Професійна освіта

В.П. Полторак

Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах

Навчальний посібник

ПРОФЕСІЙНА ОСВІТА

В.П. Полторак

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ЗАХИСТ ДАНИХ В КОМП'ЮТЕРНИХ ТЕХНОЛОГІЯХ І МЕРЕЖАХ

✦

Навчальний посібник

для студентів вищих навчальних закладів, які навчаються за напрямом підготовки «Інтегровані інформаційні системи» спеціальності «Інформаційні системи та технології».

Київ
КПІ ім. Ігоря Сікорського
2020

УДК 004.9

Рецензент: *Романкевич В.О.*, доктор технічних наук, доцент, завідувач кафедри, доцент кафедри системного програмування і спеціалізованих комп'ютерних систем, КПІ ім. Ігоря Сікорського

Відповідальний редактор *Новацький А.О.*, кандидат технічних наук, доцент

Гриф надано Методичною радою КПІ ім. Ігоря Сікорського (протокол № 4 від 10.12.2020.р.) за поданням Вченої ради Факультету інформатики та обчислювальної техніки (протокол № 4 від 23.11.2020 р.)

Електронне мережне навчальне видання

Полторак Вадим Петрович

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ЗАХИСТ ДАНИХ В КОМП'ЮТЕРНИХ ТЕХНОЛОГІЯХ І МЕРЕЖАХ

Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах [Електронний ресурс] : навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології» / В.П. Полторак ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 1,73 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2020. – 78 с.

Викладено основні поняття сучасного підходу до інформаційної безпеки та захисту даних в комп'ютерних технологіях і мережах. Наведено моделі загроз інформації та основні механізми і протоколи її захисту. Викладено математичні засади криптографічного перетворення даних та, засновані на теорії чисел, найпопулярніші сучасні асиметричні криптоалгоритми. Для кращого засвоєння розділи посібника супроводжені контрольними запитаннями та завданнями. Для студентів, які навчаються за спеціальністю 126 «Інформаційні системи та технології», буде корисний аспірантам, викладачам та спеціалістам, які працюють у галузі захисту інформації.

УДК 004.9

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

ІС – інформаційна система,

КТ – комп'ютерні технології,

ІП – інформаційні процеси,

ДСТУ – державний стандарт України,

ОІД - об'єкт інформаційної діяльності,

СІД - суб'єкт інформаційної діяльності,

ТЗІ - технічний захист інформації,

КУО - каналоутворююче обладнання,

Кодек - сукупність Кодера і Декодера,

ASCII - American Standard Code for Information Interchange,

ЕЦП – електронний цифровий підпис,

A_q - скінченний дискретнмй алфавіт,

q – потужність скінченного дискретного алфавіту A_q,

M – повідомлення,

m – числовий образ повідомлення,

c - криптограма,

K – ключ,

k_{pb} - публічний ключ,

k_{pr} - секретний або приватний ключ.

$h = hash(m)$ - функція $hash$-перетворення над m,

$GF(q)$, $GF(p)$ - скінченне поле Галуа потужності q, або p,

p - просте число,

M_p - множина всіх ненульових елементів поля $GF(p)$,

w - первісний елемент поля,

$\varphi(n_b)$ - число Ейлера, для n_b.

ПЕРЕДМОВА

Сучасне суспільство все більшою мірою спирається на Інформаційні процеси, які стають рушійною силою економіки, суспільних відносин, військової справи. Інформаційні процеси - це процеси збору, підготовки, передачі, обробки, перетворення та використання інформації в різних сферах суспільства. Інформація, за одним із продуктивних визначень, є корисні, або ж, нові відомості про навколишній і внутрішній світ. Вона не дається нам безпосередньо, через органи відчуттів. Вона дана нам опосередковано, через фізичні носії - знаки, символи, сигнали (збурення фізичного стану середовища розповсюдження), тощо. Зазвичай їх називають даними. Весь комплекс інформаційних процесів сьогодні переважно відбувається на базі комп'ютерних технологій. А середовищем для передавання інформації, що є поданою у формі даних, переважно виступає комп'ютерна мережа. То ж, питання стійкості інформації до різних загроз у інформаційних системах, її функціональної надійності та доступності для легальних користувачів, безпеки комп'ютерних технологій та мереж поєднуються у складний вузол проблем, що мають вивчатися студентами технічного ВНЗ.

Навчальний посібник може бути рекомендований студентам спеціальностей: 126 Інформаційні системи та технології, 121 Інженерія програмного забезпечення і відповідає навчальним програмам таких дисциплін як «Захист інформації в комп'ютерних системах і мережах», «Інформаційна стійкість комп'ютерних технологій і мереж», «Проектування комплексних систем захисту інформації», «Інформаційна безпека та захист даних», «Безпека мобільних систем», тощо. В межах навчальних програм дисциплін, йдеться про основні сучасні моделі, механізми захисту даних в інформаційних системах, технологіях і мережах, та про їх реалізацію методами математики (зокрема, теорії чисел та алгебри).

ВСТУП

Проблеми інформаційної безпеки, захисту даних в інформаційних системах (ІС), інформаційної стійкості комп'ютерних технологій (КТ) і мереж в цифрових інформаційних системах вимагають все більшої уваги суспільства.

Сучасне суспільство все більшою мірою спирається на Інформаційні процеси (ІП), які стають рушійною силою економіки, суспільних відносин, військової справи. Інформаційні процеси - це процеси збору, підготовки, передачі, обробки, перетворення та використання інформації в різних сферах суспільства: економічній, соціальній, освітній, політичній, військовій, тощо. Інформація, за одним із продуктивних визначень, є корисні, або ж, нові відомості про навколишній і внутрішній світ. Вона не дається нам безпосередньо, через органи відчуттів. Інформація дана нам опосередковано, через фізичні носії - знаки, символи, сигнали (збурення фізичного стану середовища розповсюдження), тощо. Зазвичай їх називають даними. Цей Навчальний посібник присвячений теоретичному викладу і практичним вправам з основних тем захисту інформації в цифрових інформаційних системах з метою їх захисту від загроз, спричинених цілеспрямованими діями зловмисників, і забезпечення інформаційної стійкості і надійності комп'ютерних технологій і мереж. Головну увагу приділено теоретичному викладу основних тем з криптографічних перетворень даних в комп'ютерних технологіях і мережах, в цифрових інформаційних системах (ІС) з метою їх захисту від загроз, математичним засадам захисту інформації віл загроз, детальному розгляду популярних на сьогодні криптографічних алгоритмів. Весь комплекс питань у галузі захисту інформації у комп'ютерних технологіях та мережах є наразі доволі розлогим, широко розгалуженим і його неможливо повністю висвітлити в одному навчальному посібнику. Тому, в межах навчальних програм дисциплін, йдеться про основні сучасні моделі і механізми захисту даних в інформаційних системах, технологіях і мережах, та про їх реалізацію методами математики (зокрема, теорії чисел та алгебри).

Під інформаційною системою (ІС) розуміють будь-яку систему, яка за допомогою організаційних, та технічних засобів виконує такі функції, як вилучення, збирання, передавання, перетворення, накопичення, зберігання, оброблення та використання інформації [1]. За ДСТУ 2392-94: Інформаційна система це є комунікаційна система, що забезпечує збирання, пошук, оброблення та пересилання інформації, а комунікація - це передача значень знаків, символів шляхом пересилання сигналів [2]. За іншим джерелом, Інформаційна система це автоматизована система, комп'ютерна мережа або система зв'язку [3]. За призначенням, ІС поділяють на системи електрозв’язку, передачі даних, інформаційно-вимірювальні системи, системи обробки даних, пошукові системи, сховища даних, системи експериментальних досліджень, автоматизовані системи управління, тощо [1].

Системи зв’язку за останні десятиліття кардинально трансформувалися і набули нових рис та можливостей, досягли високих показників ефективності за критеріями енергоспоживання, завадостійкості, використання наявної смуги частот пропускання, відношення сигнал/завада та пропускної спроможності каналу зв’язку C (за К. Шенноном [1]). Найкращі показники якості та ефективності за згаданими критеріями демонструють саме цифрові системи зв’язку, які є необхідними компонентами ІС, або ж, компонентами, що поєднують різні ІС [4]. Термін «цифрові системи» є доволі умовним і їх можна називати «числові системи». А за сутністю своєю, вони є системами зі скінченним дискретним алфавітом, тому більш точним може бути термін «дискретні системи». Тобто, цифровими є такі системи, дані в яких представлені символами (цифрами) зі скінченного дискретного алфавіту A_q потужності q, де q - кількість дискретних символів в алфавіті A_q. Так, наприклад, двійковий алфавіт $A_2 = \{0;1\}$ містить $q = 2$ дискретних символи, які є співставленні, наприклад, із цифрами «0» та «1». А взагалі, символи алфавіту є лише знаками, картинками, ієрогліфами, своєрідними піктограмами і неважливо, як ми їх позначаємо, чи які зображення вони мають [2]. Для будь-якого алфавіту A_q має значення лише величина q та імовірності появи символів

у повідомленнях. Це дозволяє вести облік кількості інформації у повідомленнях, текстах, складених із символів A_q, виводить нас на алгоритми стиснення даних (архівування), тощо.

Варто ще раз підкреслити - до інформації не можна доторкнутися, помацати її рукою, побачити її колір, відчути її запах і т.д. Всі засоби і механізми, що дозволяють «дізнатися» інформацію, є лише посередниками між джерелом і одержувачем. Інформацію можна отримати з джерела, зберегти на носії, передати через канал, захистити від зловмисника тільки у формі цифрового коду (послідовності знаків, символів, букв, обраних з деякого алфавіту та за певними, заздалегідь обумовленими правилами), тому «кодування / код» - це процес / форма подання інформації за допомогою знаків , символів, букв з деякого алфавіту з певною метою і дотриманням заздалегідь обумовлених правил і обмежень.

Контрольні запитання

1. Наведіть визначення інформаційних процесів.
2. Наведіть визначення інформації.
3. В чому полягає опосередкованість сприйняття інформації?
4. Наведіть визначення терміну «сигнал».
5. Наведіть визначення терміну «дані».
6. Наведіть три визначення терміну «інформаційна система».
7. Наведіть класифікацію інформаційних систем за призначенням.
8. Які комунікаційні системи демонструють найкращі показники за пропускною спроможністю каналів комунікації?
9. Наведіть визначення терміну «цифрова система».
10. Що таке «дискретний алфавіт»? Наведіть його характеристики.
11. Яким чином ми дізнаємося «інформацію»?
12. Наведіть визначення термінам «код», «кодування».

1. ЗАВДАННЯ ЗАХИСТУ ДАНИХ В ЦИФРОВИХ СИСТЕМАХ

Серед основних завдань захисту даних в цифрових інформаційних системах є забезпечення конфіденційності об’єктів інформаційної діяльності (ОІД) таких, як повідомлення, тексти, дані, документи, тощо; забезпечення аутентифікації ОІД та суб’єктів інформаційної діяльності (СІД); забезпечення механізмів і засобів виявлення порушень цілісності ОІД та СІД; забезпечення доступності ІС та ОІД для легальних користувачів, СІД; нонрепудіація - унеможливлення відмови СІД від виконаних в ІС дій, або прийнятих на себе обов’язків (має значення для електронного документообігу) більш точно - це унеможливлення відмови відправника від факту передачі повідомлення, а одержувача - від факту отримання повідомлення [3,4,5,6]. Так, за джерелом [3]: конфіденційність - це властивість інформації бути захищеною від несанкціонованого ознайомлення; цілісність - це властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення; доступність - це властивість інформації бути захищеною від несанкціонованого блокування; технічний захист інформації (ТЗІ) - це діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації. Нагадаємо, що інформація доступна нам опосередковано, через носії, які є фізичною формою її подання, тобто - дані (знаки, символи, сигнали). Тож, з погляду фізичного, у питаннях захисту інформації та забезпечення інформаційної стійкості ІС і мереж, ми можемо оперувати лише її носіями - даними.

Іншими словами, конфіденційність - це гарантування доступу до інформації, що зберігається в інформаційній системі і пересилається по каналах зв'язку тільки тим суб'єктам, які мають право її отримувати [6].

Цілісність - це гарантування можливості модифікації інформації, що міститься в інформаційній системі і пересилається по каналах зв'язку тільки тими суб'єктами, які мають на це право. Модифікація може означати: запис,

зміну, зміну стану, видалення, створення, затримку або повторне відтворення повідомлень, що пересилаються [6].

Керування доступом - це забезпечення можливості контролю доступу до інформаційних ресурсів або самою системою, що володіє ресурсами, або системою, якій ці ресурси надаються [6].

Доступність - це гарантування авторизованим суб'єктам доступу до інформації і ресурсів, що зберігаються в системі, в будь-який час, при першій необхідності (або відповідно до заданого розкладу доступу) [6].

Термін аутентифікація формулюється і подає, за своєю сутністю, процес підвищення ступеня довіри між ІС і ОІД та/або СІД у межах комп'ютерної технології та комунікаційної мережі, а також, встановлення достовірності (автентичності) сторін, що приймають участь у комунікації [4,5,6]. Це є гарантування автентичності, справжності джерела повідомлення або електронного документа, а так само того, що джерело не є підробленим.

Суб'єкт інформаційної діяльності (СІД) - це той, хто/що легально працює над створенням, чи модифікацією ОІД. Це може бути людина-оператор, а може бути й обчислювальний процес, автоматично запущений на обчислювальному пристрої і який може самостійно звертатися (за своїм алгоритмом чи комунікаційним протоколом) до ІС чи інших СІД відсилаючи їм, або отримуючи від них ОІД.

Об'єкт інформаційної діяльності (ОІД) - це, власне, і є «предмет праці» СІДа і предмет жадання зловмисника - це дані, повідомлення, тексти, що складаються СІДом з символів певного алфавіту, за певними правилами у формі даних і несуть в собі інформацію, що потребує захисту.

Криптографічне шифрування - це кодування, як своєрідна форма подання інформації дискретними даними, з метою забезпечити вирішення згаданих вище завдань захисту інформації.

Зловмисник – це фізична особа, або ж, група фізичних осіб; юридична особа, або ж, група юридичних осіб; обчислювальний процес, або група, пов'язаних взаємодією через мережу процесів, запущених на різних

обчислювальних ресурсах, які мають злий умисел і мету нашкодити легальній інформаційній системі і її ОІД та СІД, реалізуючи різні сценарії наведених вище загроз безпеці інформаційної системи та порушуючи її інформаційну безпеку. Зловмисника для нейтральності іноді називатимемо криптоаналітиком.

Аналіз загрози інформації виходячи з мети її досягнення, моделі зловмисника, уявлення про можливий сценарій виконання та процедури реалізації має назву «модель загрози інформації».

Уявлення про мету, властивості і характеристики передбачуваного зловмисника, можливий сценарій реалізації ним загрози інформації, має назву «модель зловмисника» в інформаційній системі.

1.1. Контрольні запитання

1.1.1 Основні завдання захисту даних в цифрових інформаційних системах.
1.1.2 Конфіденційність об’єктів інформаційної діяльності.
1.1.3 Аутентифікація об’єктів і суб’єктів інформаційної діяльності.
1.1.4 Цілісність об’єктів і суб’єктів інформаційної діяльності.
1.1.5 Доступність інформаційної системи та об’єктів і інформаційної діяльності.
1.1.6 Надайте визначення терміну «нонрепудіація».
1.1.7 Надайте визначення терміну «технічний захист інформації».
1.1.8 Визначити термін «керування доступом до інформаційних ресурсів».
1.1.9 Надайте визначення терміну «суб’єкт інформаційної діяльності».
1.1.10 Надайте визначення терміну «об’єкт інформаційної діяльності».
1.1.11 Визначити термін «Криптографічне шифрування».
1.1.12 Надайте визначення терміну «Зловмисник» в інформаційній системі.
1.1.13 Які існують загрози безпеці інформації та інформаційної системи.
1.1.14 Дайте визначення терміну «модель загрози інформації» в ІС.
1.1.15 Дайте визначення терміну «модель зловмисника» в ІС.

2. МОДЕЛЬ ЦИФРОВОЇ СИСТЕМИ КОМУНІКАЦІЇ

Як відомо, модель – це є невичерпний опис об'єкта дослідження, який висвітлює певну кількість властивостей об'єкта і його характеристик, які дослідник вважає суттєвими для набуття уяви про об'єкт у поточний час [7].

Зазвичай, під терміном канал передачі даних розуміють сукупність середовища розповсюдження сигналу та каналоутворюючого обладнання (КУО). Це достатньо умовне і широке поняття, від КУО можуть вимагати виконання певної кількості різноманітних функцій [1, 4]. Ступінь складності потрібного нам уявлення про канал і систему зв’язку впливає на кількість та взаємозалежність цих функцій і вид та вигляд відповідної моделі. Так, наприклад, для графічної моделі односторонньої цифрової системи зв’язку відомо багато варіантів - від самих простих, до найскладнішого [1, 4]. На Рис. 1 наведено одну з можливих сучасних моделей цифрової системи зв’язку.

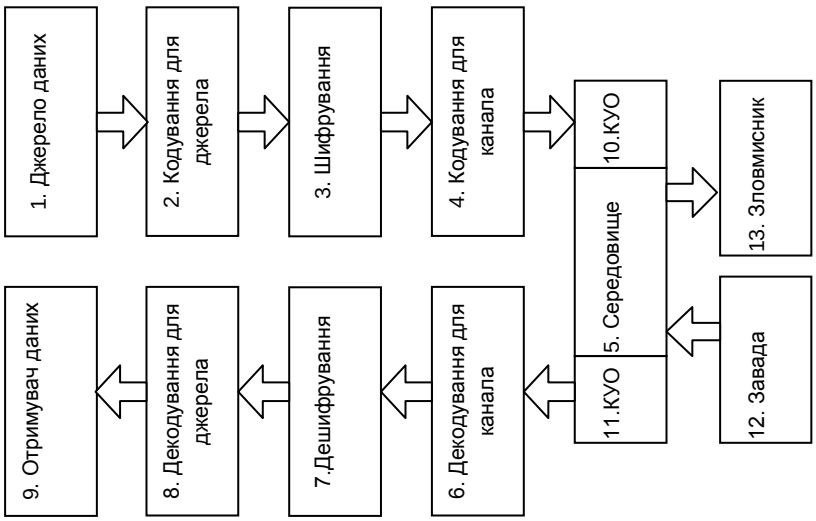

Рисунок 1 - Модель цифрової системи комунікації

На моделі Рис. 1 виокремлено найхарактерніші функціональні блоки сучасної цифрової системи комунікації: Джерело даних 1 та Отримувач даних 9; Кодек для джерела (Кодер-Декодер) 2 та 8; Криптографічні блоки Шифрування/Дешифрування 3 та 7; Кодек для канала 4 та 6; власне, канал передачі даних 5, 10 та 11; Джерело завад 12; Зловмисник 13.

