 2010. – 272 с.

5. Rivest R. L. A method for obtaining digital signatures and public-key cryptosystems./ Rivest R.L., Shamir A., Adleman L.// Communications of the ACM, - 1978 , - Vol. 21. - Issue 2, - PP. 120 – 126.

6. Даклин Пол. Простые советы по более разумному выбору и использованию паролей / Пол Даклин. [Електронний ресурс]. – Режим доступу до ресурсу: http:// www.infosecurity.ru/_gazeta/content/060525/article01.shtml.

7. Безмалый В. Парольная защита: прошлое, настоящее, будущее / В. Безмалый // Журнал «КомпьютерПресс». – 2008. – №9. [Електронний ресурс]. – Режим доступу до ресурсу: http://www.compress.ru/article.aspx?Id=20509&iid=901.

8. Джхунян В.Л. Электронная идентификация / В.Л. Джхунян, В.Ф. Шаньгин. – М.: NT Press, 2004. – 695 с.

9. Шумська А.О. Ідентифікуючі ознаки текстових повідомлень при встановленні автора // Ползуновский Вісник № 2, 2013. С. 265-266.

10. Голубев Г.А. Современное состояние и перспективы развития биометрических технологий / Г.А. Голубев, Б.А. Габриелян // Нейрокомпьютеры: разработка, применение. – 2004. – № 10. – С. 39-46.

11. Кухарев Г.А. Биометрические системы: методы и средства идентификации

личности человека / Г.А. Кухарев. – СПб.: Политехника, 2001. – 240 с.

12. Коновалов Д.Н. Технология защиты информации на основе идентификации голоса / Д.Н. Коновалов, А.Г. Бояров // [Електронний ресурс]. – Режим доступу до ресурсу: http://www.fact.ru/archive/07/voice.shtml.

13. Шарипов Р.Р. Идентификация и аутентификация пользователей по клавиатурному почерку / Р.Р. Шарипов // Электронное приборостроение: Научно практический сборник. – Казань: ЗАО «Новое знание», 2005. – Вып. 3(44).

14. Feige U.Zero knowledge proofs of identity/ Feige U.,Fiat A.,Shamir A. // Journal of Cryptology, - Vol.1, - No.2, - 1988, - PP.77-94.

15. Peng K. Attack against a batch zero-knowledge proof system./Peng K. // IET Information Security — IET, 2012. — Vol. 6, Iss. 1. — PP. 1–5. — ISSN 1751-8709 — doi:10.1049/IET-IFS.2011.0290

16. Боярский К.К. Введення в комп'ютерну лінгвістику // СП: НДУ ІТМО, 2013, С. 139

17. Menezes A. Handbook of Applied Cryptography/ A. Menezes, P. van Oorschot, S. Vanstone// CRC Press, - ISBN: 0-8493-8523-7, - 1996, - P. 816

18. Fiat A. How To Prove Yourself: Practical Solutions to Identification and Signature Problems/ Fiat A., Shamir A.// Springer, Berlin, Heidelberg, - 1987, — PP. 186–194. — P. 490.

19. Brassard G. Everything in NP can be argued in perfect zero-knowledge in a bounded number of rounds/ Brassard G., Crepeau C., Yung M.// Springer, Berlin, Heidelberg, - Vol. 372, - 1989, - PP. 111-119, - P.413

20. Kizza J. Feige-Fiat-Shamir ZKP Scheme Revisited/ Kizza J.// ESORICS 2012, LNCS 7459, - 2012.- PP. 541–556.

21. Ohta K. A Modification of the Fiat-Shamir Scheme/ Ohta K., Okamoto T.// Advances in Cryptology — CRYPTO’ 88. CRYPTO 1988. Springer, New York, NY. Lecture Notes in Computer Science, - Vol 403, - PP. 78-86, - P.250

22. Guillou L.C. A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memory/ Guillou, L.C., and

Quisquater, J.J// Eurocrypt’88 Abstracts, - 1988, - PP.71–75

23. Blum M. Non-interactive zero-knowledge and its applications./ Blum M., Feldman P., Micali S. // STOC'88: Proceedings of the twentieth annual ACM symposium on Theory of computing — New York City: ACM, - 1988. — PP. 103–112. — ISBN 978-0-89791-264-8

24. Guillou L.C. A “paradoxical” identity-based signature scheme resulting from zero-knowledge./ and Quisquater J.-J.// Advances in Cryptology, Proceedings of CKYP7‘0 ’88, - Lecture Notes in Computer Science, - Springer-Verlag, - 1989, - PP. 216-231.

25. Schnorr C.-P.. Efficient Signature Generation by Smart Cards/ Schnorr C.-P. //Journal of Cryptology, - Vol.4, - 1991, - PP.161-174.

26. Boneh D. On the Importance of Checking Cryptographic Protocols for Faults/ Boneh D., DeMillo R.A., Lipton R.J. // In: Fumy W. (eds) Advances in Cryptology — EUROCRYPT ’97. EUROCRYPT 1997. Lecture Notes in Computer Science, - Springer, Berlin, Heidelberg, - vol 1233. – PP. 232-243.

27. Okamoto T. Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes/ Okamoto T. //In: Brickell E.F. (eds) Advances in Cryptology — CRYPTO’ 92. CRYPTO 1992. Lecture Notes in Computer Science, - Springer, Berlin, Heidelberg, - vol 740. – PP. 31-53.

28. Виноградов Ю.М. Прискорення експоненціювання на полях Галуа в системах захисту інформації./ Виноградов Ю.М., Агеєнко Ю.М.// Век+. - Вісник НТУУ «КПІ». Інформатика, управління та обчислювальна техніка: збірник наукових праць, - Вип. 55. – 2012. – С.5

29. Захаріудакіс Лефтеріс, Олієвський А.А. Метод строгої ідентифікації віддалених користувачів з використанням перетворень на полях Галуа // Інформаційні системи та технології Summer InfoCom AdvAnCed SolutIonS 2017, 2017 – С. 56 – 57.

30. Николайчук Я.М. Коди поля Галуа: теорія та застосування. – Тернопіль: ТзОВ “Терн граф”, - 2012. - 576 с.

31. О.П. Марковський, Захаріудакіс Лефтеріс, В.Р. Максимук. Використання алгебри полів Галуа для реалізації концепції «нульових знань» при ідентифікації та

автентифікації віддалених користувачів // Электронное моделирование. - 2017. - Т. 39. - № 6. – С. 33 – 45.

32. Захаріудакіс Лефтеріс. Методи і засоби підвищення ефективності ідентифікації користувачів розподілених систем. Автореферат дисертації на здобуття наукового ступеня кандидата технічних наук, спеціальність 05.13.05 – Комп'ютерні системи та компоненти, Київ – 2017. – К.: КПІ. 2017. – 23 с.

33. Карпанасюк В.В., Пасічник О.А. Інформаційна технологія ідентифікації користувачів. Тези доп. XI Міжнародної науково-практичної конференції «EURASIAN SCIENTIFIC CONGRESS», 1-3 листопада 2020 р. - Барселона, Іспанія, 2020. – С. 216 – 222.

ДОДАТКИ

Додаток А

Лістинг

Ident.py

```
from math import *
from random import *
from enum import *
import time
import eulerlib
import datetime
from Crypto.Cipher import PKCS1_OAEP
from Crypto.PublicKey import RSA


# p = 2 ** 1024
# modulo = 2 ** 1023 - 1
# m = 1373

def isPrime(a):
    return not ( a < 2 or any(a % i == 0 for i in range(2, int(a ** 0.5) +
1)))

def phi(n):
    y = 1
    for i in range(2,n+1):
        if isPrime(i) is True and n % i  == 0 is True:
            y = y * (1 - 1/i)
        else:
            continue
    return int(y)

def mod(a, b):
    val = a
    residio = b
    alength = a.bit_length()
    # print('a_length',alength)
    mlength = b.bit_length()
    # print('mod_length',mlength)

    if (alength < mlength):
        return a

    difference = alength - mlength

    # if(difference == 0):
    #     return a ^ m
```

```
    residio = residio << difference
    mask = 2 ** (alength - 1)
    offset = 0

    val = val ^ residio

    for i in range(difference):
        mask = mask >> 1
        offset += 1
        if mask & val:
            residio = residio >> offset
            val = val ^ residio
            offset = 0
    return val


def mul(a, b):
    res = 0
    tmp = a

    if a == b:
        n = a.bit_length() - 1
        res = 2 ** (2 * n)

        for j in range(n):
            mask = 2 ** (n - j - 1)
            if mask & a:
                mask = mask << mask.bit_length() - 1
                res = res ^ mask
        return res

    b = b
    for i in range(b.bit_length()):
        if b & 1:
            res = res ^ tmp
        tmp = tmp << 1
        b = b >> 1
    return res


def exp(A, e, m):
    r = 1
    mask = 2 ** (e.bit_length() - 1)

    for i in range(e.bit_length()):
        r = mod(mul(r, r), m)
        if e & mask:
            r = mod(mul(A, r), m)
        mask >>= 1
```

```
    return r
```