Джерелом даних може бути людина-оператор з потребою передавати голосові повідомлення, або ж, текстові повідомлення з клавіатури від кінцевого пристрою. Це може бути сховище даних, просто блок пам’яті, або певний алгоритмічний процес, запущений на обчислювальному пристрої, тощо. У будь-якому разі, повідомлення від джерела піддають так званій процедурі форматування, яка включає в себе ряд цифрових перетворень, у тому числі, первинне кодування даних, наприклад, кодом ASCII. Мета форматування - привести повідомлення Джерела до цифрового виду, прийнятного для блоків 2, 8 та 9, можливо, і інших блоків моделі Рис. 1. Відповідно, зворотна процедура форматування дозволяє відновити цифрову форму повідомлення від блоку 8 до прийнятної для Отримувача 9.

Джерело 1 направляє Отримувачу 9 відкрите, незахищене повідомлення, яке Зловмисник 13 може перехопити у Середовищі 5 і прочитати порушивши конфіденційність, якщо не потурбуватися про захист даних, що передаються (за відсутності блоків 3 та 7).

Кодек для джерела (блоки 2 та 8) виконує функцію стиснення і відновлення даних для джерела (архівування/деархівування), що зменшує витрати ресурсів на подальше зберігання, перетворення та передачу повідомлень за рахунок зменшення кількості символів, якою подається задана у висхідному повідомленні кількість інформації. Водночас Кодек для джерела кардинально змінює статистичний розподіл ймовірностей для символів алфавіту висхідних повідомлень Джерела, що додатково маскує його властивості і суттєво зменшує шанси Зловмисника на «швидке» прочитання перехоплених у Середовищі повідомлень у разі наявності блоків 3 та 7 і задіювання їх функціоналу. Це убезпечує від (або значно ускладнює) порушення конфіденційності повідомлень таким потужним методом, як статистичний криптоаналіз. Проте стиснення даних викликає системний недолік - майже повну втрату природної (хоча і завеликої) надлишковості у повідомленнях між блоками 2 і 8. Це зовсім позбавляє цифрову систему зв’язку

можливості виявляти та виправляти випадкові помилки у повідомленнях, що виникли від спотворення сигналів Завадою у Середовищі розповсюдження.

Криптографічні блоки Шифрування/Дешифрування 3 та 7 у моделі Рис. 1 виконують функцію забезпечення конфіденційності повідомлень у блоках 4, 5, 6, 10 та 11, і, власне, у Середовищі 5, де очікується, що вони можуть бути перехоплені Зловмисником. Їх функціонування не впливає на надлишковість повідомлень у згаданих блоках. Але будь-яка випадкова помилка (-ки), викликана (-ні) впливом Завади на сигнали у Середовищі розповсюдження, призведе до унеможливлення правильного Дешифрування захищеного блоком 3 повідомлення і переривання комунікації сторін. Це, зокрема, обґрунтовує наявність Кодека для канала 4 та 6 на Рис. 1.

Кодек для канала 4 та 6 виконує функцію кодування/декодування повідомлень надлишковими кодами для забезпечення завадостійкості повідомлень, що передаються, у разі випадкового спотворення Завадою 12 деяких символів тих повідомлень. Надлишковість, у вигляді додаткових символів обчислених за висхідними даними, що передаються, тут уже штучно повертають назад у повідомлення з метою відновлення можливості виявити і виправити певну кількість помилок. Але вводять її контрольовано і суворо дозовано так, щоби виконати конкретне завдання: виявити (або виявити та виправити) задану кількість помилок у повідомленні певної довжини. Зайвої надлишковості стараються уникнути, щоби максимально ефективно використати ту її дозовану кількість, яку штучно вводили і яка тепер суттєво менша за природну, що міститься у повідомленнях Джерела. За умови узгодження параметрів Кодека для каналу 4, 6 і самого каналу 5, 10 та 11, можна очікувати надходження безпомилкових захищених повідомлень на вхід дешифратора 7. Цей механізм виявлення і виправлення помилок в криптограмах забезпечує правильне дешифрування блоком 7 захищених повідомлень, які після деархівації блоком 8 надходять до Отримувача у прийнятному, «читабельному» вигляді.

Таким чином, природні висхідні повідомлення мають завелику природну надлишковість, що зумовлює, з одного боку, можливість виявлення і виправлення помилок у повідомленнях під час їх приймання. А з іншого боку, це призводить до полегшення розкриття криптограм, перехоплених в каналі комунікації криптоаналітиком, методами статистичного аналізу їх великих колекцій, якщо Відправник не потурбувався про порушення статистики висхідних текстів перед зашифруванням. Тому має сенс спочатку піддати висхідний текст повідомлення архівуванню (стисненню даних), що порушує його статистичні властивості, потім виконати зашифрування, після чого закодувати криптограму завадостійким кодом, вносячи до повідомлення дозовану надлишковість, для виявлення і виправлення помилок.

2.1. Контрольні запитання

2.1.1 Наведіть визначення терміну «модель».
2.1.2 Наведіть визначення канала передачі даних.
2.1.3 Опишіть модель цифрової системи зв’язку.
2.1.4 Що таке Кодек для джерела, його роль в моделі канала?
2.1.5 Яке призначення криптографічних блоків Шифрування/Дешифрування?
2.1.6 Яке призначення Кодека для канала в моделі системи зв’язку?
2.1.7 Яка роль Джерела завад в моделі канала?
2.1.8 Яка роль Зловмисника в моделі канала зв’язку?
2.1.9 Опишіть Джерело даних в моделі канала зв’язку.
2.1.10 Опишіть взаємодію Джерела і Отримувача даних в моделі канала зв’язку.
2.1.11 Який системний недолік має канал без Кодека для канала?
2.1.12 Опишіть взаємодію Крипто-блоків Шифрування/Дешифрування.
2.1.13 Які наслідки випадкових помилок у криптограмах в каналі комунікації?
2.1.14 Механізм, що забезпечує правильне дешифрування в каналі комунікації?
2.1.15 Який вплив надлишковість чинить на якість захищеної комунікації?

3. МОДЕЛЬ СИМЕТРИЧНОЇ КРИПТОСИСТЕМИ

Далі поведемо мову у термінах символів, алфавітів, повідомлень, користувачів ІС (легальний суб'єкт інформаційної діяльності, СІД), об'єктів інформаційної діяльності, ОІД, тощо.

Симетричною називають криптосистему з єдиним (секретним, приватним) ключем K для зашифрування і дешифрування повідомлення - ОІД, для якого потрібно забезпечити конфіденційність у разі зберігання в ІС, або передавання його через відкритий, незахищений канал зв'язку. На Рис. 2 наведено одну із моделей симетричної криптосистеми [9].

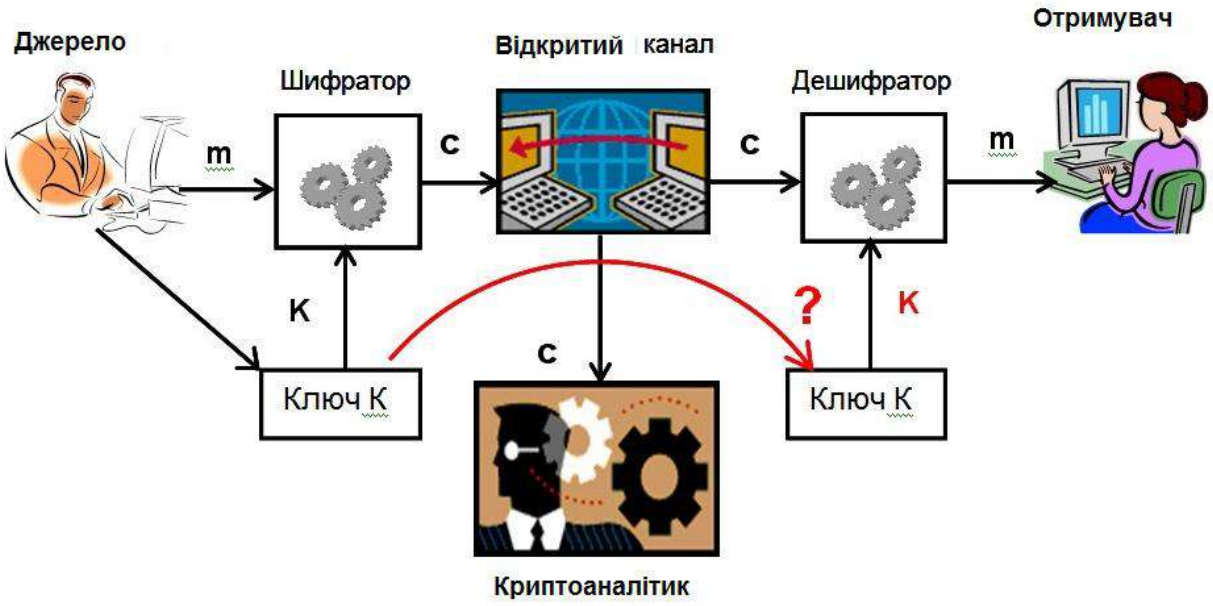

Рисунок 2 - Модель симетричної криптосистеми

Модель симетричної криптосистеми на Рис. 2 має трьох акторів: Джерело, Отримувач, Криптоаналітик, кожний з яких має свою мету, свої інтереси та свої засоби і можливості досягнення мети у процесі захищеної комунікації.

Джерело (інакше називають - відправник, суб'єкт інформаційної діяльності, СІД) на Рис. 2 готує повідомлення для відправки Отримувачеві (розглядаємо його як інший СІД). Повідомлення – ОІД, набуває цифрового

вигляду послідовності дискретних знаків m (це має назву операція форматування), які є символами скінченного алфавіту A_q. Для захисту конфіденційності повідомлення, його піддають операції шифрування у Шифраторі на ключі K.

Відправник будь-яким чином має згенерувати, або отримати у Довіреної третьої сторони, ключ K. Тема генерування «гарних» криптографічних ключів сама по собі є окремим відгалуженням криптографії і докладно розглядається у багатьох джерелах, наприклад [4,5,6]. Зашифроване повідомлення називають, зазвичай, криптограмою і воно набуває вигляду послідовності цифр c скінченного алфавіту A_q (з тим самим значенням q, або ж іншим, в залежності від застосованого криптоалгоритма). Символи криптограми c передаються через відкритий (незахищений) канал зв'язку на сторону Отримувача. У відкритому, незахищеному каналі, символи криптограми можуть бути перехоплені криптоаналітиком. У подальшому, перехоплена послідовність символів c може бути піддана криптоаналітиком спробам нелегального, незаконного дешифрування.

Вважаємо, що в каналі додатково застосовано надлишкове завадостійке кодування символів c з метою виявлення і виправлення помилок у послідовностях символів c, що дозволяє безперешкодно дешифрувати їх дешифратором, на вхід якого вони поступають з виходу канала, і отримати послідовність висхідних символів m, якими подано відкритий текст повідомлення.

Але для цього потрібно подати той же самий ключ K на відповідний вхід Дешифратора на приймальному боці системи захищеної комунікації (Рис. 2). Проблема симетричної криптосистеми полягає в тому, що для розповсюдження секретного (єдиного) ключа K, від Джерела повідомлення до Отримувача, необхідно використати секретний, захищений канал зв'язку. Інакше, у відкритому каналі, він може попасти в руки криптоаналітика і ним можуть скористатися зловмисники для проникнення у смисл перехоплених повідомлень (криптограм). У разі успішного розшифрування послідовностей

криптограм c криптоаналітиком, відбудеться порушення конфіденційності комунікацій. Якщо убезпечити секретний ключ K від потрапляння в руки криптоаналітика, то це суттєво зменшує його шанси на швидкий доступ до смислу повідомлень Джерела [9].

На Рис. 3 наведено модель симетричної криптосистеми, з чотирма акторами, з Довіреною третьою стороною, яка забезпечує незалежне генерування, узгодження та розповсюдження секретних ключів для учасників захищеного обміну [5,6]. Тут ініціатором обміну може виступати як Джерело, так і Отримувач повідомлень, а Довірена третя сторона надає їм секретний ключ.

Перевага симетричних криптосистем (з єдиним ключем) полягає в тому, що вони, маючи високу продуктивність, дозволяють передавати великі обсяги зашифрованих даних через незахищений (відкритий) канал зв'язку.

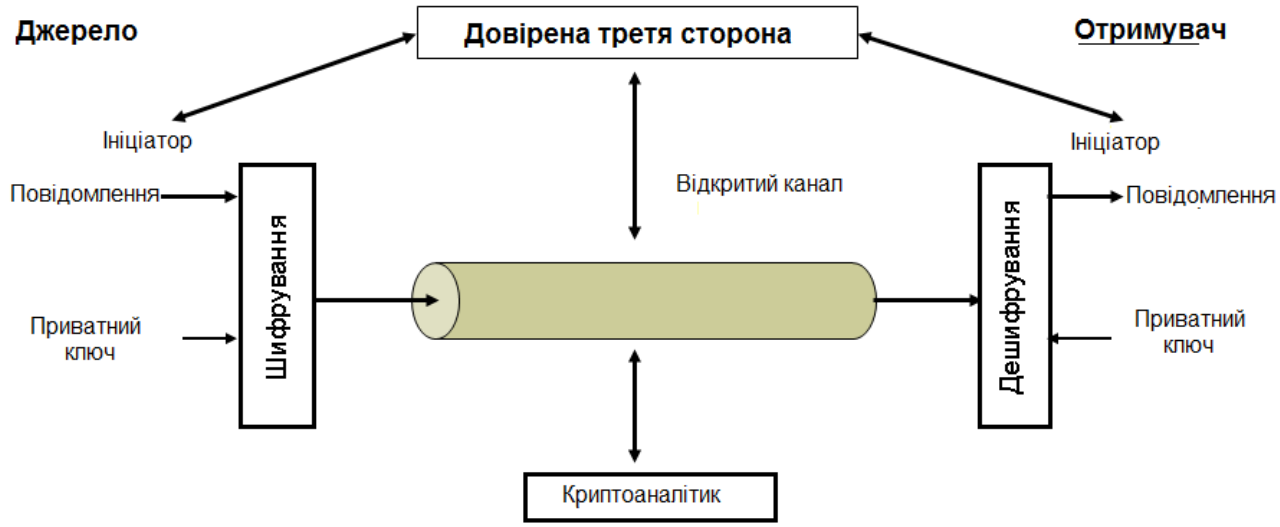

Рисунок 3 - Симетрична криптосистема з довіреною третьою стороною

А їх недолік полягає в тому, що вони не можуть повністю позбутися потреби у захищеному (секретному) каналі, що використовується для поширення секретного ключа K .

Від сивої давнини і до середини сімдесятих років минулого століття, всі, відомі за писемними джерелами, криптосистеми були симетричними і страждали на одну і ту ж саму, згадану вище проблему. Проблему

розповсюдження єдиного симетричного ключа K до Отримувача криптограм, що потребує збереження секретного, захищеного канала передачі ключів. Ця проблема супроводжує симетричні криптосистеми і сьогодні. Проте, жоден пристойний комплекс криптографічних сервісів не обходиться сьогодні без симетричних криптосистем забезпечення конфіденційності [5]. Це відбувається з огляду на їх надзвичайно високу швидкодію за рахунок використання алгоритмів, команд і програмного забезпечення, природних для масових, широко розповсюджених процесорів в обчислювальних пристроях. Тому їх застосовують для забезпечення конфіденційності великих за обсягом текстів, масивів даних, тощо, де загальні витрати часу на шифрування/дешифрування не так помітні у порівнянні, наприклад, з асиметричними криптоалгоритмами і системами.

Оцінка якості та ефективності криптоалгоритмів визначається криптостійкістю. Криптостійкість криптоалгоритма це обсяг часу, потрібний криптоаналітику для розкриття смислу зашифрованого текста без знання секретних даних, наприклад, секретного ключа.

Серед найвідоміших і найпопулярніших сьогодні симетричних криптоалгоритмів можна назвати DES (і його підсилений варіант 3DES), сучасний національний стандарт США - AES, ГОСТ 28147-89 (спадок від СРСР), міждержавний стандарт України ДСТУ ГОСТ 28147:2009 (на базі ГОСТ 28147-89), IDEA, Cast, Blowfish і багато інших зі своїми перевагами і недоліками та бажаними сферами застосування. Варто окремо виділити сучасний, перспективний національний стандарт України ДСТУ 7624:2014 (що має поступово замінити міждержавний стандарт ДСТУ ГОСТ 28147:2009), який за рядом характеристик (швидкодія, криптостійкість) переважає відомі зарубіжні аналоги і є наразі єдиним у світі діючим національним стандартом симетричного криптоалгоритма, який може використовувати ключі довжиною 512 двійкових символів, що визначає надзвичайно високий рівень криптостійкості, якої можна досягти з його використанням [8].

Ми не будемо приділяти тут великої уваги симетричним алгоритмам з огляду на те, що вони дуже докладно і ретельно описані в літературі (підручники, монографії, окремі статті в журналах і в Інтернет), наприклад [4,5,6,8]. В наступному розділі розглянемо асиметричні криптосистеми.

3.1. Контрольні запитання

3.1.1 Навести визначення симетричної криптосистеми.

3.1.2 Сформулюйте призначення симетричної криптосистеми.

3.1.3 Наведіть опис симетричної криптосистеми і її компонент.

3.1.4 Опишіть симетричну криптосистему з чотирма акторами.

3.1.5 В чому полягає проблема симетричної криптосистеми?

3.1.6 В чому полягає перевага симетричних криптосистем?

3.1.7 Чому симетричні криптосистеми використовують до сьогодні?

3.1.8 Що таке криптостійкість криптосистеми?

3.1.9 Назвіть найвідоміші симетричні криптоалгоритми.

3.1.10 Надайте характеристики алгоритмів DES, 3DES.

3.1.11 Надайте характеристики алгоритму AES.

3.1.12 Надайте характеристики алгоритму ГОСТ 28147-89.

3.1.13 Надайте характеристики алгоритму ДСТУ 7624:2014.

3.1.14 Який розмір має найдовший ключ симетричної системи?

3.1.15 Що таке Довірена третя сторона?

3.1.16 Змоделюйте описово атаку «Man-in The-Middle».

3.1.17 Охарактеризуйте пасивні атаки на інформаційну систему.

3.1.18 Охарактеризуйте пасивні атаки на інформаційну систему.

4. МОДЕЛІ АСИМЕТРИЧНОЇ КРИПТОСИСТЕМИ

У 1976 році американські математики Вітфілд Діффі і Мартін Хеллман вперше оприлюднили схему розповсюдження секретного ключа через відкритий, незахищений канал зв'язку. Це був один з перших прикладів відкритої комунікації двох суб'єктів, які ніколи не зустрічалися один з одним, що дозволяла обом дистанційно отримати спільний секретний ключ через відкритий канал. Такий ключ в подальшому можна використати для шифрування наступних повідомлень симетричним криптоалгоритмом. Цей дотепний винахід, заснований на ідеї односторонніх функціональних перетворень (варіанти з лазівкою, чи без такої) започаткував еру асиметричної криптографії.

Асиметричною називають криптосистему з двома математично взаємообумовленими ключами. Один із них називають відкритим або публічним ключем k_{pb}, а інший - секретним або приватним ключем k_{pr} . Модель асиметричної криптосистеми наведено на Рис. 4 .

Вона передбачає зовсім відмінну від симетричної криптосистеми концепцію розподілу і використання ключів. Публічний ключ k_{pb} публікується для інших користувачів, наприклад, на сервері відкритих ключів і є доступним для них у будь-який час [9].

Обчислити приватний ключ k_{pr} за відомим значенням публічного k_{pb} без знання певних секретних даних (які використовувалися легальною частиною системи під час генерування пари ключів) не є можливим за осяжний чи прийнятний час. Залишається лише один шлях - так звана атака грубої сили, тобто, прямий перебір можливих варіантів ключів, що може потребувати від Криптоаналітика неприйнятної кількості часу і ресурсів для досягнення успіху. Це твердження базується на використанні в таких алгоритмах так званих «невирішених на поточний момент математичних задач», що створює для Криптоаналітика максимально можливі складнощі, зберігаючи максимально

можливі простоту і комфортність для легальних користувачів. В цьому полягає головна властивість асиметричної криптосистеми.

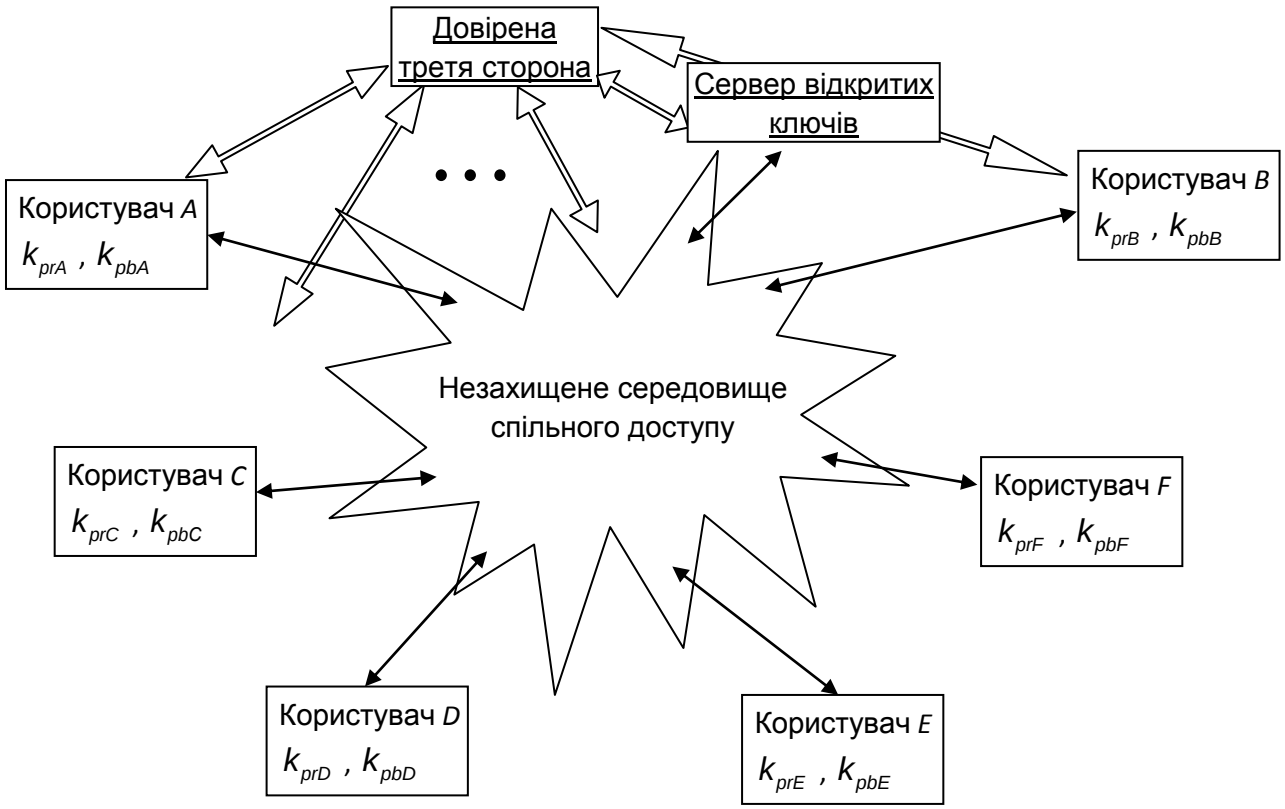

Рисунок 4 - Модель асиметричної криптосистеми

Перше, на що звертаємо увагу в межах цієї моделі, це те, що кожний користувач $СІД_j$ захищених комунікацій у Незахищеному середовищі спільного доступу (наприклад, мережа) має обчислити, або отримати від Довіреної третьої сторони власну пару зв'язаних ключів k_{prj} та k_{pbj}, де j - ім'я або номер користувача. У якості Довіреної третьої сторони може виступати певна організація, або її підрозділ, яким довіряють всі учасники захищеного інформаційного обміну. На Рис.4 звернення користувача до Довіреної третьої сторони і її відповідь умовно показані об'ємними стрілками, таку комунікацію виконують окремими засобами і процедурами, через відкриті канали із криптошифруванням. Приватні ключі k_{prj}, за визначенням, є секретними, тому мають зберігатися у користувачів під пильним наглядом і ніколи не

передаватися іншим суб'єктам ІС. Створені або отримані користувачами публічні ключі k_{pbj} зберігаються або у користувачів, або на Сервері відкритих ключів у певному форматі наборів даних, наприклад, сертифікатів відкритих ключів.

Протокол забезпечення конфіденційності Рис. 5 повідомлення M, поданого цифрами, символами m в асиметричній криптосистемі, під час передачі до Отримувача *B*, полягає в наступному [9].

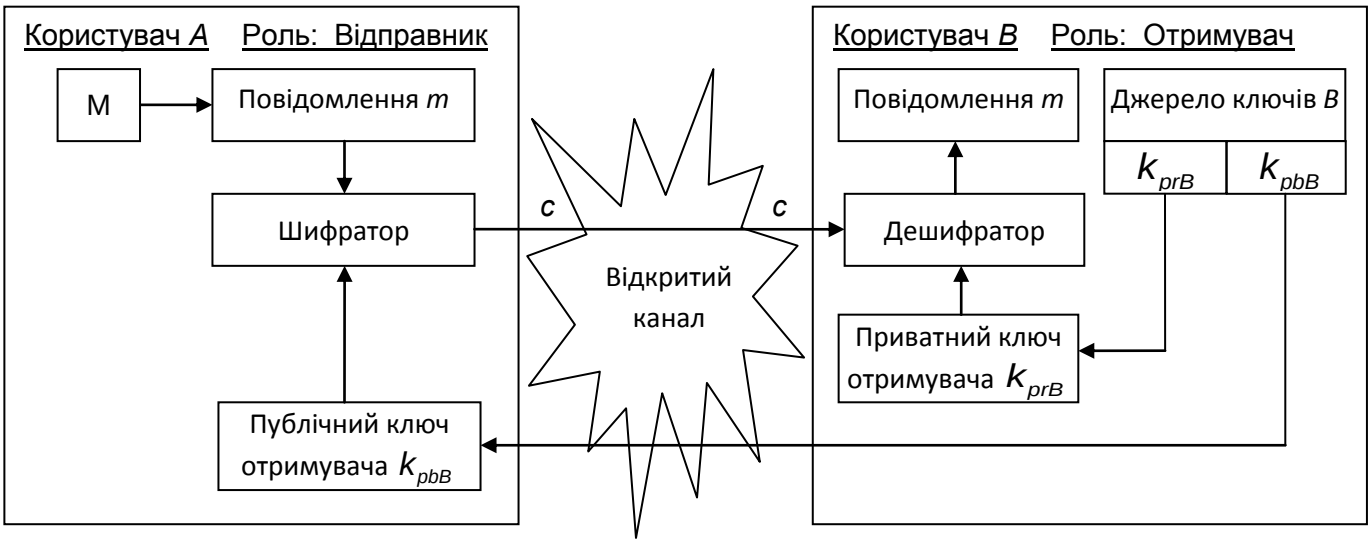

Рисунок 5 - Протокол конфіденційності в асиметричній криптосистемі

Користувач *A* зашифровує m на публічному ключі k_{pbB} отримувача *B*, а криптограму *c* він відправляє до *B*. Одержану криптограму *c* користувач *B* розшифровує на власному приватному ключі k_{prB} . Розшифрувати *c* може *B* і тільки *B* , оскільки тільки він, і ніхто інший, має приватний ключ k_{prB}. Ніхто інший, в тому числі Криптоаналітик, не має ключа k_{prB}, тому ніхто крім *B* не зможе легально (і швидко) розшифрувати криптограму *c*.

Протокол забезпечення перевірки Рис. 6 будь-ким цілісності (немодифікованості) повідомлення m від користувача *A*, автентичності повідомлення m та автентичності відправника *A* полягає у наступному [9].

Користувач A зашифровує m на власному приватному ключі k_{prA}, а криптограму c він відправляє до користувача B. Для перевірки вказаних вище статусів, одержану криптограму c користувач B розшифровує на публічному ключі відправника k_{pbA}.

Розшифрувати криптограму c може B і будь-який інший користувач системи, навіть Криптоаналітик (що може проникнути в систему, або зареєструватися, як легальний користувач) які отримали доступ до публічного ключа k_{pbA}. Схематично, оскільки тільки A, і ніхто інший, має ключ k_{prA}, то факт розшифрування криптограми c на ключі k_{pbA} і «читабельності» відновленого повідомлення m, або співпадіння його з відкритою копією повідомлення, що прийшла із каналу (або була розшифрована на місці отримання за протоколом забезпечення конфіденційності) доводить: цілісність повідомлення m, автентичність повідомлення m та автентичність відправника A.

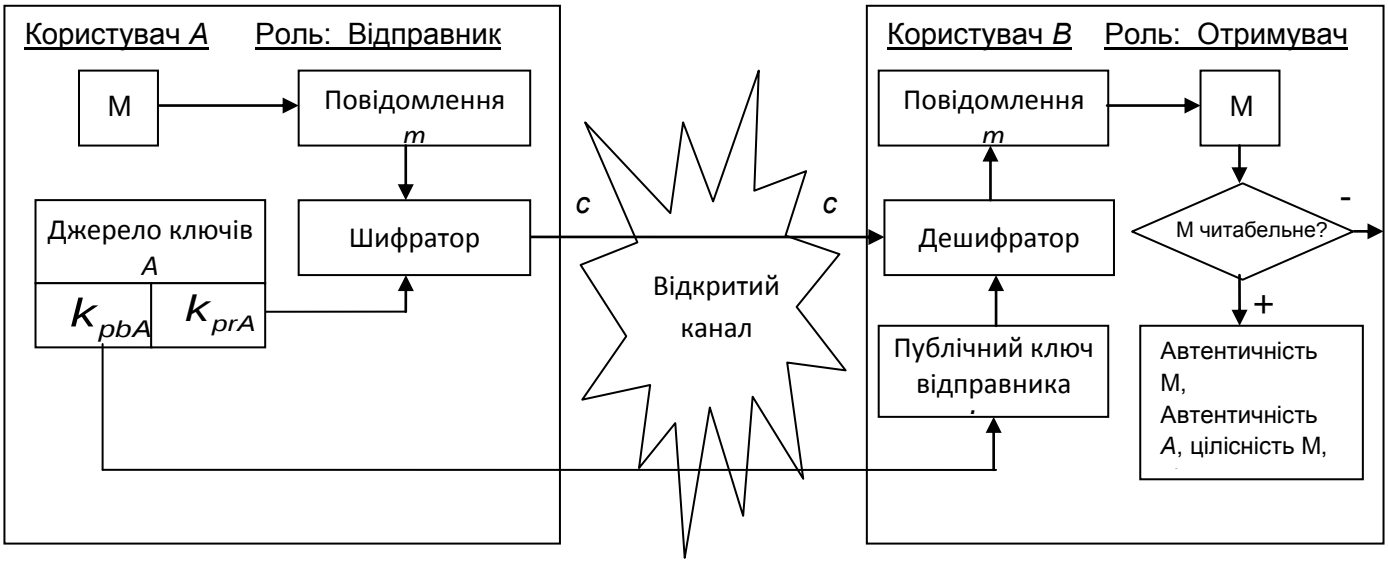

Рисунок 6 - Протокол перевірки цілісності M та автентичності A та M

Ніхто крім A не має приватного ключа k_{prA}, тому ніхто крім A не міг зашифрувати криптограму c так, щоби її можна було розшифрувати на публічному ключі k_{pbA}. Це доводить автентичність повідомлення m та автентичність відправника A, а також, цілісність m.

У протоколі, наведеному на Рис.6, є місце для критики, як, власне, і в будь-якому іншому (зараз не обговорюємо можливі загрози даному протоколу і сценарії їх реалізації). Один з перших недоліків тут - залежність витрат часу, потреби у обчислювальних ресурсах, як і продуктивності системи від обсягів висхідного повідомлення M та, відповідно, його цифрового подання m і криптограми c. Суттєво зменшити вплив цього недоліку на характеристики криптосистеми можна кардинально зменшивши обсяги даних, що піддаються алгебраїчним обчисленням у «асиметричних» шифраторах/дешифраторах. Для цього в протоколи вводять додатково операції стиснення даних з частковою втратою кількості інформації, що принципово не мають, або унеможливлюють виконання зворотного перетворення (що надавало би можливість відновити стиснений текст). Маються на увазі принципово односторонні перетворення висхідних даних m будь-якої довжини, такі, як хеш-суми (наприклад, MD5, SHA, тощо [5]) у вихідний рядок h заданої довжини - «дайджест» висхідного текста, повідомлення з високою ентропією (MD5 повертає, наприклад, «дайджест» довжини 128 двійкових символів). Такий рядок $h = hash(m)$, де $hash(m)$ позначає функцію $hash$-перетворення над цифровим образом m висхідного повідомлення M, однозначно виступає представником свого m і висхідного текста, повідомлення M. З огляду на це, значення h активно використовують у протоколах з криптоалгоритмами. Відомо, що у теорії і практиці хеш-сум присутнє негативне явище «колізії» - можливість і наявність інших текстів, m_1 скажімо, які дають точно таке ж значення $h = hash(m) = hash(m_1)$. Але позитивом тут є те, що для будь-якого m, що має осмислений текст M, імовірність осмислених, «читабельних» текстів m_1, з потрібними зловмиснику характеристиками і смислом є вкрай малою. Набагато вище імовірність знайти цифровий образ m_1 з «нечитабельним» текстом M_1 у вигляді набору випадкових символів алфавіту. Тому питання вирішується розробкою «гарних» хеш-алгоритмів та довжиною хеш-дайджеста [5]. Хоча і для випадкових текстів M_1, що дають колізію до заданого M, зловмисники можуть знайти своє застосування.

Варіант протоколу, що забезпечує перевірку цілісності та автентичності повідомлення M і автентичності відправника A, але без забезпечення конфіденційності повідомлення (існують і такі завдання) наведено на Рис. 7. Згідно цього сценарія, користувач A, що виступає в ролі відправника повідомлення M, не має наміру приховувати смисл M. Тобто, він не ставить завдання забезпечити конфіденційність документа M, зі змістом якого може ознайомитися будь-хто у середовищі вільного доступу. Проте, він бажає забезпечити цілісність документа і підтвердити перед будь-яким отримувачем B автентичність текста M і свою власну [9].

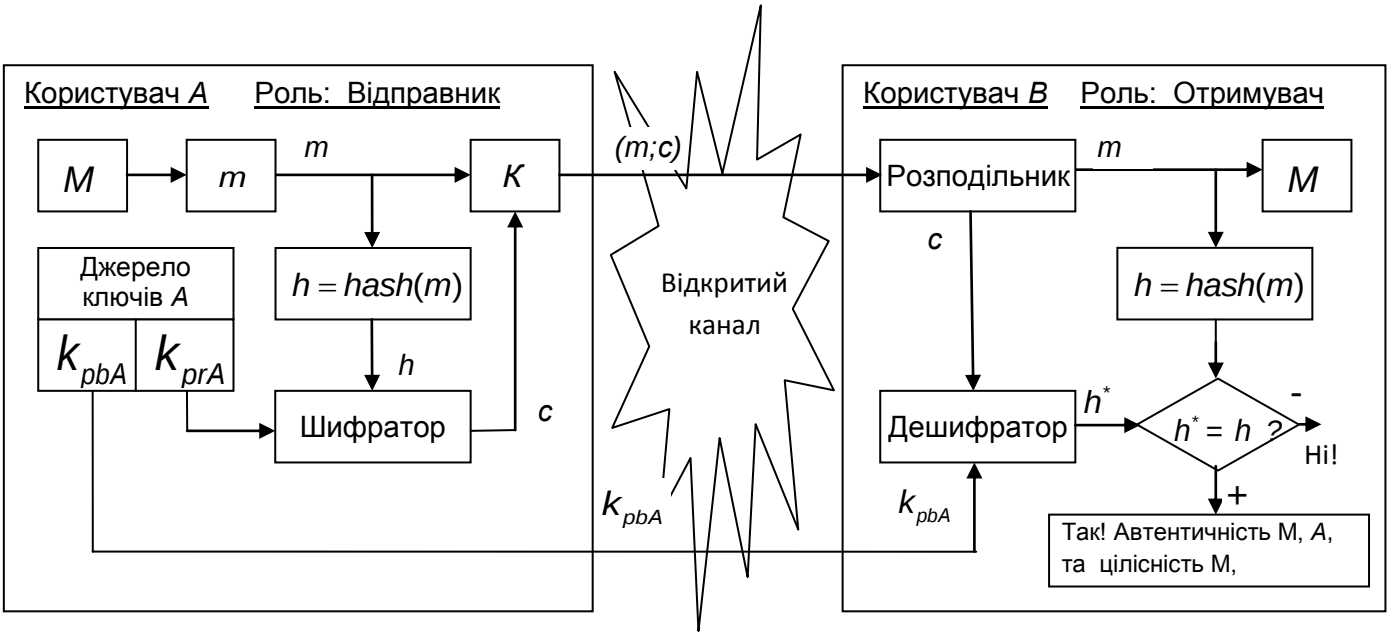

Рисунок 7 - Протокол перевірки цілісності та автентичності повідомлення M і автентичності відправника A (хеш), без конфіденційності

Це може бути, наприклад, відкритий наказ по організації, зі змістом якого мають ознайомитися працівники, які, проте, не можуть ні модифікувати його (внести непередбачені автором A зміни і порушити цілісність M), ні імітувати його - створити несправжній документ M від імені користувача A (порушуючи автентичність, справжність, достовірність документа M та автора A).