Клас Signal

```
class Signal(Enum):
    IDENT_REQUEST = 1
    REG_REQUEST = 2
    USR_SYST = 3
    SYST_USR = 4
    MSG = 5
    SEND_KEY = 6
    SEND_ENCRYPTED_MOD = 7
    REG_ACK = 8
    IDENT_ACK = 9
    IDENT_RESPONSE = 10
    IDENT_PROCEED = 11
```

Клас System

```
class System:
    usr_mod = -1

    @classmethod
    def registrationRequest(cls):
        cls.forgekeys()
        DataTransferChanel.send(cls, Signal.SEND_KEY, cls.publickey)

    @classmethod
    def receiveEncMod(cls, msg):
        # cls.decrypt(msg)
        cls.usr_mod = msg
        DataTransferChanel.send(cls, Signal.REG_ACK)

    @classmethod
    def decrypt(cls, m):
        privatecipher = PKCS1_OAEP.new(cls.keys)
        cls.usr_mod = int(privatecipher.decrypt(m))
        print('system m', cls.usr_mod)

    # doesnt check the user instance
    @classmethod
    def identificationRequest(cls):
        if cls.usr_mod != -1:
            DataTransferChanel.send(cls, Signal.IDENT_PROCEED)

    @classmethod
    def receiveIdResponse(cls, msg):
        q = msg[0]
        R = msg[1]
        E = msg[2]
        cls.verify(q, R, E)
```

```
    @classmethod
    def verify(cls, q, R, E):
        po = exp(q, E, cls.usr_mod)
        print('po', po)
        nu = mod(mul(po, R), cls.usr_mod)
        print('nu', nu)
        if nu == q:
            DataTransferChanel.send(cls, Signal.IDENT_ACK)

    @classmethod
    def forgekeys(cls):
        cls.keys = RSA.generate(2048)
        cls.publickey = cls.keys.publickey()
        print(cls.publickey)
        cls.privatekey = cls.keys.export_key()
```

Клас User

```
class User:
    syst_inst = System()
    publickey = 0


    def __init__(self):
        pass

    @classmethod
    def initiate_registration(cls):
        print('Registration is initiated by user')
        DataTransferChanel.send(cls, Signal.REG_REQUEST)
        cls.compute_M()
        # msg = cls.encryptm(cls.m)
        msg = cls.m
        print('MODULO', msg)
        DataTransferChanel.send(cls, Signal.SEND_ENCRYPTED_MOD, msg)

    @classmethod
    def initiate_identification(cls):
        DataTransferChanel.send(cls, Signal.IDENT_REQUEST)
        msg = cls.id_compute()
        # print('msg', msg)
        DataTransferChanel.send(cls, Signal.IDENT_RESPONSE, msg)

    @classmethod
    def receiveKey(cls, msg):
        cls.publickey = msg
        print(cls.publickey)

    @classmethod
```

```
    def compute_M(cls):
        # prime_gen.millerRabin(1024)
        cls.v = cls.p.bit_length() - 1
        cls.d = cls.g.bit_length() - 1
        tmp = mul(cls.p, cls.g)
        print('mod', tmp)
        cls.m = tmp

    @classmethod
    def encryptm(cls, m):
        msg = bytes(str(m), "utf-8")
        pubcipher = PKCS1_OAEP.new(cls.publickey)
        ciphertext = pubcipher.encrypt(msg)

        return ciphertext

    @classmethod
    def id_compute(cls):
        k = randint(0, 2 ** cls.d)
        # k = 22
        q = mul(k, cls.p)
        U = randint(0, 2 ** cls.d)
        # U = 13
        R = exp(q, U, cls.m)
        E = 2 ** cls.d - U

        print('k', k)
        print('q', q)
        print('U', U)
        print('R', R)
        print('E', E)
        msg = [q, R, E]
        print('msg', msg)
        return msg
```

Клас DataTransferChanel

```
class DataTransferChanel:
    @classmethod
    def send(cls, sender, signal, msg=0):
        if sender == User:
            # print('User')

            if signal == Signal.REG_REQUEST:
                print('user requested registration')
                System.registrationRequest()
                # print(signal)
            elif signal == Signal.SEND_ENCRYPTED_MOD:
                # print(msg)
                System.receiveEncMod(msg)
```

```
            elif signal == Signal.IDENT_REQUEST:
                print('user requested identification')
                System.identificationRequest()
                # print(signal)
            elif signal == Signal.IDENT_RESPONSE:
                print('user sent q,R,E')
                print(msg)
                System.receiveIdResponse(msg)
        if sender == System:
            if signal == Signal.SEND_KEY:
                print('system sent a public key')
                User.receiveKey(msg)
                # print('System')
            elif signal == Signal.REG_ACK:
                print('registration completed')
            elif signal == Signal.IDENT_PROCEED:
                print('identification proceeds')
            elif signal == Signal.IDENT_ACK:
                print('identification completed')


def run():
    # registration protocol
    p_digit = 2 ** 1000 + 2 ** 14 + 2 ** 11 + 2 ** 8 + 2 ** 6 + 3
    # p_digit =
1000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000237
    g_digit = 2 ** 1024 + 2 ** 13 + 2 ** 9 + 2 ** 7 + 2 ** 6 + 2 ** 5 + 2 **
4 + 2 ** 3 + 1
    # g_digit =
3130000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000001
1838110000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000
00313
    p_digit = 19
    g_digit = 131
    d = g_digit.bit_length() - 1
    v = p_digit.bit_length() - 1
    m = mul(p_digit, g_digit)
    print('m', m)
    # k = randint(0, 2 ** d)
    k = 18
    print('k', k)
    q_digit = mul(k, p_digit)
    print('q', q_digit)
    U = randint(1, 2 ** d)
    U = 60
```

```
    print('U', U)
    R = exp(q_digit, U, m)
    print('R', R)
    E = 2 ** d - U
    print('E', E)

    po = exp(q_digit, E, m)
    nu = mod(mul(po, R), m)
    print('po', po)
    print('nu', nu)


def modular_exp(A, E, m):
    tmp = A
    for i in range(E):
        tmp = tmp * A
        tmp %= m
    return tmp


def findPar(mu, mod):
    B = randint(1, mod)
    v = 2
    for i in range(B,mod):
        print(i)
        for j in range(int(mod/2)):
            res = (mu * (i ** j)) % mod
            if res == 1:
                v = j
                B = i
                print('found')
                return v, B
    return False


def gq():
    p = 1217
    q = 997
    m = p * q
    ph = phi(m)
    e = randint(1, ph)

    for i in range(ph):
        if i * e % m == 1:
            s = i
            break

    print('m', m)
    mu = randint(1, m)
    ar = findPar(mu, m)
```

```
    while not ar:
        mu = randint(1, m)

        ar = findPar(mu, m)
    print('mu', mu)
    v, B = ar
    print('B', B)
    print('v', v)
    print(mu * (B ** v) % m)
    r = randint(1, m)
    P = (r ** v) % m
    d = randint(1, m)
    G = (r * (B ** d)) % m
    Q = ((G ** v) * (mu ** d)) % m
    print(Q == P)


def compute_exp(step):
    A = 10 ** 143 + 3 ** 4
    E = 200
    a = 10 ** 143 + 3 ** 4
    b = 10 ** 303 + 237
    m = mul(a, b)

    for i in range(step):
        tmp1 = 10 ** int((i / 2))
        tmp2 = 5 ** (i & 1)
        P = E * tmp1 * tmp2
        print(P)
        t = time.time()
        modular_exp(A, P, m)
        # print('modular', time.time() - t)
        print(time.time() - t)
        t = time.time()
        exp(A, P, m)
        # print('polynomial',  time.time() - t)
        print(time.time() - t)


# compute_exp(20)
# print(bin(mul(19,30)))
# print(mul(15,87))
# run()
t = time.time()
# user = User()
# user.initiate_registration()
# user.initiate_identification()
print(time.time() - t)
t = time.time()
gq()
```

```
print(time.time() - t)
```