Відправник A, отримавши цифровий образ m повідомлення M, поєднує його з криптограмою c шляхом конкатенації (поєднання двох відповідних текстів) у блоці K для передачі цієї пари рядків символів $(m;c)$ через Відкритий

(незахищений) канал. Конкатенація (об'єднання) — операція склеювання об'єктів лінійної структури, зазвичай рядків символів. Наприклад, конкатенація слів «мікро» і «світ» дасть слово «мікросвіт» (https://uk.wikipedia.org/wiki).

Сам відкритий текст подається в каналі, власне цифровими символами m, і є доступним для прочитання будь-ким, зокрема, отримувачем B. Проте, його супроводжує криптограма c, яка є зашифрованою на приватному ключі k_{prA} відправника A хеш-сумою $h = hash(m)$ від цифрового образа m відкритого текста M. Цей «доданок» до канального повідомлення m і дозволяє отримувачеві виконати перевірку статусів, згаданих вище.

Так, наприклад, отримувач B розділяє у Розподільнику послання $(m;c)$, що прийшло із канала, на окремі компоненти m та c. За компонентою m він відновлює текст повідомлення M до форми, прийнятної для читання чи подальшого використання. Але перед цим мусить виконати перевірку. Для цього криптограму c він розшифровує у Дешифраторі на публічному ключі k_{pbA} відправника A, відновлюючи значення хеш-суми $h^* = hash(m)$ від цифрового образа m відкритого тексту M. Зірочкою тут позначено відновлене на боці отримувача B значення хеш-суми $hash(m)$, яке було захищене у відкритому каналі шифруванням і не могло попасти до рук зловмисника. З огляду на це h^* можна прийняти за своєрідний, невеликий за обсягом «еталон», що подає висхідний текст m. З іншого боку, цифровий образ m тексту M, що побував у відкритому каналі, міг бути модифікований, або ж, зовсім з'імітований зловмисником. Для перевірки таких порушень, отримувач B піддає компоненту m, що отримав із канала, хешуванню «на місці» і отримує своє власне значення хеш-суми $h = hash(m)$, яке порівнює із «еталонним» значенням h^*. За виконання умови $h^* = h$ отримувач B робить наступні висновки:

- порушення цілісності m (відповідно, тексту M) не виявлено і є високоімовірним, що воно відсутнє;

- текст M створено користувачем A і ніким іншим, оскільки піддається перевірці на його публічному ключі k_{pbA} і, відповідно, зашифрування h могло

бути виконано тільки на приватному ключі k_{prA} відправника A, якщо тільки цей ключ не є скомпрометований (не передавався іншим суб'єктам СІД, не був вкрадений зловмисником, тощо); це є ствердження автентичності, справжності, авторства відправника A;

- текст M є автентичним, справжнім, непідробленим, оскільки має автентичного автора - відправника A.

Після таких висновків отримувач B має всі підстави вважати достовірним відновлений текст документа M і використовувати його у подальшому.

У разі невиконання умови звірки хеш-сум $h^* = h$, отримувач B скасовує наведені вище висновки і вважає недостовірним, неавтентифікованим, або таким, що має порушення цілісності (модифікований, імітований, підроблений, тощо) відновлений текст документа M і відмовляється використовувати його у подальшому. Описаний сценарій за моделлю Рис. 7 є нічим іншим, як Протоколом постановки на документ M та верифікації Електронного Цифрового Підпису (ЕЦП). У даному випадку ЕЦП ставився на відкритий документ M і мав форму криптограми c (набору цифрових даних) від хеш-дайджеста цифрового образа m документа. Варто зауважити що вагу в цій гілці криптозахисту даних має не сам ЕЦП, а весь той комплекс задач криптозахисту, який має розв'язок і реалізацію завдяки використанню ЕЦП.

Варіант протоколу, що забезпечує перевірку цілісності та автентичності повідомлення і автентичності відправника, а також, забезпечує конфіденційність повідомлення у незахищеному відкритому каналі наведено на Рис. 8. Згідно цього сценарію, користувач A, що виступає в ролі відправника повідомлення M, має намір приховати смисл M від сторонніх суб'єктів СІД. Він ставить завдання забезпечити конфіденційність документа M, зі змістом якого може ознайомитися лише визначений ним суб'єкт, в даному разі - отримувач B. Він бажає забезпечити цілісність документа і підтвердити перед отримувачем B автентичність текста M і свою власну. Зі змістом M не може ознайомитися ніхто інший, окрім B. Отримувачу B додатково надаються засоби і механізми, що дозволяють виявити порушення цілісності M, та

пересвідчитися в автентичності документа та відправника. Будь-хто у середовищі вільного доступу не може непомічено ні модифікувати документ (внести непередбачені автором A зміни і порушити цілісність M), ні імітувати його - створити несправжній документ M від імені користувача A (порушуючи автентичність, справжність, достовірність документа M та автора A).

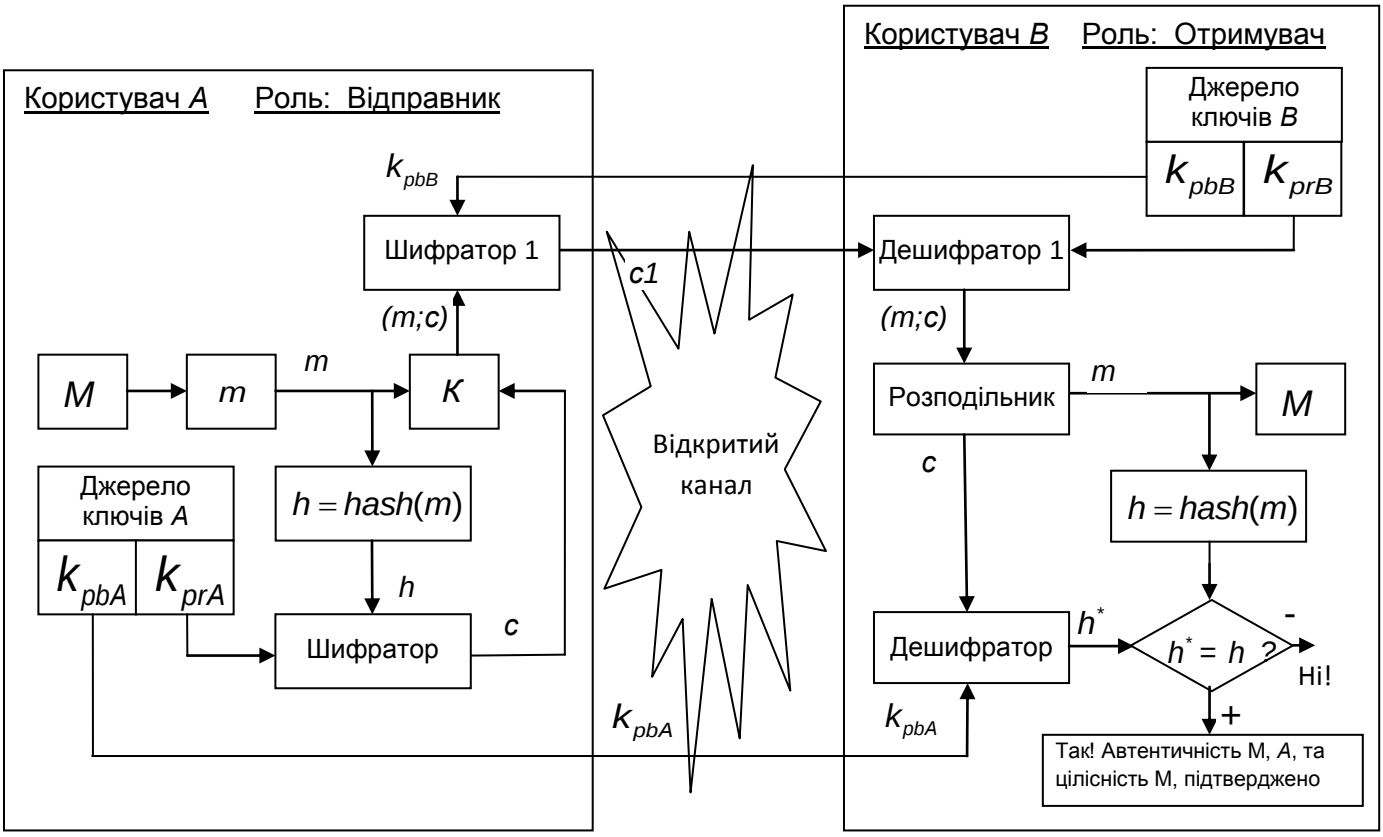

Рисунок 8 - Протокол перевірки цілісності та автентичності повідомлення M і автентичності відправника A та конфіденційності M у відкритому каналі

Протокол Рис. 8 доволі подібний до протоколу, представленого на Рис.7 і відрізняється від останнього наявністю функцій шифрування Шифратором 1 і розшифрування Дешифратором 1 пари наборів даних $(m;c)$, тобто - наявністю захищеного шифруванням каналу передачі повідомлень у формі криптограм $c1$, що і забезпечує конфіденційність при їх передачі через відкритий канал [9].

Відправник A, отримавши цифровий образ m повідомлення M, поєднує його з криптограмою c шляхом конкатенації (поєднання двох відповідних текстів) у блоці K для зашифрування цих даних на публічному ключі k_{pbB}

отримувача B і передачі відповідної криптограми $c1$ через Відкритий (незахищений) канал до отримувача B.

Тепер відкритий текст не подається в канал і не є доступним для прочитання будь-ким, окрім отримувача B. Цифровий образ m відкритого текста разом з криптограмою c (яка є зашифрованою на приватному ключі k_{prA} відправника A хеш-сумою $h = hash(m)$ від цифрового образа m) піддається шифруванню у Шифраторі 1 до отримання криптограми $c1$, яку передають через відкритий канал до отримувача B. «Доданок» c до повідомлення m і дозволяє отримувачеві B виконати перевірку статусів, згаданих вище, після розшифрування $c1$ Дешифратором 1 на власному приватному ключі k_{prB}.

Після відновлення Дешифратором 1 пари $(m;c)$, отримувач B розділяє у Розподільнику послання $(m;c)$, на окремі компоненти m та c. За компонентою m він відновлює текст повідомлення M до форми, прийнятної для читання чи подальшого використання. Але перед цим мусить виконати перевірку. Для цього криптограму c він розшифровує у Дешифраторі на публічному ключі k_{pbA} відправника A, відновлюючи значення хеш-суми $h^* = hash(m)$ від цифрового образа m відкритого тексту M. Зірочкою тут позначено відновлене на боці отримувача B значення хеш-суми $hash(m)$, яке було захищене у відкритому каналі подвійним шифруванням і не могло попасти до рук зловмисника. З огляду на це h^* можна прийняти за своєрідний, невеликий за обсягом «еталон», що подає висхідний текст m. З іншого боку, цифровий образ m тексту M, міг бути спотворений, змодифікований, або ж, зовсім з'імітований зловмисником (наприклад, атака «зловмисник посередині»). Для перевірки таких порушень, отримувач B піддає компоненту m, що отримав із канала, хешуванню «на місці» і отримує своє власне значення хеш-суми $h = hash(m)$, яке порівнює із «еталонним» значенням h^*. За виконання умови $h^* = h$ отримувач B робить наступні висновки:

- порушення цілісності m (відповідно, тексту M) не виявлено і є високоімовірним, що воно відсутнє;

- текст M створено користувачем A і ніким іншим, оскільки піддається перевірці на його публічному ключі k_{pbA} і, відповідно, зашифрування h могло бути виконано тільки на приватному ключі k_{prA} відправника A, якщо тільки цей ключ не є скомпрометований (не передавався іншим суб'єктам, СІД, не був вкрадений зловмисником, тощо); це є ствердження автентичності, справжності, авторства відправника A;

- текст M є автентичним, справжнім, непідробленим, оскільки має автентичного автора - відправника A та не має ознак порушення цілісності;

- текст M переданий через відкритий канал конфіденційно, оскільки був зашифрованим на публічному ключі отримувача B і розшифрованим на його приватному ключі, жоден інший суб'єкт не може цього зробити, оскільки не має у своєму розпорядженні такого ключа.

За таких висновків отримувач B має підстави вважати конфіденційним, цілісним і достовірним відновлений текст документа M і використовувати його у подальшому.

У разі невиконання умови звірки хеш-сум $h^* = h$, отримувач B скасовує наведені вище висновки і вважає недостовірним, неавтентифікованим, або таким, що має порушення цілісності (змодифікований, імітований, підроблений, тощо) відновлений текст документа M і відмовляється використовувати його у подальшому, незважаючи на виконання умов конфіденційності передачі документа.

Описаний сценарій за моделлю Рис. 8 є Протоколом постановки на документ M та верифікації Електронного Цифрового Підпису (ЕЦП). У даному випадку ЕЦП теж ставився на відкритий документ M і мав форму криптограми c (набору цифрових даних) від хеш-дайджеста цифрового образа m документа. Задля забезпечення конфіденційності документа у відкритому каналі, він разом із ЕЦП піддавався зашифруванню на публічному ключі k_{pbB} , а розшифрувати його міг тільки отримувач B на своєму приватному ключі.

Використовуючи такі пари ключів за певними алгоритмами і протоколами, кожний користувач $СІД_j$ відповідно до моделі Рис.4, може

виконати практично весь комплекс згаданих вище завдань із захисту даних в ІС в обох напрямках, а саме: забезпечити конфіденційність своїх відправлень іншим користувачам, отримати конфіденційні повідомлення від інших учасників інформаційного обміну; забезпечити автентифікацію власних відправлень та перевірку автентичності повідомлень від інших; забезпечити свою власну автентифікацію та перевірку автентичності інших користувачів; забезпечити перевірку цілісності власних відправлень для отримувачів та виконати перевірку цілісності повідомлень від інших відправників.

Атаки на інформаційні системи поділяють на два великих класи: пасивні атаки, активні атаки. Пасивні атаки – це атаки зловмисника на інформаційні ресурси в ІС з метою підслухати, перехопити, прочитати, вкрасти, скопіювати чужі дані, тексти, документи – об’єкти інформаційної діяльності ОІД, непомітно для їх власників чи суб’єктів інформаційної діяльності СІД (чужі - такі, що йому не призначені, ознайомитися з якими він не має права). Таку атаку зловмисник, як правило, намагається виконати без помітного фізичного впливу на канали комунікації і каналоутворююче обладнання, та без помітного логічного впливу на ОІД, уникаючи зміни, модифікації, фальсифікації, імітації текстів ОІД (бо це веде до порушення цілісності ОІД, до суттєвого підвищення ймовірності виявлення такого втручання та викриття нападника). Зловмисник розробляє для пасивної атаки відповідні сценарії її виконання. Додатково, супутньою метою зловмисника у такому сценарії є якомога довше зберегти факт виконання такої атаки непоміченим.

Моделі і Протоколи криптосистем подано тут у чистому і схематичному вигляді, без розгляду можливих більш витончених загроз, моделей зловмисника, сценаріїв виконання атак. Звісно, ці питання потребують свого ретельного розгляду, аналізу і викликають потребу у обговоренні і дискусіях на відповідні теми. Більшість подібних питань і обговорень вже знайшли своє відбиття у широко доступній літературі, до якої автор наразі і відсилає зацікавленого читача, наприклад [4,5,6]. Не можна сказати, що ці джерела дають вичерпну відповідь на всі питання про сучасний стан справ у галузі

захисту інформації (більш широкий перелік джерел займає декілька тисяч позицій, це і книги, і статті у фахових виданнях, тощо). Гарні результати дає пошук в Інтернет, який дозволяє визначити чіткі посилання на справжню фахову літературу (паперову, друковану) з тих, чи інших питань, яку варто знаходити і читати.

А ми перейдемо далі до математичних засад криптоперетворень в асиметричних алгоритмах, без більш-менш чіткого уявлення про які буде важко зрозуміти процедури, технології та тонкощі реалізації розглянутих вище моделей і Протоколів, та ту роль, яку грають в них такі відомі асиметричні криптосистеми, як: алгоритми Діффі-Хеллмана, Ель-Гамаль, алгоритм RSA.

4.1. Контрольні запитання

4.1.1 Що таке асиметрична криптосистема (АКС)?

4.1.2 Що таке приватний і публічний ключі в АКС?

4.1.3 Яка головна властивість асиметричної криптосистеми?

4.1.4 Опишіть модель асиметричної криптосистеми.

4.1.5 Де і як можуть зберігатися приватний і публічний ключі АКС?

4.1.6 Опишіть Протокол забезпечення конфіденційності повідомлення в АКС.

4.1.7 Опишіть Протокол перевірки цілісності та автентичності повідомлення M та відправника A в АКС.

4.1.8 Опишіть Протокол перевірки цілісності та автентичності повідомлення M і автентичності відправника A (з hesh), без конфіденційності.

4.1.9 Опишіть протокол перевірки цілісності та автентичності повідомлення M і автентичності відправника A та конфіденційності M у АКС.

4.1.10 Опишіть комплекс завдань із захисту даних в ІС в обох напрямках.

4.1.11 Яка основна і додаткова мета пасивної атаки на ІС?

5. МАТЕМАТИЧНІ ЗАСАДИ АСИМЕТРИЧНИХ КРИПТОАЛГОРИТМІВ

Матеріал цього розділу надзвичайно важливий для розуміння принципів побудови і функціонування сучасних асиметричних криптоалгоритмів і систем захисту даних. Він не є складний. Незвичний - так! Але не складний. Автор намагався максимально спростити подачу матеріалу і обмежити його найнеобхіднішими відомостями і практичними Вправами. Зважаючи на це, автор наперед перепрошує у фахівця і підготовленого читача за можливі неточності і нестрогий виклад матеріалу, який вимагає суворішого підходу. Зацікавленому читачеві можна порекомендувати озброїтися олівцем і аркушем, і читати цей розділ «практично», намагаючись повторити те, що тут викладено, виконати ті Вправи, які наведені нижче, самостійно міняти дані завдань у Вправах і повторно їх виконати [10]. Всі ці відомості широко опубліковані в літературі та Інтернет. Тому з пошуком відповідей на можливі запитання не має бути проблем. Перелік рекомендованих джерел наведено в кінці цього Навчального посібника.

Знову мусимо згадати про скінченний алфавіт A_q, який являє собою скінченну множину знаків, символів, кількість яких складає q дискретних елементів, і які несуть в собі певну кількість інформації. Згадаємо, що букви, символи – це цифри з алфавіту, слова – це цифри з алфавіту, речення – це цифри з алфавіту, взагалі, тексти - це цифри із алфавіту. Справа лише у кількості цифр q в алфавіті та n у ланцюжках, якими подають букви, символи, слова, речення, тексти, тощо. Символи у алфавіті A_q є дискретні, їх можна розрізнити, їх кількість чітко обмежена величиною q. Одна із форм подання елементів множини A_q - суть цілі числа, цифри. З огляду на потреби завдань криптографії, у межах захисту інформації, над ними необхідно вміти виконувати різні операції перетворення, які називають «арифметичні операції».

Щоби набути таких можливостей, до розгляду залучають такий відомий математичний об’єкт, як скінченне поле Галуа - $GF(q)$ [5,6,9,10]. У теорії чисел, як розділі математики, існує важливий математичний об’єкт - скінченне поле

Галуа, яке саме по собі є представником ряду алгебричних структур, що базуються на скінченному алфавіті A_q, на якому визначають ряд перетворень над його елементами, операцій над ними, задають ряд аксіоматичних вимог до їх властивостей і властивостей операцій над ними. У цьому сенсі, скінченне поле Галуа $GF(q)$, що оперує власним алфавітом з цілим набором добре вивчених його властивостей, так і властивостей його елементів (символів, цифр, тощо) має певну подобу, схожі риси з алфавітом A_q, ланцюжками символів якого (цифр) подають повідомлення в ІС. Тому символи алфавіту A_q співставляють із символами-елементами $GF(q)$.

Перше, з чим нам доведеться визначатися, це величина q, і тут вагу має не стільки її значення, скільки її арифметичні властивості. Мається на увазі така властивість числа q як його простота $q = p$ (p - просте число, таблиця простих до 1000 наведена у Додатку А), чи його розкладеність у добуток простих множників $q = p_1^{i_1} \bullet p_2^{i_2} \bullet p_3^{i_3} \ldots p_j^{i_j} \ldots$, де p_j - просте число, таке, що має лише два дільники: саме число p_j та одиницю, а i_j - цілі числа. Наприклад, $q = p = 83$ - просте число, яке ділиться лише на себе і на 1. Наприклад, $q = 256 = 2^8$ та $q = 255 = 3 \bullet 5 \bullet 17$ є розкладені числа, де 2, 3, 5, 17 - прості числа. У такому разі мову ведуть про структуру числа q, що подає потужність множини алфавіту A_q (кількість елементів в алфавіті). Вибір структури числа q впливає на визначення і спосіб виконання операцій над елементами Алфавіту, або множини $GF(q)$ та на форми подання самих елементів множини. Не строго кажучи, за іншими властивостями, поля $GF(q)$ та $GF(p)$ де q - розкладене, а p - просте, в основному подібні.

За визначенням, при q - розкладеному, всі елементи множини $GF(q)$ подають у формі поліномів-остач за модулем деякого незвідного полінома $P(x)$ від формальної змінної x (за $\mathrm{mod} P(x)$) [5,6,9,10]. Це дуже зручно та ефективно для обчислювальних систем, з огляду на можливість застосувати таку структуру q, як ціла степінь z «двійки»: $q = 2^z$ (див. приклад вище).

При $q = p$ (p - просте число), всі елементи множини $GF(p)$ подають у формі чисел-остач за модулем p (за $\mathrm{mod}\, p$). Відповідно, і всі арифметичні операції над елементами $A_q = A_p$ виконують за $\mathrm{mod}\, p$ [5,6,9,10]. Розглянемо для однозначності поле $GF(p)$, потужність множини якого подається простим числом p.

Визначення: скінченним полем Галуа $GF(p)$ називають скінченну множину що складається із p дискретних елементів $\alpha_i \in GF(p)$, $i = 0, 1, 2, \ldots (p-1)$, (символ «$\in$» означає належність елементів α_i множині $GF(p)$) будь-якої фізичної природи, які можна розрізнити один від одного і перелічити, з заданими на них двома прямими, замкненими відносно множини, операціями. Ці операції умовно називають «складанням», позначимо «+» і «множенням», позначимо «*», або «», оскільки вони певним чином схожі зі звичайними складанням і множенням, але не обов'язково співпадають із ними.

Бінарну операцію над парою елементів $\alpha \in GF(p)$ та $\beta \in GF(p)$ розумітимемо в узагальненому сенсі (1),

$$(\alpha)Оп.j(\beta) = (\beta)Оп.j(\alpha) = \delta, \qquad (1)$$

де *On.j* - символ операції з ім'ям (номером) j , як певний спосіб постановки деякого елемента $\delta \in GF(p)$ множини $GF(p)$ у відповідність двом елементам α та β тої ж самої множини (властивість замкненості операції, див. Рис. 9) Так, наприклад, це може бути операція додавання, або операція множення (умовні назви) [10].

Тоді відношення на виразах (1) можна переписати, як

$$\alpha + \beta = \beta + \alpha = \delta \text{ , або } \alpha * \beta = \beta * \alpha = \delta \qquad (2)$$

При цьому не виключено, що може відбутися $\delta = \alpha$ або $\delta = \beta$. Прикладні аспекти скінченних полів $GF(p)$, що нас цікавлять, вимагають виконання

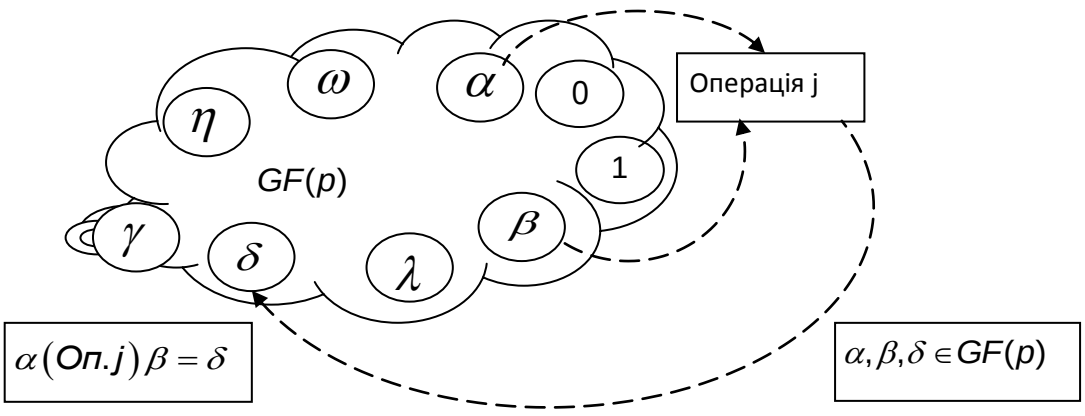

Рисунок 9 - Узагальнене поняття замкненої бінарної операції [10]

аксіоми про комутативність операцій, що відображено у виразах (1) і (2), а також ряду інших відомих нам аксіом алгебри. Таких, наприклад, як асоціативний або дистрибутивний закони однієї операції щодо іншої:

$$(\alpha+\beta)+\delta=\alpha+(\beta+\delta) \text{ або } (\alpha+\beta)*\delta=\alpha*\delta+\beta*\delta \ . \qquad (3)$$

У кожній такій множині $GF(p)$ присутні два особливих елемента: елемент зі властивостями нуля (позначимо його як «0»), і елемент з властивостями одиниці (позначимо його як «1») такі, що для кожного елемента $\alpha \in GF(p)$ є справедливими наступні твердження

$$\alpha+0=\alpha \ ,$$

$$\alpha*0=0 \ , \qquad (4)$$

$$\alpha*1=\alpha \ .$$

Елементи $0,1 \in GF(p)$ є єдиними у множині $GF(p)$ із властивостями (4).

Операції, зворотні названим - «Віднімання» і «Ділення», прямо не визначені. Але вони задаються процедурно, шляхом визначення особливих,

«Обернених» елементів скінченного поля $GF(p)$. Так, до кожного елементу $\beta \in GF(p)$ визначено елемент $(-\beta) \in GF(p)$, обернений за додаванням, такий, що

$$\beta + (-\beta) = 0 \ . \qquad (5)$$

Цим самим (5) задається операція унарного типу над елементами множини $GF(p)$, з одним операндом. А до кожного ненульового елементу , $\lambda \neq 0$, $\lambda \in GF(p)$ визначений елемент $(\lambda^{-1}) \in GF(p)$, $\lambda^{-1} \neq 0$, обернений (зворотний) за множенням, такий, що

$$\lambda * (\lambda^{-1}) = 1 \ . \qquad (6)$$

При цьому, операцію віднімання елемента $\beta \in GF(p)$ від $\alpha \in GF(p)$ з урахуванням визначення (5) можна виконати за наступною процедурою

$$\alpha - \beta = \alpha + (-\beta) = \delta \ , \ \delta \in GF(p), \qquad (7)$$

а операцію ділення елемента $\alpha \in GF(p)$ на $\beta \in GF(p)$, $\beta \neq 0$ з урахуванням визначення (6) можна виконати як

$$\alpha : \beta = \alpha / \beta = \alpha * (\beta^{-1}) = \eta \ , \ \eta \in GF(p) . \qquad (8)$$

З виразу (7) випливає, що для того, щоб відняти β від α необхідно спочатку знайти $(-\beta)$, елемент обернений за додаванням до β, і скласти його з α. А з виразу (8) випливає, що для того, щоб розділити α на β, необхідно спочатку знайти (β^{-1}), елемент обернений за множенням до β, і помножити α на нього. Відносно рівності (8) необхідно зауважити, що дроби в скінченних полях не визначені, тому перші два вирази рівності можна розглядати лише як

спосіб символьного запису бажаної арифметичної дії - ділення. А третій вираз з (8) - це вже алгоритм (процедура) виконання ділення. Зауважимо також, що саме визначення операції ділення, як процедури, виключає поділ на нуль, знімаючи пов'язані з цією ситуацією проблеми.

Дане визначення скінченного поля GF (p) не є строгим, але є достатнім для першого ознайомлення з його основними властивостями, що мають прикладне значення в криптографії [5,6,9,10].

Як вже відмічалося, елементи поля можуть мати будь-яку фізичну природу. Головне те, щоби їх можна було скласти до купи у множину $GF(p)$, щоби вони утворили певну сукупність елементів, які мають певні спільні риси. Вони мають надавати можливість перелічити їх, тобто, з кожним з них пов'язати певне число $i = 0,\ 1,\ 2,\ldots,(p-1)$.

Наприклад, для $p = 19$, $A_{19} = \{0,1,2,3,\ldots,18\}$, це і є той алфавіт елементів, з яким оперує $GF(19)$.

Наприклад, для $p = 83$, $A_{83} = \{0,1,2,3,\ldots,82\}$, це і є той алфавіт елементів, з яким оперує $GF(83)$.

Для $GF(p)$, де p - просте число, виконання двох прямих арифметичних операцій (додавання і множення) задають як і у звичайній арифметиці, але з редукцією результату операції до меж множини $GF(p)$ (див. Рис. 9) шляхом взяття того результату за $\mathrm{mod}\, p$ (читати, «взяття за модулем p»). За дотримання замкненості операції таким чином, виконуються всі аксіоми і умови, наведені вище у визначенні поля, рівності (1)-(8).

Операція взяття цілого числа a за $\mathrm{mod}\, p$ (форма запису 1 на Рис. 10,б) полягає у багатократному відніманні модуля p від a до отримання r , що підпорядковується умовам $0 \le r < p$ [10]. А саме, запис $a \ \mathrm{mod}\, p = r$ означає $a - j \bullet p = r$, де j - деяке ціле число і виконується умова $0 \le r < p$ (форма запису 2 на Рис. 10,б). На Рис. 10, а) подана інша, більш відома форма цієї операції - ділення цілого числа a на ціле p з отриманням остачі $0 \le r < p$ від ділення [10].

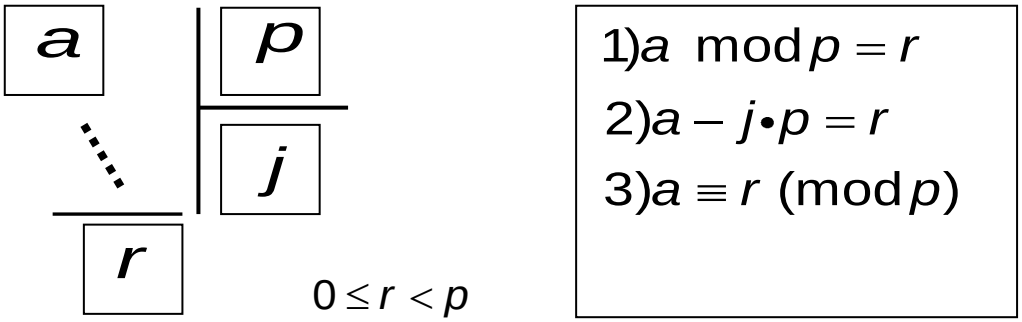

Рисунок 10 - Форми подання операції $a \bmod p = r$

Власне, ділення цілих чисел є скороченою формою запису саме багатократного віднімання модуля p від a. Практично у всіх випадках, нас цікавить саме r як результат цієї операції. Ця операція має своє подання і в теорії чисел у формі зрівняння $a \equiv r \pmod p$, яка часто використовується в криптографії, дивись Рис.10, б), форма 3 запису [10].

Помітимо, що $p = 2$ є простим числом (ділиться на себе і на 1), а найменше за потужністю алфавіту скінченне поле Галуа $GF(2)$ є відомим нам під ім'ям «двійкова арифметика», або «двійкова система числення» і є лише частковим випадком загальної теорії скінченних полів $GF(q)$.

Як вже відмічено вище, у множині кожного поля $GF(p)$ обов'язково є два особливих елементи із властивостями (4). Подивимося на $GF(2)$, де множина виглядає як $A_2 = \{0,1\}$ і складається саме і тільки із цих двох елементів: 0 та 1. Вище були довільно наведені приклади алфавітів A_{19} та A_{83} для $GF(19)$ та $GF(83)$, відповідно. Як бачимо, їх склад містить ті ж самі два елементи 0 та 1 із тими ж властивостями (4). І у кожній з цих множин, узятих для прикладу, немає жодних інших елементів, що мали б такі ж властивості (4). У теорії чисел доведено теоремою у загальному випадку єдиність цих елементів у множині поля. Звернути увагу на це було важливо, оскільки саме єдиність 0 і 1 у полях $GF(q)$ та $GF(p)$ забезпечує однозначність виконання операцій над їх елементами.

За структурою, поле $GF(p)$ містить дві скінченні алгебраїчні групи (за кількістю основних операцій): адитивна група A_p - це сама множина елементів поля A_p з однією заданою на ній операцією додавання «+», та мультиплікативна група M_p - це множина всіх ненульових елементів $\alpha_i \neq 0$ із поля A_p (M_p є підмножиною A_p такою, що не містить 0) з однією заданою на ній операцією множення «•». Оскільки M_p не містить 0, то кожний елемент $\alpha_i \in M_p$ має свій обернений за множенням елемент $\alpha_i^{-1} \in M_p$ [10].

Так, наприклад, для $p = 19$ адитивною групою $GF(19)$ є сама множина $A_{19} = \{0,1,2,3,\ldots,18\}$ разом із операцією додавання «+» за $(\mathrm{mod}19)$. А мультиплікативною групою $GF(19)$ є множина $M_{19} = \{1,2,3,\ldots,18\}$, що є підмножиною A_{19} (без елемента 0), разом з заданою на ній операцією множення «•» за $(\mathrm{mod}19)$.

Відповідно, наприклад, для $p = 83$ адитивною групою $GF(83)$ є сама множина $A_{83} = \{0,1,2,3,\ldots,82\}$ разом із операцією додавання «+» за $(\mathrm{mod}83)$. А мультиплікативною групою $GF(83)$ є множина $M_{83} = \{1,2,3,\ldots,82\}$, що є підмножиною A_{83} (без елемента 0), разом з заданою на ній операцією множення «•» за $(\mathrm{mod}83)$.

Обидві групи, A_p та M_p поля $GF(p)$, різною мірою активно використовуються у сучасних асиметричних криптосистемах. Розглянемо трохи докладніше мультиплікативну групу M_p, оскільки саме її властивості було використано у найбільш знакових асиметричних криптоалгоритмах (Діффі-Хеллмана, Ель-Гамаль, RSA). Всі елементи $\alpha_i \in M_p$ (нагадаємо, що $\alpha_i \neq 0$ та одночасно з тим $\alpha_i \in GF(p)$) мають своє подання у формі степенів так званого первісного (первинного, простого - prime, eng) елемента w:

$$\alpha_i \equiv w^j (\mathrm{mod}\, p) \quad \text{для } j = 0,1,2,3,\ldots,(p-1). \qquad (9)$$

У російськомовній літературі за w закріпилася назва - примітивний елемент. За формою 2 подання з Рис. 10, б) можна записати вираз (9) у звичному алгебричному вигляді:

$$\alpha_i = w^j - tp \quad \text{для} \quad j = 0,1,2,3,\ldots,(p-1), \tag{10}$$

де t - ціле число, що враховує кількість цілих входжень модуля p у значення w^j, а α_i - остача від t - кратного віднімання p від w^j. Первісний елемент $w \in GF(p)$ - це елемент, що має мультиплікативний порядок $_{\min} j = (p-1)$. А мультиплікативний порядок елемента w взагалі це мінімальне значення $_{\min} j \neq 0$, для якого

$$w^{(\min j)} \equiv 1 \,(\mathrm{mod}\, p). \tag{11}$$

Зрівняння (11) у звичному алгебричному вигляді можна розгорнути так

$$w^{(\min j)} - tp = 1. \tag{12}$$

Вирази (11) та (12) є у певному сенсі еквівалентними, оскільки трохи різними мовами висловлюють одну і ту ж саму властивість: вираз (11) - мовою теорії чисел, а (12) - мовою звичної алгебри (нагадаємо, що за визначенням, взяття за $\mathrm{mod}\, p$ є багатократне віднімання модуля p). Тож, якщо для $w \in GF(p)$ виконується $_{\min} j = (p-1)$, $_{\min} j \neq 0$, то w є первісний елемент $GF(p)$ і всі його степені w^j для $j = 1,2,3,\ldots,(p-1)$ пробігають однократно значення всіх елементів мультиплікативної групи M_p (нагадаємо, всі вони ненульові, див. приклади вище). Значення первісного елемента $w \in GF(p)$ якраз і полягає у тому, що через всі цілі степені $j = 1,2,3,\ldots,(p-1)$ одного елемента w можна подавати всі ненульові елементи $GF(p)$ у вигляді $(w^j) \mathrm{mod}\, p$. Це дає

конструктивні виходи на виконання мультиплікативних операцій над елементами M_p (ненульовими елементами $GF(p)$): обернення, множення, ділення, піднесення до степені.