Prime_gen.py

```
import random
import math
import sys

def rabinMiller(n):
     s = n-1
     t = 0
     while int(s) &  1 == 0:
         s = s/2
         t +=1
     k = 0
     while k<128:
         a = random.randrange(2,n-1)
         v = pow(a,s,n) #where values are (num,exp,mod)
         if v != 1:
             i=0
             while v != (n-1):
                 if i == t-1:
                     return False
                 else:
                     i = i+1
                     v = (v**2)%n
         k+=2
     return True

def isPrime(n):
     lowPrimes =
[3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97

,101,103,107,109,113,127,131,137,139,149,151,157,163,167,173,179

,181,191,193,197,199,211,223,227,229,233,239,241,251,257,263,269

,271,277,281,283,293,307,311,313,317,331,337,347,349,353,359,367

,373,379,383,389,397,401,409,419,421,431,433,439,443,449,457,461

,463,467,479,487,491,499,503,509,521,523,541,547,557,563,569,571

,577,587,593,599,601,607,613,617,619,631,641,643,647,653,659,661

,673,677,683,691,701,709,719,727,733,739,743,751,757,761,769,773

,787,797,809,811,821,823,827,829,839,853,857,859,863,877,881,883
```

```
,887,907,911,919,929,937,941,947,953,967,971,977,983,991,997]
     if (n >= 3):
         if (n&1 != 0):
             for p in lowPrimes:
                 if (n == p):
                    return True
                 if (n % p == 0):
                     return False
             return rabinMiller(n)
     return False

def generateLargePrime(k):
     #k is the desired bit length
     r=100*(math.log(k,2)+1) #number of attempts max
     r_ = r
     while r>0:
        #randrange is mersenne twister and is completely deterministic
        #unusable for serious crypto purposes
         n = random.randrange(2**(k-1),2**(k))
         r-=1
         if isPrime(n) == True:
             return n
     return "Failure after "+'r_' + " tries."

#print(generateLargePrime(1024))
```

RSA.py

```
import random
import time

def decrypt(F, d):
    if d == 0:
        return 1
    if d == 1:
        return F
    w, r = divmod(d, 2)
    if r == 1:
        return decrypt(F * F % n, w) * F % n
    else:
        return decrypt(F * F % n, w)


def correct():
    for i in range(len(C)):
        if len(str(P[i])) % 2 != 0:
            y = str(0) + str(P[i])
            P.remove(str(P[i]))
            P.insert(i, y)
```

```
def cipher(b, e):
    if e == 0:
        return 1
    if e == 1:
        return b
    w, r = divmod(e, 2)
    if r == 1:
        return cipher(b * b % n, w) * b % n
    else:
        return cipher(b * b % n, w)


def group(j, h, z):
    for i in range(int(j)):
        y = 0
        for n in range(h):
            y += int(numP[(h * i) + n]) * (10 ** (z - 2 * n))
        X.append(int(y))


def gcd(a, b):
    while b != 0:
        (a, b) = (b, a % b)
    return a


letter = ["a", "b", "c", "d", "e", "f", "g", "h", "i", "j", "k", "l", "m",
"n", "o", "p", "q",
          "r", "s", "t", "u", "v", "w", "x", "y", "z", ",", ".", "!", "?", "
"]
number = ["01", "02", "03", "04", "05", "06", "07", "08", "09", "10", "11",
"12", "13",
          "14", "15", "16", "17", "18", "19", "20", "21", "22", "23", "24",
"25", "26", "27",
          "28", "29", "30", "31"]

print('\n')


def Decrypt():
    # decrypts an encoded message
    global m, P, C, x, h, p, Text, y, w
    P = []
    C = str(input("Enter ciphertext blocks:"))
    C = C.lstrip('[')
    C = C.rstrip(']')
    C = C.split(',')
    for i in range(len(C)):
```

```
        x = decrypt(int(C[i]), d)
        P.append(str(x))
    correct()
    # print(P)
    h = len(P[0])
    p = []
    for i in range(len(C)):
        for n in range(int(h / 2)):
            p.append(str(P[i][(2 * n):((2 * n) + 2)]))

    Text = []
    for i in range(len(p)):
        for j in range(len(letter)):
            if str(p[i]) == number[j]:
                Text.append(letter[j])
    PText = str()
    for i in range(len(Text)):
        PText = PText + str(Text[i])
    print("Plaintext is:", PText)


def Encrypt():
    # encrypts a plaintext message using the current key
    global plaintext, numP, q, j, z, X, C
    plaintext = (input("Enter Plaintext :"))
    plaintext = plaintext.lower()
    numP = []
    for i in range(len(plaintext)):
        for j in range(len(letter)):
            if plaintext[i] == letter[j]:
                numP.append(number[j])
    h = (len(str(n)) // 2) - 1
    q = len(numP) % h
    for i in range(h - q):
        numP.append(number[random.randint(0, 25)])
    j = len(numP) / h
    # print(numP)
    X = []
    z = 0
    for m in range(h - 1):
        z += 2
    group(j, h, z)
    k = len(X)
    C = []
    for i in range(k):
        b = X[i]
        r = cipher(b, e)
        C.append(r)
    print("Ciphertext:", C)
    print("Number of Ciphertext blocks:", len(C))
```

```
def setup():
    global n, e, d
    while True:
        try:
            n = int(input(" Enter a value for n :"))
            if n > 2:
                break
        except ValueError:
            print('please enter a number')
    while 1 != 2:
        try:
            e = int(input(" Enter a value for e :"))
            if e >= 2:
                break
        except ValueError:
            print('please enter a number')
    while True:
        try:
            if d >= 0:
                break
        except ValueError:
            print('please enter a number')


# setup()
n = 2537
e = 13
d = 937


mm = str()
while mm != 'quit':
    mm = input("Enter Command...")
    if mm.lower() == 'encrypt':
        Encrypt()
    elif mm.lower() == 'decrypt':
        Decrypt()
    elif mm.lower() == 'n':
        try:
            print('current n = ', n)
            n = int(input(" Enter a value for n :"))
        except ValueError:
            print('That is not a valid entry')
    elif mm.lower() == 'help':
        print("To redefine n,e, or d, type 'n','e',... etc.")
        print("To encrypt a message with the current key, type 'Encrypt'")
        print("To decrypt a message with the current key, type 'Decrypt'")
        print("Type quit to exit")
```

```
    print('\n')
    print('\n')
elif mm.lower() == 'e':
    try:
        print('current e = ', e)
        e = int(input(" Enter a value for e :"))
    except ValueError:
        print('That is not a valid entry')
elif mm.lower() == 'd':
    try:
        print('current d = ', d)
        d = int(input(" Enter a value for d :"))
    except ValueError:
        print('That is not a valid entry')
else:
        print(statements[ii])
```

CERTIFICATE

is awarded to

Karpanasiuk Viktor

for being an active participant in
XI International Scientific and Practical Conference

"EURASIAN SCIENTIFIC CONGRESS"

24 Hours of Participation

BARCELONA

1-3 November 2020

sci-conf.com.ua

SCI-CONF.COM.UA

EURASIAN SCIENTIFIC CONGRESS

ABSTRACTS OF XI INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE NOVEMBER 1-3, 2020

BARCELONA 2020

EURASIAN SCIENTIFIC CONGRESS

Abstracts of XI International Scientific and Practical Conference

Barcelona, Spain

1-3 November 2020

Barcelona, Spain

2020

UDC 001.1

The 11th International scientific and practical conference "Eurasian scientific congress" (November 1-3, 2020) Barca Academy Publishing, Barcelona, Spain. 2020. 613 p.

ISBN 978-84-15927-31-0

The recommended citation for this publication is:
Ivanov I. Analysis of the phaunistic composition of Ukraine // Eurasian scientific congress. Abstracts of the 11th International scientific and practical conference. Barca Academy Publishing. Barcelona, Spain. 2020. Pp. 21-27. URL: https://sci-conf.com.ua/xi-mezhdunarodnaya-nauchno-prakticheskaya-konferentsiya-eurasian-scientific-congress-1-3-noyabrya-2020-goda-barselona-ispaniya-arhiv/.