Розглянемо для прикладу послідовні піднесення до степені $j = 0,1,2,3,\ldots,(p-1)$ елементів M_7 із $GF(7)$, де $p = 7$ і зведемо результати до Таблиці 5.1 [10]. Очевидно, що $A_7 = \{0,1,2,3,\ldots,6\}$, а елементи $M_7 = \{1,2,3,\ldots,6\}$ внесені у перший стовпчик «Елемент a» Таблиці 5.1. Рядки Таблиці 5.1 послідовно містять всі передбачені степені $j = 0,1,2,3,\ldots,6$ відповідних елементів. Із Таблиці 5.1 можна побачити, що для різних елементів $M_7 = \{1,2,3,\ldots,6\}$ порядок $\min j \neq 0$ набуває різних значень. Так, наприклад, елемент 1 має порядок $\min j = 1$, елементи 2 і 4 мають порядок $\min j = 3$, елементи 3 і 5 мають порядок $\min j = 6$, а елемент 6 має порядок $\min j = 2$. Таким чином, лише два елементи $3,5 \in GF(7)$ мають порядок $\min j = (p-1) = (7-1) = 6$, звідки робимо висновок, що елементи 3 та 5 є первісними елементами $GF(7)$ і будь-який з них можна використовувати у цій якості при роботі у скінченному полі $GF(7)$. У Таблиці 5.1 відповідні рядки вбрано у червону рамку. Там же, клітини у рядках до першої одиниці (за виразом (11)) виділено темним кольором. Кількість темних клітин у відповідному рядку таким графічним чином, вказує на мультиплікативний порядок елемента $\min j \neq 0$. Так от, множина результатів послідовних піднесень будь-якого елемента $a \neq 0$ у степені, до першої одиниці в рядку, має назву «мультиплікативний цикл», або, просто - цикл елемента a. У Таблиці 5.1 цикли відповідних елементів відмічені темним кольором. Довжина цикла елемента співпадає з його мультиплікативним порядком $\min j \neq 0$. Бачимо, що тільки для первісних елементів 3 і 5 довжина цикла та порядок набувають значення $\min j = (p-1) = (7-1) = 6$. Первісні елементи утворюють «довгий» цикл.

Остання колонка Таблиці 5.1 що має заголовок a^6 демонструє на кожному елементі $a \in M_7$ дію малої теореми Ферма: $a^{p-1} \equiv 1 \bmod p$. А друга

колонка Таблиці 5.1, що має заголовок $a^0 = a^{p-1}$ демонструє на кожному елементі $a \in M_7$ точку завершення чергового цикла і точку перетинання циклів. У непервісних елементів M_7 є кілька коротких циклів, поки у первісного елемента формується єдиний «довгий» цикл довжиною $_{\min} j = p - 1 = 7 - 1 = 6$.

Таблиця 5.1 - Мультиплікативні цикли елементів M_7 із $GF(7)$

$p = 7$	a^j, $j = 1, 2, 3, \ldots, p - 1$						
Елемент a	$a^0 = a^{p-1}$	a^1	a^2	a^3	a^4	a^5	a^6
1	1	1	1	1	1	1	1
2	1	2	4	1	2	4	1
3	1	3	2	6	4	5	1
4	1	4	2	1	4	2	1
5	1	5	4	6	2	3	1
6	1	6	1	6	1	6	1

У Таблиці 5.1 стовпчик із заголовком $a^0 = a^{p-1}$ містить тільки 1-ці. Очевидно, що $a^0 = 1$ для будь-якого елемента a, та може здатися не так очевидним, що $a^{p-1} = 1$. У зв'язку з цим, нагадаємо, що операції тут виконуються за $\bmod 7$. Тому мусимо записати більш строго $a^{7-1} \equiv 1 (\bmod 7)$. Взагалі, цей факт є відбиттям основної теореми теорії чисел - малої теореми Ферма, яка набула великого значення у прикладних питаннях криптографії

$$a^{p-1} \equiv 1 (\bmod p). \qquad (13)$$

Тепер бачимо (Табл.5.1), що цикли елементів завершуються 1-цею і повторюються знов і знов, навіть цикли первісних елементів (довгі цикли) повторюються, якщо продовжити ряд степенів $j = 1, 2, 3, \ldots, (p-1)$ за межі $(p-1)$, для даного прикладу $j = 7, 8, 9, \ldots$ і так далі.

Оскільки $_{\min} j = (p-1) = 6$ має розкладення на прості множники $6 = 1 \cdot 2 \cdot 3$, то всі можливі дільники числа $(p-1) = 6$, такі як 1, 2, 3, 6 задають очікувані значення довжин циклів і порядків елементів $GF(7)$. Первісні елементи порядку $_{\min} j = 6$ ми вже визначили вище. Інші дільники $_{\min} j = (p-1) = 6$, такі як 1, 2, 3 задають всі непервісні елементи $a \in GF(7)$, що мають порядки 1, 2, 3.

Бачимо, що кожний цикл має точку замикання на 1-ці, перетинаючи яку він повторюється до нескінченної кількості разів. І тільки у довгі цикли, цикли первісних елементів, по одному разу входить кожний ненульовий елемент із $GF(7)$. В інших циклах не вистачає деяких елементів M_7 із $GF(7)$. Тому саме первісний елемент $3 \in GF(7)$, або $5 \in GF(7)$ однозначно задає мультиплікативну групу M_7 і може сам її представляти в мультиплікативних операціях поля.

Розглянемо інший приклад послідовних піднесень до степені $j = 1,2,3,\ldots,(p-1)$ елементів M_{19} із $GF(19)$, де $p = 19$ і зведемо результати до Таблиці 5.2 [10]. Очевидно, що $A_{19} = \{0,1,2,3,\ldots,18\}$, а елементи $M_{19} = \{1,2,3,\ldots,18\}$ внесені у перший стовпчик «а» Табл. 5.2. Рядки Таблиці 5.2 послідовно містять всі передбачені степені $j = 1,2,3,\ldots,18$ відповідних елементів M_{19}, крім 1-ці, яка у будь-якій степені дає 1-цю. Із Таблиці 5.2 можна побачити, що для різних елементів $M_{19} = \{1,2,3,\ldots,18\}$ порядок $_{\min} j \neq 0$ набуває різних значень. Так, наприклад, елемент 1 має очевидний порядок $_{\min} j = 1$ (тому він в Табл.5.2 не занесений).

Елементи $2, 3, 10, 13, 14, 15 \in GF(19)$ мають порядок і довжину цикла $_{\min} j = (p-1) = (19-1) = 18$, тому вони є первісними елементами $w \in GF(19)$ і будь-який з них можна використовувати у цій якості при роботі у скінченному полі $GF(19)$. Оскільки $_{\min} j = (p-1) = 18$ має наступне розкладення на прості множники $18 = 1 \cdot 2 \cdot 3 \cdot 3$, то всі можливі дільники числа $(p-1) = 18$, такі як 1, 2, 3, 6, 9, 18 задають очікувані значення довжин циклів і порядків елементів $GF(19)$. Первісні елементи порядку 18 ми вже визначили вище, інші дільники $_{\min} j = (p-1) = 18$, такі як 1, 2, 3, 6, 9 задають всі непервісні елементи $\alpha \in GF(19)$.

Таблиця 5.2 - Мультиплікативні цикли елементів M_{19} із $GF(19)$

j	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**
a	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
2	**2**	**4**	**8**	**16**	**13**	**7**	**14**	**9**	**18**	**17**	**15**	**11**	**3**	**6**	**12**	**5**	**10**	**1**
3	**3**	**9**	**8**	**5**	**15**	**7**	**2**	**6**	**18**	**16**	**10**	**11**	**14**	**4**	**12**	**17**	**13**	**1**
4	**4**	**16**	**7**	**9**	**17**	**11**	**6**	**5**	**1**	4	16	7	9	17	11	6	5	1
5	**5**	**6**	**11**	**17**	**9**	**7**	**16**	**4**	**1**	**5**	**6**	**11**	**17**	**9**	**7**	**16**	**4**	**1**
6	**6**	**17**	**7**	**4**	**5**	**11**	**9**	**16**	**1**	**6**	**17**	**7**	**4**	**5**	**11**	**9**	**16**	**1**
7	**7**	**11**	**1**	**7**	**11**	**1**	**7**	**11**	**1**	**7**	**11**	**1**	**7**	**11**	**1**	**7**	**11**	**1**
8	**8**	**7**	**18**	**11**	**12**	**1**	**8**	**7**	**18**	**11**	**12**	**1**	**8**	**7**	**18**	**11**	**12**	**1**
9	**9**	**5**	**7**	**6**	**16**	**11**	**4**	**17**	**1**	**9**	**5**	**7**	**6**	**16**	**11**	**4**	**17**	**1**
10	**10**	**5**	**12**	**6**	**3**	**11**	**15**	**17**	**18**	**9**	**14**	**7**	**13**	**16**	**8**	**4**	**2**	**1**
11	**11**	**7**	**1**	**11**	**7**	**1**	**11**	**7**	**1**	**11**	**7**	**1**	**11**	**7**	**1**	**11**	**7**	**1**
12	**12**	**11**	**18**	**7**	**8**	**1**	**12**	**11**	**18**	**7**	**8**	**1**	**12**	**11**	**18**	**7**	**8**	**1**
13	**13**	**17**	**12**	**4**	**14**	**11**	**10**	**16**	**18**	**6**	**2**	**7**	**15**	**5**	**8**	**9**	**3**	**1**
14	**14**	**6**	**8**	**17**	**10**	**7**	**3**	**4**	**18**	**5**	**13**	**11**	**2**	**9**	**12**	**16**	**15**	**1**
15	**15**	**16**	**12**	**9**	**2**	**11**	**13**	**5**	**18**	**4**	**3**	**7**	**10**	**17**	**8**	**6**	**14**	**1**
16	**16**	**9**	**11**	**5**	**4**	**7**	**17**	**6**	**1**	**16**	**9**	**11**	**5**	**4**	**7**	**17**	**6**	**1**
17	**17**	**4**	**11**	**16**	**6**	**7**	**5**	**9**	**1**	**17**	**4**	**11**	**16**	**6**	**7**	**5**	**9**	**1**
18	**18**	**1**	**18**	**1**	**18**	**1**	**18**	**1**	**18**	**1**	**18**	**1**	**18**	**1**	**18**	**1**	**18**	**1**

Елементи 2, 3, 10, 13, 14, 15 із GF(19) мають довгий цикл $_{\min} j = (p-1) = 18$, тому вони є первісними, а їх степені $\boldsymbol{j}$ = 0…18 пробігають однократно значення всіх елементів M_{19} . Непервісні елементи мають короткі, тому – неповні цикли, наприклад, елемент 11 має цикл і порядок 3, а 12 має цикл і порядок 6.

У Таблиці 5.2 у відповідних рядках червоною рамкою і затемненням окреслено цикли елементів $\alpha \in GF(19)$. Кількість темних клітин у відповідному рядку таким графічним чином вказує на мультиплікативний порядок елемента. Довжина цикла елемента співпадає з його мультиплікативним порядком. Тут отримуємо, аналогічно результатам Таблиці 5.1, $a^{19-1} \equiv 1 (\mathrm{mod} 19)$ тому що тут теж діє мала теорема Ферма (13). Бачимо (Табл.5.2), що цикли елементів завершуються 1-цею і повторюються знов і знов, навіть цикли первісних елементів (довгі цикли) повторюються, якщо продовжити ряд степенів $j = 1,2,3,\ldots,(p-1)$ за межі $(p-1)$, для даного прикладу $j = 19,20,21,\ldots$ і так далі. Бачимо, що кожний цикл має точку замикання на 1-ці, перетинаючи яку він повторюється до нескінченної кількості разів. І тільки у довгі цикли, цикли первісних елементів, по одному разу входить кожний ненульовий елемент із $GF(19)$. В інших циклах не вистачає деяких елементів M_{19} із $GF(19)$. Тому саме первісний елемент $2, 3, 10, 13, 14, 15 \in GF(19)$ однозначно задає мультиплікативну групу M_{19} і може сам її представляти в мультиплікативних операціях поля.

Таким чином, саме первісний елемент $w \in GF(p)$ однозначно задає мультиплікативну групу M_p і може сам її представляти в мультиплікативних операціях поля. Це є найважливіший висновок із довгих попередніх пояснень і досліджень властивостей мультиплікативної групи M_p скінченного поля $GF(p)$.

Виконаємо кілька вправ на оперування з елементами $GF(p) = GF(19)$. Очевидно, що $p = 19$ і, відповідно, M_{19}. Операції виконуємо за $\mathrm{mod} 19$.

Вправа 1. Операція додавання, за визначеннями (1), (2) та Рис.9:

$$7 + 10 = 10 + 7 = 17 \equiv 17 (\mathrm{mod} 19),$$

$$16 + 12 = 12 + 16 = 28 \equiv 9 (\mathrm{mod} 19). \qquad (14)$$

Елементи $17,\ 9 \in GF(19)$ є результатами додавання в цих прикладах.

Вправа 2. Операція множення, за визначеннями (1), (2) та Рис.9:

$$7*10=10*7=70\equiv 13\ (\mathrm{mod}19),$$
$$16*12=12*16=192\equiv 2\ (\mathrm{mod}19). \qquad (15)$$

Елементи $13,\ 2\in GF(19)$ є результатами множення в цих прикладах.

Вправа 3.1. Елементи, обернені за «+». Нехай $\beta=7\in GF(19)$, потрібно знайти $(-\beta)\in GF(19)$. Виходимо із визначення (5) з урахуванням виконання операцій за $\mathrm{mod}19$.

$$7+(-\beta)\equiv 0(\mathrm{mod}19). \qquad (16)$$

З огляду на вирази (9) та (10), зрівняння (16) перепишемо наступним чином

$$7+(-\beta)-i*19=0,\ \text{або}\quad (-\beta)=i*19-7 \qquad (17)$$

Оскільки $(-\beta)\in GF(19)$ і має виконуватися $(-\beta)<19$, то очевидно, що $i=1$, тоді

$$(-\beta)=i*19-7=19-7=12 \qquad (18)$$

Вправа 3.2. Нехай $\beta=3\in GF(19)$, потрібно знайти $(-\beta)\in GF(19)$. За визначенням (5) має виконуватись наступне зрівняння

$$3+(-\beta)\equiv 0(\mathrm{mod}19). \qquad (19)$$

З огляду на вирази (9) та (10), зрівняння (19) перепишемо наступним чином

$$3+(-\beta)-i*19=0,\ \text{або}\quad (-\beta)=i*19-3. \qquad (20)$$

Оскільки $(-\beta) \in GF(19)$ і має виконуватися $(-\beta) < 19$, то очевидно, що $i = 1$, тоді

$$(-\beta) = i * 19 - 3 = 19 - 3 = 16. \qquad (21)$$

Проста перевірка: $7 + 12 \equiv 0 (\text{mod} 19)$ та $3 + 16 \equiv 0 (\text{mod} 19)$ підтверджує, що елементи $12,\ 16 \in GF(19)$ є оберненими до $7,\ 3 \in GF(19)$ за додаванням.

Вправа 4.1. Знайти елементи, обернені за множенням. Нехай $\beta = 8 \in GF(19)$, потрібно знайти $(\beta^{-1}) \in GF(19)$. Виходимо із визначення (6) з урахуванням виконання операцій за mod19

$$8 * (\beta^{-1}) \equiv 1 (\text{mod} 19). \qquad (22)$$

Звернімо увагу на Таблицю 5.2. Оберемо $w = 3 \in GF(19)$ у якості первісного елемента. Подамо 8 через первісний - у рядку для $a = 3$ в Табл.5.2 знаходимо, що $\beta = 8 \equiv 3^3 (\text{mod} 19)$. Тоді маємо $(\beta^{-1}) = (8)^{-1} \equiv (3^3)^{-1} \equiv (3^{-3}) \ \text{mod} 19$. Тепер використаємо властивість формальної 1-ці за теоремою Ферма, а саме $w^{p-1} \equiv 1 (\text{mod} p)$, тобто $3^{18} \equiv 1 (\text{mod} 19)$:

$$(\beta^{-1}) \equiv (3^{-3}) \equiv (1 * 3^{-3}) \equiv (3^{18} * 3^{-3}) \equiv 3^{15} \ \text{mod} 19, \qquad (23)$$

звідки та з Таблиці 5.2 витікає, що $(\beta^{-1}) \equiv 3^{15} (\text{mod} 19) = 12$. Перевірка $8 * 12 \equiv 1 (\text{mod} 19)$ підтверджує, що $12 \in GF(19)$ є обернений до $8 \in GF(19)$ за множенням.

Вправа 4.2. Нехай $\beta = 16 \in GF(19)$, знайти $(\beta^{-1}) \in GF(19)$. За визначенням (6) запишемо:

$$16 * (\beta^{-1}) \equiv 1 (\text{mod} 19). \qquad (24)$$

За Таблицею 5.2 оберемо $w = 3 \in GF(19)$ у якості первісного елемента. Подамо елемент 16 через первісний - у рядку для $a = 3$ в Табл.5.2 знаходимо, що $\beta = 16 \equiv 3^{10} (\text{mod} 19)$. Тоді маємо $(\beta^{-1}) = (16)^{-1} \equiv (3^{10})^{-1} \equiv (3^{-10}) \ \text{mod} 19$.