Editor
Komarytskyy M.L.
Ph.D. in Economics, Associate Professor

Collection of scientific articles published is the scientific and practical publication, which contains scientific articles of students, graduate students, Candidates and Doctors of Sciences, research workers and practitioners from Europe, Ukraine, Russia and from neighbouring coutries and beyond. The articles contain the study, reflecting the processes and changes in the structure of modern science. The collection of scientific articles is for students, postgraduate students, doctoral candidates, teachers, researchers, practitioners and people interested in the trends of modern science development.

e-mail: barca@sci-conf.com.ua

homepage: *https://sci-conf.com.ua*

TABLE OF CONTENTS

AGRICULTURAL SCIENCES

BIOLOGICAL SCIENCES

MEDICAL SCIENCES

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

Карпанасюк Віктор Володимирович
Магістр
Пасічник Олександр Анатолійович
к.т.н., доцент
Хмельницький національний університет
м. Хмельницький, Україна

Вступ./Introductions. Основною рушійною силою технологічного прогресу людства в останні десятиліття є активна інтеграція інформаційних систем та утворення інформаційного простору, в якому надається доступ до великих обсягів приватної та конфіденційної інформації як до підґрунтя прийняття оптимальних рішень. Використання таких систем може бути доцільним та раціональним лише за умови ефективного вирішенням питання ідентифікації віддалених користувачів.

Мета роботи./Aim. Мета роботи полягає у розробці інформаційної технології, яка буде надійно захищати різноманітні системи від протиправного доступу шляхом ідентифікації користувачів на основі криптографічної концепції нульових знань.

Матеріали и методы./Materials and methods. Базовою складовою будь-яких інформаційних систем є модулі захисту, які виконують ідентифікацію користувачів, оскільки всі механізми захисту інформації розраховані на роботу з пойменованими суб'єктами і об'єктами систем. Слід зазначити, що як суб'єкти систем можуть виступати як користувачі, так і процеси, а я об'єкти - інформація та інші інформаційні ресурси системи.

Присвоєння суб'єктам і об'єктам доступу особистого ідентифікатора і порівняння його з заданим переліком називається ідентифікацією.

Ідентифікація забезпечує виконання таких функцій:

- встановлення автентичності та визначення повноважень суб'єкта при

його допуску в систему;

- контроль встановлених повноважень в процесі сеансу роботи;

- реєстрація дій тощо.

Одними з найпоширеніших технологій ідентифікації користувачів є технології, засновані на знанні особою, яка має право на доступ до ресурсів системи, деякою секретної інформації, наприклад, пароля. Такі методи ідентифікації є найбільш поширеними, простими і звичними. Парольні методи класифікують за ступенем частоти змінюваності паролів на методи з постійними (багаторазовими) або динамічно змінюваними (одноразовими) паролями.

У більшості систем використовуються багаторазові паролі, хоча більш надійним є спосіб з використанням одноразових або динамічно змінюваних паролів. Існують такі методи парольного захисту, засновані на одноразових паролів: - методи модифікації схеми простих паролів; - методи «запит-відповідь»;

До методів модифікації схеми простих паролів відносять випадкову вибірку символів пароля і одноразове використання паролів.

При використанні методу модифікації простих паролів, кожному користувачеві виділяється досить довгий пароль, причому щоразу для ідентифікації використовується не весь пароль, а тільки його деяка частина. У процесі перевірки автентичності система запитує у користувача групу символів під заданим порядковим номерам. Кількість символів і їх порядкові номери для запиту визначаються за допомогою датчика псевдовипадкових чисел.

При одноразовому використанні паролів кожному користувачеві виділяється список паролів. В процесі запиту номер пароля, який необхідно ввести, вибирається послідовно за списком або по схемі випадкової вибірки.

Недоліком методів модифікації схеми простих паролів є необхідність запам'ятовування користувачами довгі паролі або їх списки. Запис же паролів на папір або в записники призводить до появи ризику втрати або розкрадання носіїв інформації з записаними на них паролями.

При використанні методу «запит-відповідь» система задає користувачеві деякі питання загального характеру, правильні відповіді на які відомі тільки конкретного користувача.

Відзначимо, що методи ідентифікації, засновані на одноразових паролях, також не забезпечують абсолютного захисту. До прикладу, якщо зловмисник має можливість підключення до мережі і перехоплювати передані пакети, то він може посилати останні як власні.

Базовими критеріями ефективності будь-якої системи захисту є рівень захищеності при її використанні та обсяг ресурсів для реалізації функцій захисту. Складність проблеми визначається неможливістю побудови адекватної формальної моделі дій сторони, яка намагається реалізувати незаконний доступ до ресурсів системи.

Всі сучасні протоколи ідентифікації абонентів розділяють на два класи:

- з використанням паролів, що перевіряються системою шляхом порівняння (“слабка” ідентифікація),

- на основі концепції “нульових знань” (“сурова” ідентифікація).

Сутність концепції “нульових знань” полягає в тому, що для доведення своєї ідентичності абонент має неявним чином виявити знання певної інформації, якою система не володіє, але може перевірити її наявність у абонента. При цьому в системі не зберігається жодних секретних даних, які б дозволили б відновити ідентифікаційні дані абонента "нульових знань”. Під час кожного зверненні до системи генерується нова ідентифікуюча інформація. Таким чином, концепція “нульових знань” найбільш повною мірою задовольняє вимогам забезпечення високого рівня захищеності від спроб несанкціонованого доступу.

Концепція “нульових знань” ґрунтується на використанні незворотних математичних перетворень. В більшості існуючих схем строгої ідентифікації як такі перетвореньня використовуються аналітично нерозв’язувані задачі теорії чисел, зокрема відома задача дискретного логарифмування. Найбільш відомими з схем ідентифікації цього класу є FFSIS (Feige Fiat Shamir Identification

Scheme), методи Шнора (Schnorr) та Гіллоу-Квіскатера (Guillou- Quisquater).

Важливою передумовою взаємодії віддалених користувачів та інформаційних систем є наявність ефективних механізмів контролю доступу до інформаційних ресурсів. Як основа існуючих методів ідентифікації використовуються операції модулярної арифметики з числами розрядність яких значно перевищує розрядність процесорів й, відповідно, потребують суттєвих обчислювальних витрат.

Розширення спектру та обсягів інформації широкого кола користувачів, що зберігається у цифровому форматі, обумовлює об'єктивну зацікавленість певних «недоброзичливців» в отриманні доступу до неї в обхід законних процедур. Разом із тим, система ідентифікації не повинна створювати незручності, зокрема, збільшення часу очікування для отримання доступу, для доброчесних користувачів.

Таким чином, розробка нових підходів до підвищення швидкості програмної та апаратної реалізації базових обчислювальних процедур в методах ідентифікації є актуальною проблемою. Для її вирішення пропонується як основа для обчислювальних процедур методів ідентифікації, використовувати алгебру кінцевих полів Галуа з реалізація операції експоненціювання.

Для ефективної організації експоненціювання на кінцевих полях важливе значення має специфічна властивість поліноміального квадрату, а саме - двійкові розряди поліноміального квадрату числа А, що знаходяться на парних позиціях дорівнюють нулю, в той час, як розряди з непарними номерами співпадають з двійковими розрядами числа А, тобто, якщо $A=a_0+a_1\cdot 2+a_2\cdot 2^2+...+a_{n-1}\cdot 2^{n-1}$, то $A\otimes A=A|^2 = a_0+a_1\cdot 2^2+a_2\cdot 2^4+...+a_{n-1}\cdot 2^{2\cdot n-2}$.

Поліноміальне представлення числа A має вигляд $P(A) = a_{n-1}\cdot x^{n-1} + a_{n-2}\cdot x^{n-2} + ... + a_1\cdot x + a_0$. Відповідно, поліноміальне представлення квадрату $A\otimes A$ числа А має наступний вигляд: $P(A\otimes A) = b_{2\cdot n-2}\cdot x^{2\cdot n-2} + b_{2\cdot n-3}\cdot x^{2\cdot n-3} + ... + b_3\cdot x^3 + b_2\cdot x^2 + b_1\cdot x + b_0$. Кожен коефіцієнт $b_l \in\{0,1\}$, де $l\in\{0,1,...,2\cdot n-2\}$ поліноміального представлення квадрату $P(A\otimes A)$ дорівнює сумі попарних добутків коефіцієнтів $a_q\cdot a_g$ таких, що арифметична сума їх індексів дорівнює l: $q+g=l$; наприклад, $b_0 =$

$a_0 \cdot a_0$, $b_1 = a_1 \cdot a_0 + a_0 \cdot a_1$ $b_1 = a_2 \cdot a_0 + a_0 \cdot a_2 + a_1 \cdot a_1$. Очевидно, якщо $g \neq q$, то до складу вказаної суми входять обидва коефіцієнти $a_q \cdot a_g$ та $a_g \cdot a_q$, а якщо $g = q$, то лише один: $a_q \cdot a_g$. Оскільки $a_q \cdot a_g = a_g \cdot a_q$ то, в алгебрі кінцевих полів вони при додаванні взаємно компенсуються. Тобто, для непарних значень l коефіцієнт $b_l = 0$, а для парних значень l коефіцієнт $b_l = a_{l/2} \cdot a_{l/2} = a_{l/2}$, тобто $b_0 = a_0$, $b_1 = 0$, $b_2 = a_1$, $b_3 = 0$, $b_4 = a_3, \ldots, b_{2 \cdot n-2} = a_{n-1}$. Таким чином, поліноміальне представлення квадрату $A \otimes A$ може бути трансформовано до вигляду:

$$P(A \otimes A) = a_{n-1} \cdot x^{2 \cdot n-2} + a_{n-2} \cdot x^{2 \cdot n-4} + \ldots + a_1 \cdot x^2 + a_0.$$

Ґрунтуючись на властивостях поліноміального квадрату та використані передобчислень може бути реалізовано спосіб прискореного експоненціювання на кінцевих полях. Процедура експоненціювання складається з n циклів послідовного аналізу розрядів експоненти, починаючи зі старшого. Якщо поточний біт експоненти дорівнює одиниці, то виконуються обчислення $R \otimes R \otimes A$ rem M. Якщо $r_0, r_1, \ldots, r_{n-1}$ - двійкові розряди R, тобто $R = r_0 + r_1 \cdot 2 + r_2 \cdot 2^2 + \ldots + r_{n-1} \cdot 2^{n-1}$, де $\forall j \in \{0,1,\ldots,n-1\}$ $r_j \in \{0,1\}$, то згідно (2.1) $R \otimes R = r_{n-1} \cdot 2^{2 \cdot n-2} + r_{n-2} \cdot 2^{2 \cdot n-4} + \ldots + r_1 \cdot 2^2 + r_0$. Якщо вважати, що A - множиме, а $P(R \otimes R)$ - множник, то поліноміальний добуток $R|^2 \otimes A$ можна представити у вигляді суми добутків коду А на компоненти квадрату $R|^2$: $R|^2 \otimes A = A \cdot (r_{n-1} \cdot 2^{2 \cdot n-2} + r_{n-2} \cdot 2^{2 \cdot n-4} + \ldots + r_1 \cdot 2^2 + r_0) = A \cdot r_0 \oplus A \cdot 2^2 \cdot r_1 \oplus A \cdot 2^4 \cdot r_2 \oplus \ldots \oplus A \cdot 2^{2 \cdot n-4} \cdot r_{n-2} \oplus A \cdot 2^{2 \cdot n-2} \cdot r_{n-1})$. Залишок від поліноміального ділення $(R|^2 \otimes A)$ rem M відповідно дорівнює: $(R|^2 \otimes A)$ rem $M = (A \cdot r_0 \oplus A \cdot 2^2 \cdot r_1 \oplus A \cdot 2^4 \cdot r_2 \oplus \ldots \oplus A \cdot 2^{2 \cdot n-4} \cdot r_{n-2} \oplus A \cdot 2^{2 \cdot n-2} \cdot r_{n-1})$ rem $M = A \cdot r_0 \oplus (A \cdot 2^2)$ rem $M \cdot r_1 \oplus (A \cdot 2^4)$ rem $M \cdot r_2 \oplus \ldots \oplus (A \cdot 2^{2 \cdot n-4})$ rem $M \cdot r_{n-2} \oplus (A \cdot 2^{2 \cdot n-2})$ rem $M \cdot r_{n-1}$. Очевидно, що значення $A \cdot 2^2$ rem M , $A \cdot 2^4$ rem M, ..., $A \cdot 2^{2 \cdot n-4}$ rem M, $A \cdot 2^{2 \cdot n-2}$ rem M можуть бути обчислені перед експоненціюванням і збережені в таблиці: T[0]=A, T[1]= $A \cdot 2^2$ rem M, T[2]= $A \cdot 2^4$ rem M,..., T[n-2]= $A \cdot 2^{2 \cdot n-4}$ rem M, T[n-1]= $A \cdot 2^{2 \cdot n-2}$ rem M. Відповідно, обчислення організуються згідно з наступного виразу: $(R|^2 \otimes A)$ rem M = T[0]$\cdot r_0 \oplus$ T[1]$\cdot r_1 \oplus$ T[2]$\cdot r_2 \oplus \ldots \oplus$ T[n-2]$\cdot r_{n-2} \oplus$ T[n-1]$\cdot r_{n-1}$. Аналогічно, якщо поточний біт експоненти дорівнює нулю, то реалізується лише піднесення до квадрату: $R \otimes R$ rem M. У відповідності з (2.1) $R \otimes R = r_{n-1} \cdot 2^{2 \cdot n-2} + r_{n-2} \cdot 2^{2 \cdot n-4} + \ldots +$

$r_1 \cdot 2^2 + r_0$. Залишок від поліноміального ділення $R|^2$ rem M відповідно в цьому випадку дорівнює: $R|^2$ rem $M = (r_0 \oplus 2^2 \cdot r_1 \oplus 2^4 \cdot r_2 \oplus ... \oplus 2^{2 \cdot n-4} \cdot r_{n-2} \oplus 2^{2 \cdot n-2} \cdot r_{n-1})$ rem $M = r_0 \oplus 2^2 \cdot r_1 \oplus 2^4 \cdot r_2 \oplus ... \oplus 2^{n-2} \cdot r_{n/2-1} \oplus 2^n$ rem $M \cdot r_{n/2} \oplus ... \oplus 2^{2 \cdot n-2}$ rem $M \cdot r_{n-1}$. Чисельні значення 2^n rem M , 2^{n+2} rem M, ..., $2^{2 \cdot n-4}$ rem M, $2^{2 \cdot n-2}$ rem M можуть бути обчислені перед експоненціюванням і збережені в таблиці W : W[0]= 2^n rem M, W[1]= 2^{n+2} rem M , W[2]=2^{n+4} rem M,..., W[n/2-2]= $2^{2 \cdot n-4}$ rem M, W[n/2-1]= $2^{2 \cdot n-2}$ rem M. З урахуванням наведеного, обчислення $R|^2$ rem M організується в наступному вигляді : $R|^2$ rem M = = $r_0 \oplus 2^2 \cdot r_1 \oplus 2^4 \cdot r_2 \oplus ... \oplus 2^{n-2} \cdot r_{n/2-1} \oplus$ W[0]$\cdot r_{n/2} \oplus$ W[1]$\cdot r_{n/2+1} \oplus ... \oplus$ W[n/2-2]$\cdot r_{n-2} \oplus$ W[n/2-1]$\cdot r_{n-1}$.

Таким чином, для обчислення $A|^E$ rem M на кінцевих полях попередньо виконується формування двох таблиць W та T. Таблиця W не залежить від A, і необхідність її попереднього формування визначається зміною M - числа, що співвідноситься з утворюючим поліномом кінцевого поля. Формування таблиці W виконується у відповідності з алгоритмом: 1. W[0] = 2^n rem M; i = 0; 2. W[i] = 2·W[i-1] rem M, i=i+1; 3. Якщо $i < n/2$, повернення на п.2. Таблиця T заповнюється перед початком обчислення $A|^E$ rem M згідно з наступним алгоритмом: 1. T[0] = A; j = 0; 2. T[j] = 2·T[j-1] rem M, j = j+1; 3. Якщо $j<n$, повернення на п.2.