Тепер використаємо властивість формальної 1-ці за теоремою Ферма, а саме $w^{p-1} \equiv 1 (\text{mod} p)$, тобто $3^{18} \equiv 1 (\text{mod} 19)$:

$$(\beta^{-1}) \equiv (3^{-10}) \equiv (1 * 3^{-10}) \equiv (3^{18} * 3^{-10}) \equiv 3^{8} \ \text{mod} 19, \qquad (25)$$

звідки та з Таблиці 5.2 витікає, що $(\beta^{-1}) \equiv 3^{8} (\text{mod} 19) = 6$. Перевірка $16 * 6 \equiv 1 (\text{mod} 19)$ підтверджує, що $6 \in GF(19)$ є обернений елемент до $16 \in GF(19)$ за множенням.

Вправа 5. Віднімання елемента β від елемента α . Це неосновна, додаткова операція, яка організовується процедурно через використання оберненого за додаванням $(-\beta)$. Процедуру виконують як додавання $\alpha + (-\beta) \equiv \delta (\text{mod} p)$ наступним чином

$$\alpha - \beta = \alpha + (-\beta) \equiv \delta (\text{mod} p) \qquad (26)$$

Нехай, наприклад, $\alpha = 8 \in GF(19)$, а $\beta = 17 \in GF(19)$, тоді завдання ставиться так

$$\alpha - \beta = 8 - 17 = 8 + (-17) \equiv \delta (\text{mod} 19). \qquad (27)$$

За процедурою, наведеною у Вправах 3.1 та 3.2, знаходимо що $(-17) \equiv 2 (\text{mod} 19)$, тоді

$$8 - 17 \equiv 8 + (-17) \equiv 8 + 2 \equiv 10 (\text{mod} 19),$$

тобто, маємо остаточно $8 - 17 \equiv 10 (\text{mod} 19)$. Перевірка додаванням підтверджує, що 10 є результатом віднімання: $10 + 17 \equiv 8 (\text{mod} 19)$.

Вправа 6. Операція ділення елемента α на β . Це неосновна, додаткова операція, яка організовується процедурно через використання оберненого за множенням (β^{-1}). Процедуру виконують як множення $\alpha*(\beta^{-1})\equiv\delta(\mathrm{mod}\,p)$ наступним чином

$$\alpha/\beta=\alpha:\beta\equiv\alpha*(\beta^{-1})\equiv\delta(\mathrm{mod}\,p). \qquad (28)$$

Нехай, наприклад, $\alpha=8\in GF(19)$, а $\beta=17\in GF(19)$, тоді формулювання ділення елемента a на елемент β запишемо так

$$\alpha:\beta=8:17=8*(17^{-1})\equiv\delta(\mathrm{mod}19). \qquad (29)$$

За процедурою, наведеною у Вправах 4.1 та 4.2, знаходимо що $(17^{-1})\equiv 9(\mathrm{mod}19)$, тоді можемо записати наступне

$$8:17\equiv 8*(17^{-1})\equiv 8*9=72\equiv 15(\mathrm{mod}19), \qquad (30)$$

тобто, маємо результат ділення $8:17\equiv 15(\mathrm{mod}19)$. Перевірка множенням підтверджує правильність виконання ділення: $15*17\equiv 8(\mathrm{mod}19)$.

Вправа 7. Піднесення елемента $\alpha=12\in GF(19)$ до степені $m=897$. Завдання формулюється як $\alpha^m\equiv\delta(\mathrm{mod}\,p)$, тобто, у даному прикладі, як $12^{897}\equiv\delta(\mathrm{mod}19)$, визначити δ. Звернімося, наприклад, до Таблиці 5.2 і оберемо первісний елемент $w=10\in GF(19)$. У рядку $a=10$ знайдемо подання елемента 12 як степінь первісного: $12\equiv w^j\equiv 10^3(\mathrm{mod}19)$, тоді перепишемо завдання так $12^{897}\equiv(10^3)^{897}\equiv 10^{2691}\equiv\delta(\mathrm{mod}19)$. Зважаючи на цикловість піднесення елементів M_{19} до степені і знаючи порядок первісного $n=18$, врахуємо кількість циклів довжини $n=18$ первісного елемента 10 при піднесенні його до степені: $2691=149\cdot 18+9$. Мовою теорії чисел це записують як $2691\equiv 9\ (\mathrm{mod}18)$. Тут прошу читача бути уважним: $2691\equiv 9$ саме за $(\mathrm{mod}18)$, оскільки $n=18$ є порядок первісного 10. Бачимо, що кількість таких циклів

складає 149. Це означає, що, при піднесенні до вказаної степені, елемент 10 пройшов свій мультиплікативний цикл (перетнув 1-цю в кінці цикла) 149 разів, і вже на 150-му разі (циклі) був піднесений до степені 9. Зважаючи на це перепишемо наведений вираз наступним чином

$$12^{897} \equiv 10^{2691} \equiv 10^{149 \cdot 18+9} \equiv 10^{9} \equiv \delta \ (\text{mod}19). \qquad (31)$$

Остаточно, знов звернімо увагу на Таблицю 5.2. У рядку для первісного $a = 10$, у його циклі бачимо, що $10^{9} \equiv 18 \ (\text{mod}19)$. Інші способи обчислення, включаючи пряме обчислення на калькуляторі, дають той же самий результат. Отже, степінь $12^{897} \equiv 18 \ (\text{mod}19)$ і $\delta = 18$.

Як бачимо із Таблиці 5.2, кожний елемент $\alpha \in M_p = M_{19}$ має своє подання у формі степені первісного $\alpha = w^j \in GF(19)$. Це дозволяє легко і просто виконати операції множення, ділення, та обернення елементів поля, оперуючи показниками степенів лише одного, первісного елемента w з використанням лише звичайних множення, додавання та віднімання на цих показниках.

Вправа 8.1. Множення, елементів поля $\alpha, \beta, \delta \in GF(19)$ на базі степенів первісного елемента $w^j \in GF(19)$. Нехай потрібно обчислити δ як добуток $\alpha * \beta = \delta \ (\text{mod}19)$ для $\alpha = 15$ та $\beta = 8$. Оберемо із Таблиці 5.2 первісний елемент $w = 10 \in GF(19)$, нагадаємо - це один із елементів порядку $n = 18$. У рядку $a = 10$ в Таблиці 5.2 знайдемо подання елементів 15 та 8 як степенів первісного $15 \equiv w^j \equiv 10^{7} \ (\text{mod}19)$ та $8 \equiv w^j \equiv 10^{15} \ (\text{mod}19)$, тоді можемо записати наступне $\alpha * \beta = 15 * 8 \equiv 10^{7} * 10^{15} \equiv 10^{7+15} \equiv 10^{22} \ (\text{mod}19)$, далі із показника 22 виділяємо кількість цілих порядків $n = 18$, тобто, беремо показник $22 \bmod 18 = 4$ і завершуємо перетворення, зауваживши, що $10^{18} \equiv 1 \ (\text{mod}19)$

$$10^{22} \equiv 10^{18+4} \equiv 10^{18} * 10^{4} \equiv 1 * 10^{4} \equiv 10^{4} \equiv 6 \ (\text{mod}19) \qquad (32)$$

Таким чином, отримуємо $15*8\equiv 6\ (\mathrm{mod}19)$, тобто $\delta = 6$.

Подібним чином можна обчислити і приклади (15) із Вправи 2. А саме:

$$7*10\equiv 10^{12}*10^{1}\equiv 10^{13}\equiv 13\ (\mathrm{mod}19),$$
$$16*12\equiv 10^{14}*10^{3}\equiv 10^{17}\equiv 2\ (\mathrm{mod}19). \qquad (33)$$

При великих обсягах алфавіту $\boldsymbol{M_p}$, виконання операції множення за процедурою (33) значно скорочує витрати часу і обчислювальних ресурсів. Очевидно, що це вимагає нескладних обчислень над показниками степенів операндів і результату операції. При цьому є потреба тримати таблицю елементів поля GF(p) у формі степенів первісного у пам'яті обчислювального пристрою.

Вправа 8.2. Ділення, елементів поля $\alpha,\beta,\delta\in GF(19)$ на базі степенів первісного елемента $w^j\in GF(19)$. Зауважимо, що $\alpha,\beta,\delta\in GF(19)$ суть цілі числа. У полі $GF(19)$ принципово немає дробів, тільки цілі числа. Нехай потрібно обчислити δ як частку $\alpha:\beta=\delta\ (\mathrm{mod}19)$ для $\alpha=15$ та $\beta=8$. Оберемо із Таблиці 5.2 первісний елемент $w=10\in GF(19)$, нагадаємо - це один із елементів порядку $n=18$. У рядку $a=10$ в Таблиці 5.2 знайдемо подання елементів 15 та 8, як степенів первісного: $15\equiv w^j\equiv 10^7\ (\mathrm{mod}19)$ та $8\equiv w^j\equiv 10^{15}\ (\mathrm{mod}19)$, тоді можемо записати наступне, зауваживши, що $10^{18}\equiv 1\ (\mathrm{mod}19)$

$$15:8\equiv 10^7:10^{15}\equiv 10^{(7-15)}\equiv 10^{-8}\equiv 1*10^{-8}\equiv 10^{18}*10^{-8}\equiv 10^{10}(\mathrm{mod}19), \qquad (34)$$

остаточно отримуємо $15:8\equiv 10^{10}\equiv 9\ (\mathrm{mod}19)$, тобто $\delta=9$. Перевірка множенням підтверджує цей результат $9*8\equiv 15\ (\mathrm{mod}19)$.

Подібним чином можна обчислити і приклад (30) із Вправи 6. А саме:

$$8:17 \equiv 10^{15}:10^{8} \equiv 10^{15-8} \equiv 10^{7} \equiv 15 \ (\text{mod}19) \qquad (35)$$

Вправа 8.3. Обернення, елементів поля $\alpha,\delta \in GF(19)$ на базі степенів первісного елемента $w^j \in GF(19)$. Зауважимо, що $\alpha,\delta \in GF(19)$ суть цілі числа. У полі принципово немає дробів, тільки цілі числа. Нехай потрібно обчислити обернений $\delta \equiv \alpha^{-1} \ (\text{mod}19)$ для $\alpha = 15$ та $\alpha = 8$. Оберемо із Таблиці 5.2 первісний елемент $w = 10 \in GF(19)$, нагадаємо - це один із елементів порядку $n = 18$. У рядку $a = 10$ в Таблиці 5.2 знайдемо подання елементів 15 та 8 як степенів первісного $15 \equiv w^j \equiv 10^7 \ (\text{mod}19)$ та $8 \equiv w^j \equiv 10^{15} \ (\text{mod}19)$, тоді можемо записати наступне, зауваживши, що $10^{18} \equiv 1 \ (\text{mod}19)$:

$$\delta \equiv 15^{-1} \equiv (10^7)^{-1} \equiv 1 * 10^{-7} \equiv 10^{18} * 10^{-7} \equiv 10^{11} \equiv 14 \ (\text{mod}19),$$

$$\delta \equiv 8^{-1} \equiv (10^{15})^{-1} \equiv 1 * 10^{-15} \equiv 10^{18} * 10^{-15} \equiv 10^{3} \equiv 12 \ (\text{mod}19). \qquad (36)$$

Перевірка множенням підтверджує ці результати із (36). Справді, бачимо що $15 * 14 \equiv 1 \ (\text{mod}19)$ та $8 * 12 \equiv 1 \ (\text{mod}19)$.

Слід знову зауважити, що при великих обсягах алфавіту M_p , виконання мультиплікативних операцій за процедурами із Вправ №№ 4.1, 4.2, 6, 7, 8.1, 8.2, 8.3 значно скорочує витрати часу і обчислювальних ресурсів. Не складно пересвідчитися, що це вимагає звичайних обчислень над показниками степенів операндів і результату операції.

Оскільки в криптографії використовують великі і дуже великі прості числа p утворюючи скінченні поля $GF(p)$ з відповідною потужністю множини M_p, то обернення елементів (як і множення, піднесення до степені та ділення) $\alpha \in GF(p)$ вимагає зберігати таблиці подання $\alpha \equiv w^j \in GF(p)$ великого обсягу, як степенів обраного первісного елемента, або використовувати алгоритм обернення елементів «походу» в момент виникнення потреби. Найвідомішим з таких алгоритмів є розширений алгоритм Евкліда [5,6].

Слід зауважити, що дроби і взяття кореня на елементах поля GF(p) є невизначеними об’єктами і діями, тому їх виконати неможливо. Дріб ***a/b*** можна розглядати лише як формулювання задачі для процедури ділення на ***b***, відповідно до виразу (28) із Вправи 6.

Ще раз варто підкреслити, матеріал цього розділу може здаватися складним, але це не так. Він є максимально спрощений автором для надання можливості читачеві більш швидко проникнути у неочевидні властивості чисел і механізми їх взаємодії, на базі яких і створено знакові сучасні асиметричні криптоалгоритми: Діффі-Хеллмана, Ель-Гамаль, RSA. Ці відомості, навички оперування елементами скінченного поля стануть у нагоді і при ознайомленні із внутрішніми механізмами протоколів ЕЦП та криптографії на еліптичних кривих.

5.1. Контрольні запитання

5.1.1 Надайте визначення скінченного поля Галуа GF(p).

5.1.2 Надайте визначення скінченного поля Галуа $GF(p^m)$.

5.1.3 Що таке замкнена операція над операндами?

5.1.4 Визначити унарну операцію над елементами поля.

5.1.5 Визначити бінарну операцію над елементами поля.

5.1.6 Які властивості мають два особливих елемента поля?

5.1.7 Як визначають операцію додавання над елементами поля GF(p)?

5.1.8 Як визначають операцію добутку над елементами поля GF(p)?

5.1.9 Як визначають операцію віднімання над елементами поля GF(p)?

5.1.10 Як визначають операцію ділення на елемент поля GF(p)?

5.1.11 Як знайти зворотний за складанням елемент поля GF(p)?

5.1.12 Як знайти зворотний за множенням елемент поля GF(p)?

5.1.13 Як знайти цілу степінь елемента поля GF(p)?

5.1.14 Як визначено дріб на елементах поля GF(p)?

5.1.15 Як обчислити корінь степеня k із елемента поля GF(p)?

5.1.16 Що таке алгебрична група поля GF(p), властивості?

5.1.17 Що таке мультиплікативна група поля GF(p), властивості?

5.1.18 Що таке порядок елемента поля GF(p)?

5.1.19 Що таке і які бувають цикли елементів поля GF(p)?

5.1.20 Що таке короткий цикл елементів поля GF(p)?

5.1.21 Що означає довгий цикл елементів поля GF(p)?

5.1.22 Як визначають первісний елемент поля GF(p)?

5.1.23 Як визначають елементи групи M_p через первісний елемент GF(p)?

5.1.24 Як виконують мультиплікативні операції через степеневе подання GF(p)?

5.1.25 Як формулюють алгоритм Евкліда, його призначення?

5.1.26 Як формулюють розширений алгоритм Евкліда, його призначення?

5.1.27 Як формулюють малу теорему Ферма, її призначення?

5.2. Контрольні завдання

5.2.1 Записати A_p та M_p для $GF(p)$, при а) p = 23; б) p = 43.

5.2.2 Дано $a,b,c \in GF(p)$, $a = 158$, $b = 139$, $p = 181$, визначити $a + b \equiv c$.

5.2.3 Дано $a,b,c \in GF(p)$, $a = 177$, $b = 297$, $p = 379$, визначити $a + b \equiv c$.

5.2.4 Дано $a,b,c \in GF(p)$, $a = 108$, $b = 91$, $p = 163$, визначити $a + b \equiv c$.

5.2.5 Дано $a,b,c \in GF(p)$, $a = 88$, $b = 71$, $p = 241$, визначити $a + b \equiv c$.

5.2.6 Дано $a,b,c \in GF(p)$, $a = 298$, $b = 71$, $p = 401$, визначити $a + b \equiv c$.

5.2.7 Дано $a,b,c \in GF(p)$, $a = 28$, $b = 169$, $p = 181$, визначити $a - b \equiv c$.

5.2.8 Дано $a,b,c \in GF(p)$, $a = 56$, $b = 197$, $p = 379$, визначити $a - b \equiv c$.

5.2.9 Дано $a,b,c \in GF(p)$, $a = 34$, $b = 71$, $p = 163$, визначити $a - b \equiv c$.

5.2.10 Дано $a,b,c \in GF(p)$, $a = 81$, $b = 173$, $p = 241$, визначити $a - b \equiv c$.

5.2.11 Дано $a,b,c \in GF(p)$, $a = 281$, $b = 373$, $p = 401$, визначити $a - b \equiv c$.

5.2.12 Дано $a,b,c \in GF(p)$, $a = 32$, $b = 154$, $p = 167$, визначити $a \bullet b \equiv c$.

5.2.13 Дано $a,b,c \in GF(p)$, $a = 82$, $b = 326$, $p = 179$, визначити $a \bullet b \equiv c$.

5.2.14 Дано $a,b,c \in GF(p)$, $a = 112$, $b = 93$, $p = 227$, визначити $a \bullet b \equiv c$.

5.2.15 Дано $a,b,c \in GF(p)$, $a = 179$, $b = 105$, $p = 263$, визначити $a \bullet b \equiv c$.

5.2.16 Дано $a,b,c \in GF(p)$, $a = 233$, $b = 308$, $p = 383$, визначити $a \bullet b \equiv c$.

5.2.17 Дано $a,b,c \in GF(p)$, $a = 132$, $b = 14$, $p = 167$, визначити $a/b \equiv c$.

5.2.18 Дано $a,b,c \in GF(p)$, $a = 65$, $b = 144$, $p = 179$, визначити $a/b \equiv c$.

5.2.19 Дано $a,b,c \in GF(p)$, $a = 142$, $b = 123$, $p = 227$, визначити $a/b \equiv c$.

5.2.20 Дано $a,b,c \in GF(p)$, $a = 78$, $b = 135$, $p = 263$, визначити $a/b \equiv c$.

5.2.21 Дано $a,b,c \in GF(p)$, $a = 209$, $b = 187$, $p = 383$, визначити $a/b \equiv c$.

5.2.22 Дано $a,c \in GF(p)$, $a = 107$, $p = 167$, визначити $a^{-1} \equiv c$.

5.2.23 Дано $a,c \in GF(p)$, $a = 147$, $p = 179$, визначити $a^{-1} \equiv c$.

5.2.24 Дано $a,c \in GF(p)$, $a = 213$, $p = 227$, визначити $a^{-1} \equiv c$.

5.2.25 Дано $a,c \in GF(p)$, $a = 152$, $p = 263$, визначити $a^{-1} \equiv c$.

5.2.26 Дано $a,c \in GF(p)$, $a = 61$, $p = 383$, визначити $a^{-1} \equiv c$.