Процес експоненціювання організовується у вигляді циклу, що повторюється n раз: 1. R=1; j =n-1; 2. Якщо e_j=0 виконання пп. 2.1.-2.5. 2.1. i=0 ; D = 1; S=0; 2.2. Якщо r_i =0, перехід на п. 2.4. 2.3. Якщо $i < n/2$, то S=S+D, інакше S=S+W[i-n/2]. 2.4. D=D ·2; i = i + 1; 2.5. Якщо $i < n$, повернення на п. 2.2., інакше перехід на п. 4. 3. Якщо e_j=1 виконання пп. 3.1.-3.5. 3.1. i=0 ; S=0; 3.2. Якщо r_i =0, перехід на п. 3.4. 3.3. $S = S +$ T[i]; 3.4. $i = i + 1$; 3.5. Якщо $i < n$, повернення на п. 3.2. 4. $j = j - 1$; якщо $j \geq 0$, то повернення на п. 2

Наведена процедура експоненціювання на скінчених полях Галуа може бути прямо використана для прискореної ідентифікації користувачів.

Реалізована інформаційна технологія включає такі структурні модулі:

1. модуль для знаходження простих поліномів

2. модуль для шифрування повідомлень
3. модуль з реалізацією методу ідентифікації

Проведений аналіз ефективності методу шляхом порівняння часу виконання процедури експоненціювання в різних математичних базисах. Отримані результати свідчать, що швидкість ідентифікації при використанні запропонованого методу зростає на декілька порядків, в порівнянні з відомими методами, що є суттєвим показником

Результати та обговорення./Results and discussion. Запропоновано метод строгої ідентифікації користувачів з використанням незворотних перетворень на полях Галуа, який включає в себе процедуру реєстрації користувача в системі та процедуру одного сеансу ідентифікації. Розроблено метод прискореної строгої ідентифікації користувачів розподілених систем на основі незворотних перетворень алгебри полів Галуа, і який використовує встановлені властивості локальних циклів експоненціювання на полях Галуа, утворюючий поліном яких є добутоком двох простих поліномів.

Висновки./Conclusions. Реалізовано інформаційну технологію ідентифікації користувачів яка ґрунтується на локальних циклах утворюваних при виконанні експоненціювання на полях Галуа на основі методу суворої ідентифікації користувачів з використанням незворотних перетворень на полях Галуа, який включає в себе процедуру реєстрації користувача в системі та процедуру одного сеансу ідентифікації.

ДИПЛОМНА РОБОТА МАГІСТРА

Інформаційна технологія ідентифікації користувачів

Студент гр. *КНм-19-1* *В.В. Карпанасюк*

Керівник *О.А. Пасічник*

Актуальність теми

- Загальносвітовим трендом технічного та технологічного прогресу людства в останні десятиліття є активна інтеграція інформаційних систем. Утворений внаслідок цього процесу інформаційний простір надає можливість використовувати великі обсяги інформації задля вирішення широкого кола питань, завдань та проблем й задоволення найрізноманітніших потреб. Отримуваний результат визначається широким спектром різнопланових чинників, у тому числі і суб'єктивних. Суб'єктивізм у цих питаннях пов'язаний з двома головними аспектами. По-перше, це належні виконавці, а по-друге, відповідні вигідоотримувачі. Обидва ці аспекти об'єднує питання розподілу прав доступу, яке, у свою чергу, об'єктивно та обов'язково включає задачу ідентифікації віддалених користувачів.

Мета і задачі робити

Мета роботи полягає у реалізація інформаційної технології ідентифікації користувачів на основі концепції «нульових знань» з достатнім рівнем обчислювальної здатності.

Для досягнення поставленої мети визначені наступні задачі дослідження:

- - провести аналіз існуючих методів, технологій та рішень методів ідентифікації користувачів, що реалізують концепцію «нульових знань»;
- - удосконалення існуючих методів ідентифікації у напрямку покращення обчислювальної здатності;
- - розробити інформаційну технологію ідентифікації користувачів за допомогою отриманих моделей та методів;
- - виконати експериментальну перевірку інформаційної технології ідентифікації користувачів.

Об’єкт дослідження – процес ідентифікації користувачів з використанням інформаційних технологій.

Предмет дослідження – моделі, методи, підходи та засоби інформаційної технології ідентифікації користувачів.

Наукова новизна одержаних результатів

- - удосконалено існуючі методи ідентифікації у напрямку покращення обчислювальної здатності;
- - встановлено межі використання поліноміальної арифметики у порівнянні з модулярною в залежності від значення експоненти в частині покращення обчислювальної складності при ідентифікації користувачів.

Практичне значення одержаних результатів

- У результаті виконання дипломної роботи магістра за інформаційною технологією розроблено відповідне експериментальне програмне забезпечення, яке підтвердило вірність запропонованих положень. Застосування інформаційної технології дає можливість ідентифікації віддалених користувачів із використанням концепції «нульових знань», яка унеможливлює розголошення персональних даних, а експоненціонування при використанні модулярної арифметики суттєво покращує обчислювальну складність.

Апробація результатів дипломної роботи

Основні наукові та практичні результати доповідалися на конференціях:

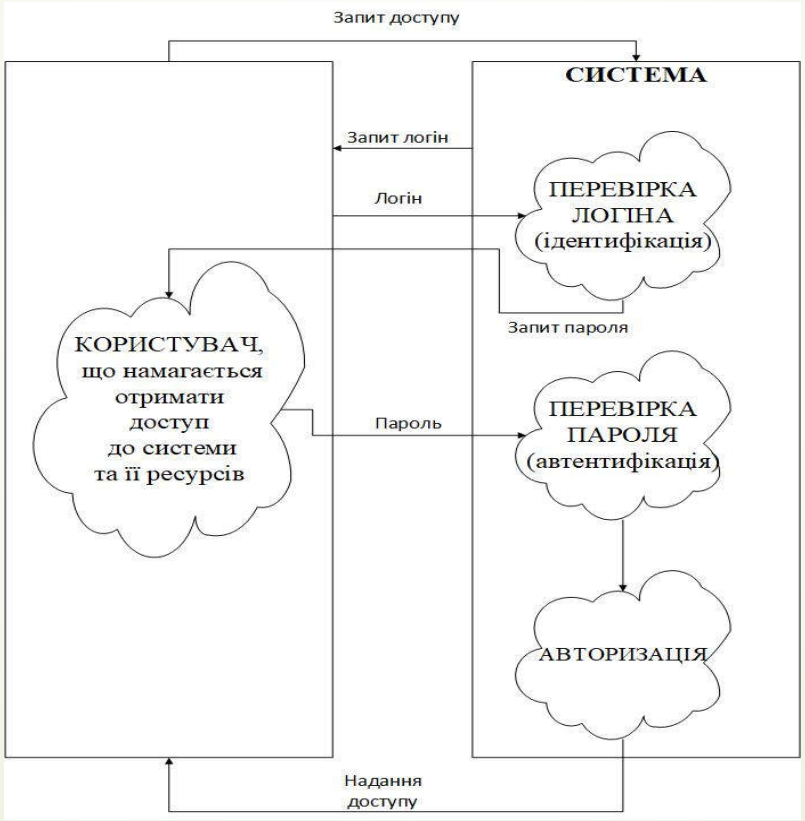
- - доповідь на тему «Інформаційна технологія ідентифікації користувачів» на XI Міжнародній науково-практичній конференції «Eurasian scientific congress», 1-3 листопада 2020 р., Барселона, Іспанія

За темою дипломної роботи магістра автором виконано одну наукову публікацію.

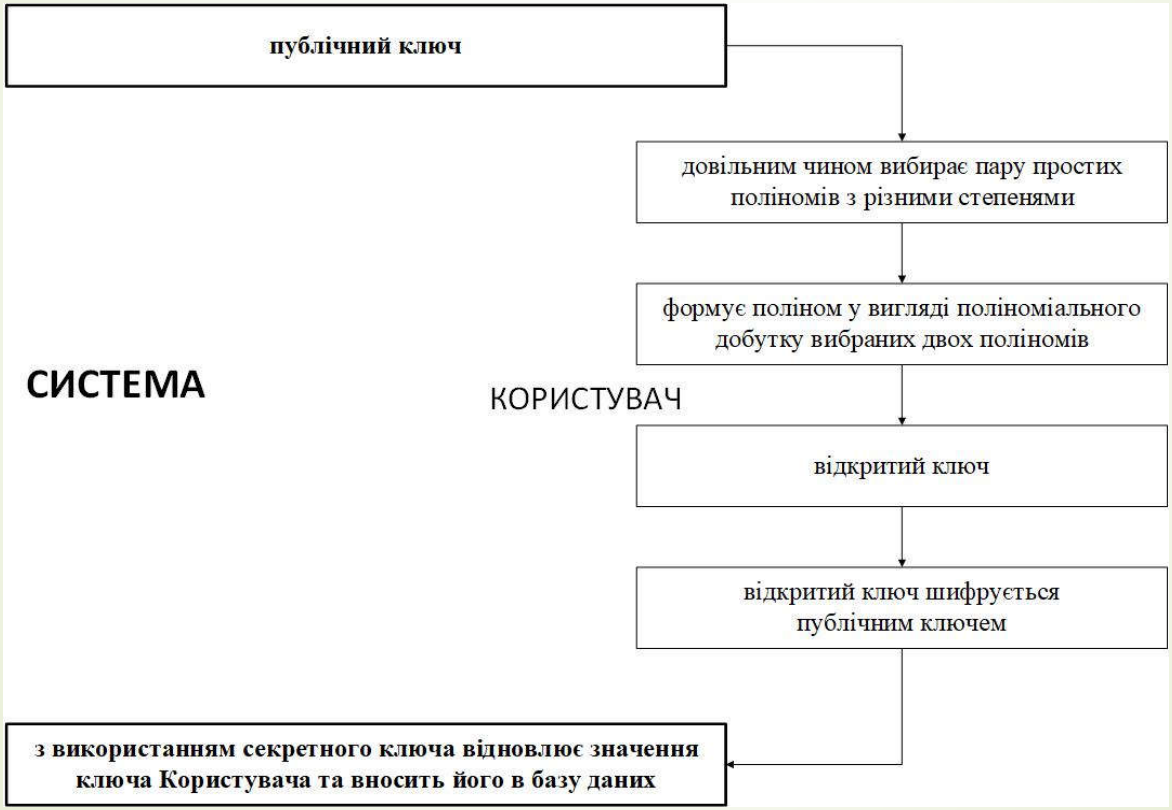
Аналіз сучасного стану технологій ідентифікації користувачів

- Створення єдиної, централізованої системи безпеки є необхідною умовою існування сучасної інформаційної інфраструктури, а управління доступом – ефективним методом захисту інформації, регулюючим використання ресурсів інформаційної системи, для якої розроблялася концепція інформаційної безпеки.
- На сьогоднішній десь існує велика кількість різноманітних технологій для ідентифікації користувачів, які умовно можна розділити на дві групи.
- До першої групи відносяться технології, що передбачають використання певної наперед визначеної інформації для ідентифікації користувача системою.
- До другої групи відносять технології, що передбачаються імплементацію концепції «нульових знань».

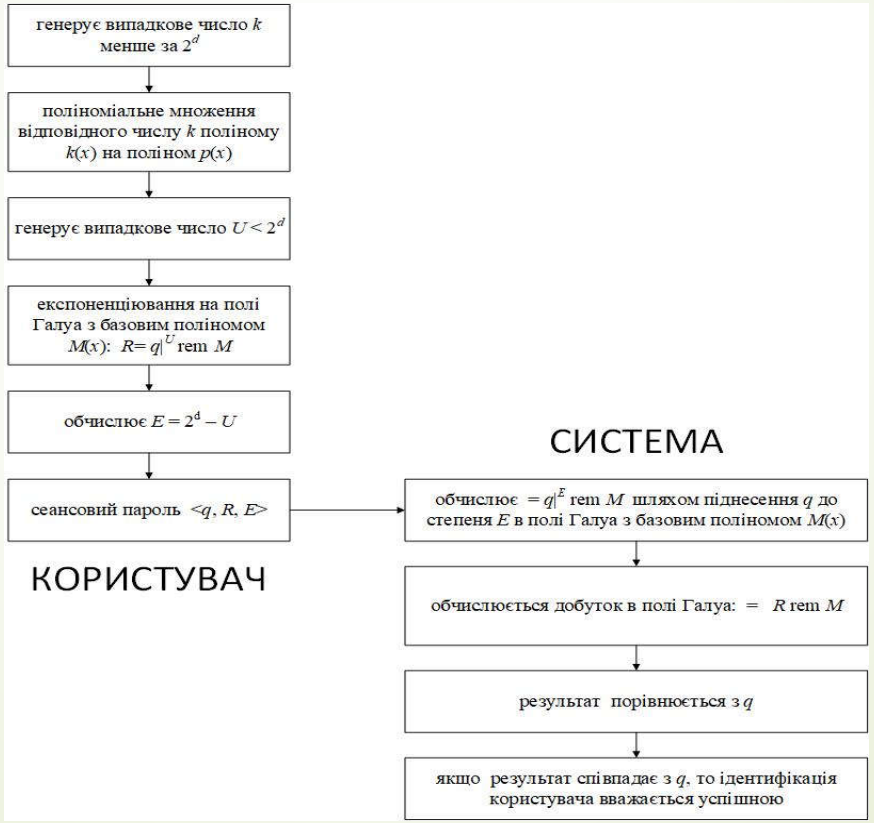
Розробка технології ідентифікації користувачів



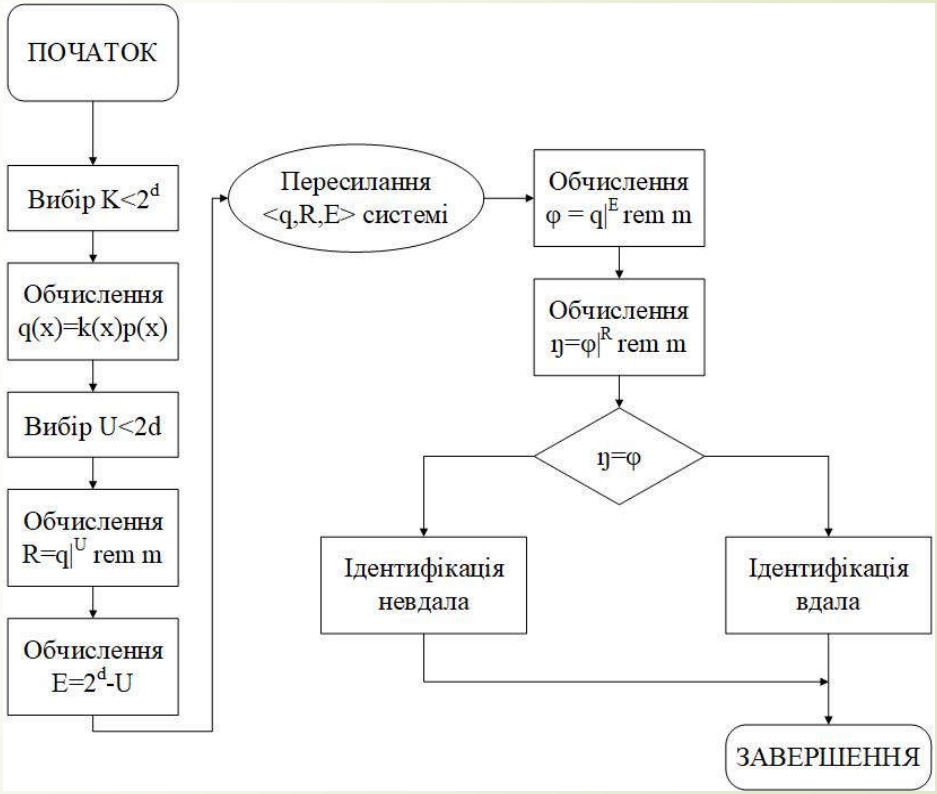
Послідовність дій при реєстрації користувача



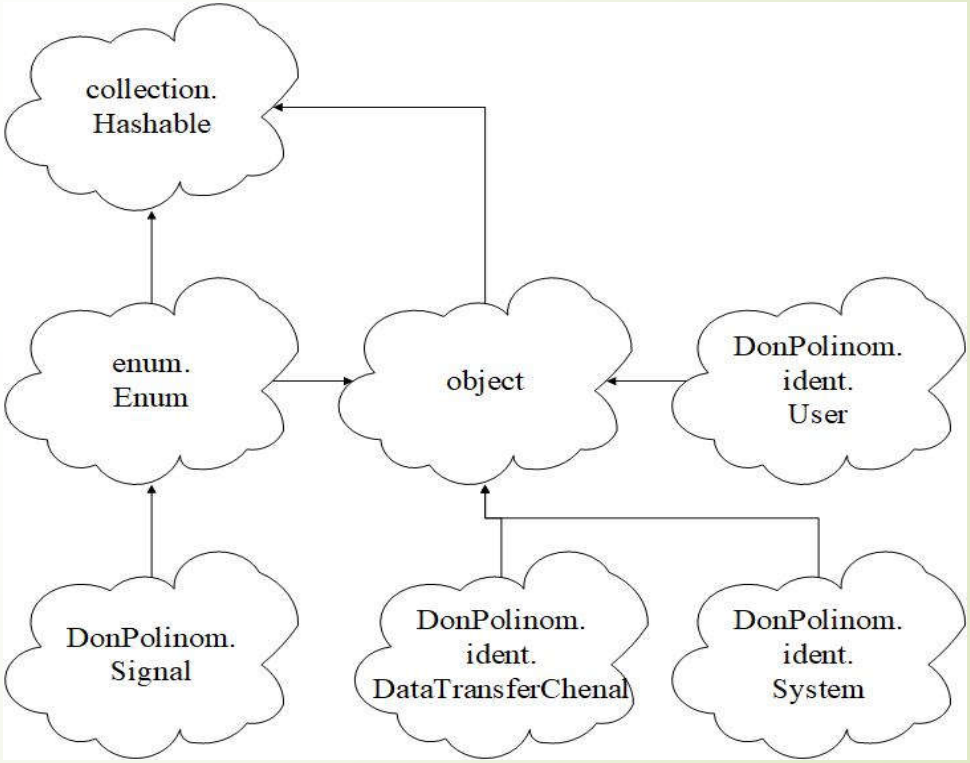
Процедура одного циклу ідентифікації



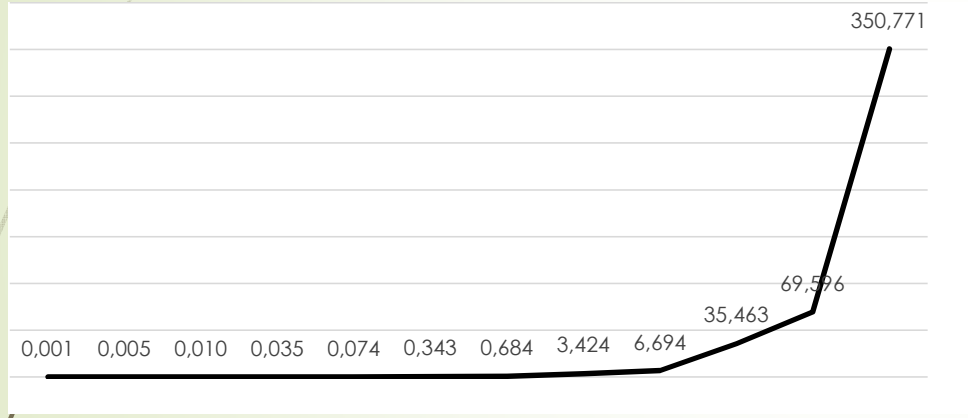
Інформаційна модель технології ідентифікації користувачів

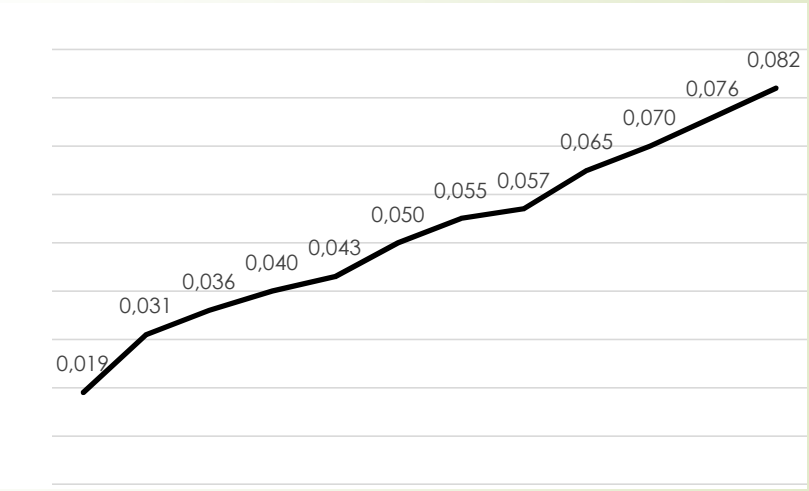


Основні рішення з реалізації програми



Апробація інформаційної технології ідентифікації користувачів





Загальні висновки

Дана робота є закінченим дослідженням, розв'язує науково-технічну задачу створення інформаційної технології ідентифікації користувачів. У рамках роботи поставлені та вирішені такі завдання:

- 1. За результатами аналізу існуючих методів, технологій та рішень методів ідентифікації користувачів обґрунтовано потребу у створення інформаційної технології, яка реалізує концепцію «нульових знань».
- 2. Удосконалено існуючих методів ідентифікації у напрямку покращення обчислювальної здатності, яка використовує метод експоненціонування з використанням поліноміальної арифметики.
- 3. Розроблено нову інформаційну технологію ідентифікації користувачів, яка має покращену обчислювальну здатність.
- Виконано експериментальну перевірку інформаційної технології ідентифікації користувачів. Результати експериментального тестування запропонованої інформаційної технології довели її спроможність розв'язувати поставлені задачі.

Mon Nov 30 19:23:52 EET 2020, Петровський Сергій Степанович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 78%**

	Документ		Сумарний збіг по Базі Даних	
ID: 81738 Назва: Інформаційні технології ідентифікації користувачів Додано в БД: 2020-11-30 Автора: Карпанасюк Віктор Володимирович Керівники: Пасічник О.А. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	57493	423	429 (1%)	7 (2%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

РІШЕННЯ КАФЕДРИ **КОМП'ЮТЕРНИХ НАУК ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ** ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: **Інформаційні технології ідентифікації користувачів**
Автор: **Карпанасюк В.В.**
Спеціальність: **122 Комп'ютерні науки**
Науковий керівник: **к.т.н., доцент Пасічник О.А.**

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	**відповідає**
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	-
3	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	-
4	Інше:	-

Підтвердження: Виявленні запозичення не є плагіатом т.я. розміщенні в розділах, які не описують безпосередньо авторське дослідження, складають 10,2% та мають посилання на приведений список літературних джерел

02.12.2020
Дата

Підпис керівника

Підпис завідувача кафедри

Хмельницький національний університет

Кафедра комп'ютерних наук та інформаційних технологій

ВІДГУК ОПОНЕНТА
на дипломну роботу магістра

Магістра *гр. КНм-19-1 Карпанасюка Віктора Володимировича*

На тему: *Інформаційна технологія ідентифікації користувачів*

1. Актуальність і значення теми

Загальносвітовим трендом технічного та технологічного прогресу людства в останні десятиліття є активна інтеграція інформаційних систем. Утворений внаслідок цього процесу інформаційний простір надає можливість використовувати великі обсяги інформації задля вирішення широкого кола проблем. Особливої актуальності питання ідентифікації користувачів набуло останнього часу коли інформатизація та цифровізація охопили практично усі сфери життєдіяльності людини, а мережеві технології стають повсякденним інструментарієм практичного кожного пересічного громадянина. Наявні значні за обсягом інформаційні ресурси стають доступними широкому колу користувачів створюючи, одночасно, нові можливості для протиправних дій, у тому числі, шляхом зламу існуючих механізмів захисту та контролю доступу. Потенціал мережевих технологій опосередковано впливає на зниження криптографічної стійкості існуючих методів та порушує баланс сил у світі інформаційної безпеки. Це вимагає пошуку адекватних рішень щодо вдосконалення існуючих криптографічних методів, в тому числі і методів ідентифікації користувачів.

2.Оцінка якості та достовірності проведених досліджень.

Результати досліджень є достатньо чіткими та обгрунтованими, відповідними до завдань дипломної роботи.

3. Оцінка запропонованих заходів та пропозицій, практичної цінності та ефективності.

Робота студента є закінченим дослідженням, розв'язує певну науково-технічну задачу створення інформаційної технології ідентифікації користувачів на основі концепції «нульових знань».

4. Загальний висновок та оцінка

Робота студента є достатньо актуальною. Робота студента була виконана загалом у відповідності до поставлених задач. Робота логічно структурована, дослідження відповідають поставленим завданням. Робота відповідає вимогам, що ставляться до магістрів. Карпанасюк В.В. заслуговує присвоєння кваліфікації магістра з комп'ютерних наук та інформаційних технологій.

Робота заслуговує на оцінку « добре ».

Опонент Медведчук И.К., к.т.н., доцент кафедри галузевого машинобудування та агроінженерії.