5.2.27 Дано $a,b,c \in GF(p)$, $a = 102$, $b = 587$, $p = 167$, визначити $a^b \equiv c$.

5.2.28 Дано $a,b,c \in GF(p)$, $a = 96$, $b = 423$, $p = 179$, визначити $a^b \equiv c$.

5.2.29 Дано $a,b,c \in GF(p)$, $a = 89$, $b = 354$, $p = 227$, визначити $a^b \equiv c$.

5.2.30 Дано $a,b,c \in GF(p)$, $a = 65$, $b = 262$, $p = 263$, визначити $a^b \equiv c$.

5.2.31 Дано $a,b,c \in GF(p)$, $a = 53$, $b = 195$, $p = 383$, визначити $a^b \equiv c$.

5.2.32 Визначити критичні степені w, обрати первісний в $GF(p)$, $p = 97$.

5.2.33 Визначити критичні степені w, обрати первісний в $GF(p)$, $p = 193$.

5.2.34 Визначити критичні степені w, обрати первісний в $GF(p)$, $p = 241$.

5.2.35 Визначити критичні степені w, обрати первісний в $GF(p)$, $p = 163$.

5.2.36 Визначити критичні степені w, обрати первісний в $GF(p)$, $p = 181$.

6. КРИПТОАЛГОРИТМ ДІФФІ-ХЕЛЛМАНА

Публікація у 1975 році революційних пропозицій В. Діффі та М. Хеллмана (у статті New Directions in Cryptography) про односпрямовані функціональні перетворення з лазівкою започаткувала широкомасштабне застосування асиметричних криптоалгоритмів з двома ключами – приватним і публічним, у системах комунікації.

Перший із асиметричних криптоалгоритмів це алгоритм Діффі-Хеллмана (часто позначають D-H), який призначено для узгодження (розповсюдження) єдиного, секретного ключа K сеансу комунікації (з метою використання його у подальшому в симетричній криптосистемі Рис. 2, Рис. 3) серед кількох суб'єктів СІД, через незахищене, відкрите середовище комунікацій, наприклад, мережу спільного доступу. Секретні дані і ключі у відкритому середовищі не передаються. Передаються лише певні дані Y_i, математично пов'язані із секретними даними, а саме - відкриті, публічні ключі [5,6]. Можливо тому у стандартах цю дію називають «узгодження ключа». Відкриті ключі Y_i можуть бути перехоплені у середовищі криптоаналітиком, але за ними надзвичайно важко (чи взагалі нереально) за осяжний час дізнатися K, якщо секретні дані не попали йому до рук.

Розглянемо докладніше алгоритм Діффі-Хеллмана для двох суб'єктів, поданий на Рис. 11, для користувача А та користувача В [11].

Спочатку користувачі домовляються про параметри сеансу узгодження ключа: p - велике просте число та $w \in GF(p)$ - первісний елемент скінченного поля, які можуть бути опубліковані відкрито одним із них (Рис. 2), або Довіреною третьою стороною (Рис. 3). Оберемо для прикладу $p = 83$ та кандидата на статус первісного $w = 5$. Перевіримо, чи має $w = 5$ порядок $(p-1) = 82$, тобто, довгий цикл. Для цього потрібно пересвідчитися, що $w = 5$ не має коротких циклів. Їх імовірність виникає на критичних степенях кандидата на статус первісного - показниках $m \mid (p-1)$, тобто на дільниках m числа $(p-1)$.

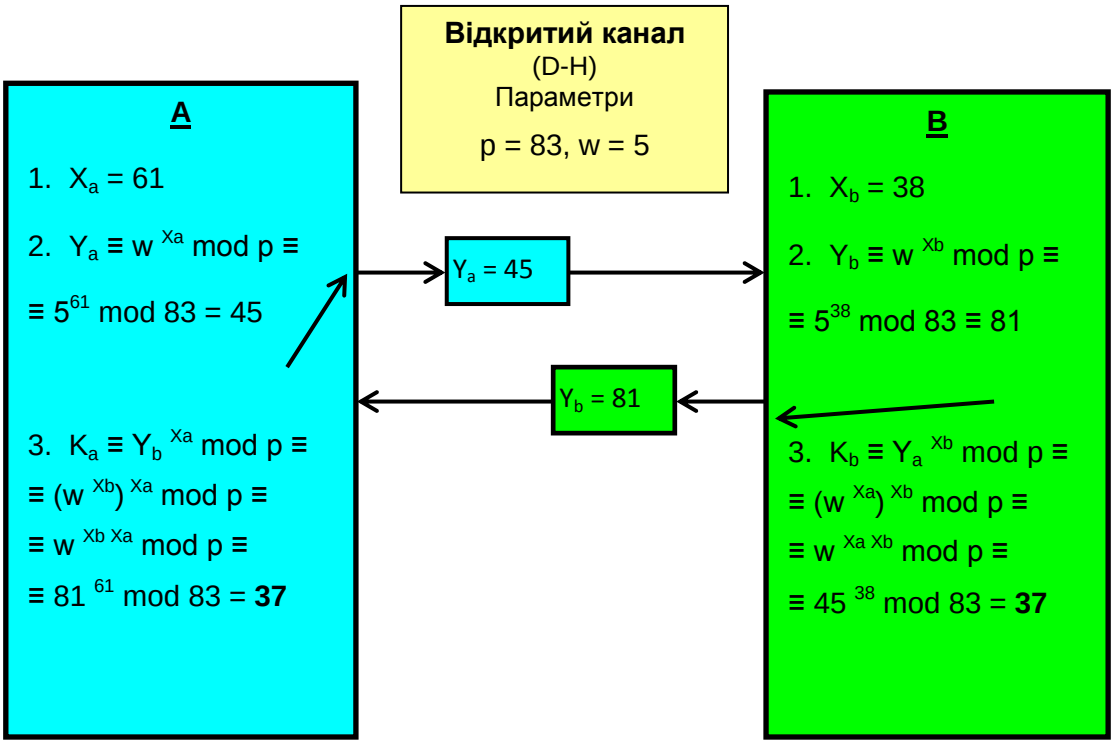

Рисунок 11 - Алгоритм Діффі-Хеллмана, $K_a = K_b = K$

При піднесенні кандидата $w^m \pmod p$ до степенів m таких дільників $m \mid (p-1)$, може утворитися 1-ця, це і буде індикатором короткого цикла у w. У такому разі відповідний кандидат w не є первісним елементом і треба обрати інший w (і перевірити його порядок та на наявність коротких циклів). Під час перевірки, у даному прикладі знаходимо, що $(p-1) = 82 = 2 \cdot 41$, тобто критичні степені дорівнюють $m = 2; 41$. Бачимо, що $w^m \pmod p$ дає наступні результати $5^2 \pmod{83} = 25$ та $5^{41} \pmod{83} = 82$. Очевидно, що $w^m \pmod p \neq 1$ на критичних степенях, тому можемо обрати $w = 5$, у якості первісного елемента.

Тепер сам алгоритм Діффі-Хеллмана. На першому кроці користувач A та користувач B незалежно один від одного генерують свої власні випадкові секретні (приватні) ключі X_a та X_b, які вони мають утримувати в секреті від інших учасників комунікації, нехай вони згенерували $X_a = 61$ та $X_b = 38$.

На другому кроці користувач A та користувач B незалежно один від одного, кожен на своєму робочому місці, генерують свої відкриті (публічні)

ключі Y_a та Y_b, підносячи спільний первісний елемент $w = 5$ до степені свого локального секретного ключа X_a та X_b, відповідно:

$$Y_a \equiv w^{Xa} mod\ p \equiv 5^{61} mod\ 83 = 45,$$
$$Y_b \equiv w^{Xb} mod\ p \equiv 5^{38} mod\ 83 = 81. \quad (37)$$

Користувачі А та В обмінюються відкритими ключами 45 та 81 через відкритий канал, як показано на Рис. 11. Вважаємо, що і Криптоаналітик перехопив ці відкриті ключі (разом із $p = 83$ та $w = 5$).

На третьому кроці користувачі А та В незалежно один від одного на своїх робочих місцях генерують свій єдиний сеансовий ключ $K_a = K_b = K$, підносячи відкритий ключ Y протилежної сторони до степені свого секретного ключа X:

$$K_a \equiv Y_b{}^{Xa} mod\ p \equiv \left(w^{Xb}\right)^{Xa} mod\ p \equiv w^{Xb\ Xa} mod\ p \equiv 81^{61} mod\ 83 = \mathbf{37},$$
$$K_b \equiv Y_a{}^{Xb} mod\ p \equiv \left(w^{Xa}\right)^{Xb} mod\ p \equiv w^{Xa\ Xb} mod\ p \equiv 45^{38} mod\ 83 = \mathbf{37}. \quad (38)$$

Як бачимо, дійсно, на відстані, незалежно, в результаті короткої комунікації двох сторін, на їх робочих місцях створено (узгоджено) абсолютно однакові значення $K_a = K_b = K = 37$, це власне і є той елемент, який умовно називаємо ключ сеансу K. В реальних системах значення K стає основою для генерації однакового «криптографічно гарного» ключа сеансу у кожного користувача А та В, яким вони можуть у подальшому шифрувати і дешифрувати повідомлення один одному, забезпечуючи конфіденційність та цілісність комунікації. Виникає тим часом питання, як часто потрібно міняти ключ сеансу? Воно дуже цікаве і пов'язане зі статистикою та практикою захисту інформації, але вимагає окремого обговорення. Можемо тут згадати

про наявність різних керівних документів та посадових інструкцій в організаціях, де мають бути наявними відповідні рекомендації та вимоги. За відсутності таких дивимося відповідну літературу.

Проаналізуємо, які шанси у Криптоаналітика? Вище вже згадувалося, що він перехопив начебто багато даних із відкритого каналу, а саме: $p = 83$, $w = 5$, $Y_a = 45$ та $Y_b = 81$. Його мета розкрити $K = K_a = K_b$. Він знає вирази (37) та (38), застосовані користувачами А та В для обчислень, але не знає застосованих там секретних ключів X_a та X_b. Якщо він зможе їх обчислити, то він зможе використати будь-який вираз із (38) і тоді розкриє $K = K_a = K_b$. Для обрахунку жаданих локальних секретних ключів X_a та X_b він може скласти систему зрівнянь за виразами (37), він знає ці вирази, бо алгоритм є відкритим

$$\begin{cases} Y_a \equiv 5^{X_a} \bmod 83 = 45 \\ Y_b \equiv 5^{X_b} \bmod 83 = 81 \end{cases} . \qquad (39)$$

Кожне зрівняння із системи (39) є прикладом так званого дискретного піднесення до степені. Обернена задача обчислення X_a за відомими $Y_a = 45$, $p = 83$ та $w = 5$, або обчислення X_b за відомими $Y_b = 81$, $p = 83$ та $w = 5$ є нерозв'язаною на поточний момент математичною задачею яка має назву «проблема дискретного логарифмування». І Криптоаналітик мусить або вчинити наукову математичну звитягу, або вдатися до атаки грубої сили і виконати перебір варіантів X_a або X_b. У системі (39) кожне зрівняння само по собі несе проблему дискретного логарифмування. А як щодо системи зрівнянь?

Згадаємо, що зрівняння мають еквівалентну форму у звичній алгебрі (9), (10), згадаємо також вираз 2) на Рис. 10, б). Скористаємося цими виразами і розкриємо систему зрівнянь (39) до системи рівнянь (40):

$$\begin{array}{l} Y_a \Rightarrow \begin{cases} 5^{X_a} - i \bullet 83 = 45 \\ 5^{X_b} - j \bullet 83 = 81 \end{cases} . \\ Y_b \Rightarrow \end{array} \qquad (40)$$

Бачимо, що система із двох рівнянь має чотири невідомих: X_a , X_b та i , j . Кожного разу, коли Криптоаналітик перехопить іще відкриті ключі у каналі, він додасть до системи ще рівнянь, але кількість невідомих буде у два рази перевищувати кількість незалежних рівнянь. У таких випадках кажуть, що система має нескінченну кількість розв'язків, що і обґрунтовує для Криптоаналітика єдиний можливий шлях до успіху: прямий перебір значень X_a або X_b, чи i та j. Тепер стосовно значення p, звісно $p = 83$, як у прикладі, є замалим. Для навчального прикладу його достатньо, щоби показати внутрішні механізми алгоритму. Насправді p має бути великим, або дуже великим простим числом, щоби незрівнянно ускладнити для Криптоаналітика процес перебору варіантів, поставити його перед потребою витратити неосяжні ресурси: часові, обчислювальні, енергетичні, економічні зрештою.

Отже, саме проблема дискретного логарифмування і є основою криптостійкості алгоритму Діффі-Хеллмана протягом кількох десятків років, що дозволило йому надзвичайно масово розповсюдитися в цифрових системах комунікацій, різних ІС, у галузях ІТ та ІКТ.

Він має своє призначення, яке було розкрито в цьому розділі, проте не забезпечує конфіденційність, автентифікацію, перевірку цілісності повідомлень, доступність ІС та інформаційних ресурсів. Все це має бути забезпечено іншими засобами. Одна з відомих загроз, про яку слід турбуватися стосовно цього алгоритму - атака «людина посередині» [5].

6.1. Контрольні запитання

6.1.1 Що таке алгоритм Діффі-Хеллмана?

6.1.2 Яке призначення алгоритма Діффі-Хеллмана?

6.1.3 Що таке секретний ключ в алгоритмі D-H?

6.1.4 Як обирають первісний елемент ***w*** для алгоритма D-H?

6.1.5 Що таке критичні степені кандидата ***w*** на статус первісного?

6.1.6 Які секретні дані і ключі передаються в каналі для алгоритма D-H?

6.1.7 Яку процедуру виконує користувач за алгоритмом D-H?

6.1.8 Чому ключі $\boldsymbol{K_a}$ та $\boldsymbol{K_b}$ користувачів A та B співпадають в D-H?

6.1.9 Чому Криптоаналітик не зможе обчислити $\boldsymbol{K_a}$ чи $\boldsymbol{K_b}$ в D-H?

6.1.10 Яка математична проблема забезпечує криптостійкість алгоритма D-H?

6.2. Контрольні завдання

6.2, A Виконати узгодження єдиного ключа $\boldsymbol{K}$ на двох локаціях A та B комунікаційної системи над полем GF(p) за алгоритмом Діффі-Хеллмана. Значення p, w, X_a, X_b обирати із Таблиці 6.2.A за номером завдання:

Таблиця 6.2.A - Контрольні завдання A

№	P	w	Xa	Xb
6.2.1	191	19	87	165
6.2.2	223	3	193	201
6.2.3	227	13	154	212
6.2.4	239	7	161	224
6.2.5	263	5	178	235
6.2.6	269	2	256	183
6.2.7	283	3	47	211
6.2.8	293	7	59	194
6.2.9	311	17	239	138
6.2.10	317	3	84	146
6.2.11	347	5	257	122
6.2.12	359	7	192	42
6.2.13	367	10	314	37
6.2.14	383	5	48	243
6.2.15	389	3	335	61
6.2.16	419	2	72	393
6.2.17	431	7	405	214
6.2.18	467	8	163	359
6.2.19	479	13	218	186
6.2.20	503	5	500	394

6.2.Б Обрати самостійно первісний елемент ***w*** поля GF(p). Перевірити і показати його первісність. Виконати узгодження єдиного ключа ***K*** на двох локаціях А та В комунікаційної системи за алгоритмом Діффі-Хеллмана. Значення p, X_a, X_b обирати із Таблиці 6.2.Б за номером завдання:

Таблиця 6.2.Б - Контрольні завдання Б

№	P	Xa	Xb
6.2.21	271	25	61
6.2.22	277	38	52
6.2.23	281	63	48
6.2.24	307	34	95
6.2.25	313	73	102
6.2.26	331	87	41
6.2.27	337	97	111
6.2.28	349	129	39
6.2.29	353	56	77
6.2.30	373	84	92
6.2.31	379	26	31
6.2.32	397	42	51
6.2.33	401	53	45
6.2.34	409	85	93
6.2.35	421	27	32
6.2.36	433	43	54
6.2.37	449	86	94
6.2.38	457	28	33
6.2.39	461	44	55
6.2.40	463	88	96

7. КРИПТОАЛГОРИТМ ШИФРУВАННЯ EL-GAMAL

Алгоритм шифрування Ель-Гамаль запропонований у 1985 році і призначений для забезпечення конфіденційності повідомлення M у відкритому каналі. Взагалі, схема Ель-Гамаль має також варіант електронного цифрового підпису (ЕЦП), але тут ми зосередимо увагу саме на забезпеченні конфіденційності повідомлення M у відкритому каналі. Тема ЕЦП заслуговує на окрему розмову. В літературі існує багато описів цього алгоритма і всіх їх об'єднує одне - процедурно в ньому можна виокремити два етапи [11]. Перший етап - узгодження і створення ключа сеансу $K = K_a = K_b$ буквально за алгоритмом Діффі-Хеллмана (чомусь мало хто із авторів це визнає). Основні кроки цієї частини алгоритма розставлені дещо інакше ніж ми бачили вище у Розділі 6, але суть їх залишається такою ж самою. А другий етап - власне, шифрування, передача криптограми через відкритий канал та дешифрування у отримувача. Основні ідеї алгоритма полягають у наступному [11]. На першому етапі він працює як асиметричний алгоритм Діффі-Хеллмана і забезпечує узгодження (створення) спільного ключа сеансу $K = K_a = K_b$ на робочих місцях двох сторін A та B , які перед цим згенерували для того випадкові локальні власні секретні ключі X_a та X_b (див. Рис. 11). На другому етапі, відправник, наприклад, A зашифровує повідомлення M шляхом множення його цифрового образа m на K, звісно, у межах скінченного поля $GF(p)$ за $(\mathrm{mod}\, p)$ і отримує криптограму (нагадаємо Вправу 2 і вираз (15) з Розділу 5), яку відправляє через відкритий канал до B

$$c \equiv m * K \ (\mathrm{mod}\, p). \qquad (41)$$

Отримувач B розшифровує криптограму c дискретним «діленням» на K (згадаємо вираз (8), і Вправу 6 з Розділу 5)

$$m \equiv c * K^{-1} \ (\mathrm{mod}\, p), \qquad (42)$$

тобто, отримувач застосовує для розшифрування той же самий ключ сеансу K, тільки з оберненням. У цьому алгоритм Ель-Гамаль несе в собі риси симетричної криптосистеми, модель якої ми розглянули на Рис.2, чи Рис.3, відмінність полягає лише в тому, що тут ключ K не передається.

Єдина додаткова дія, яку має виконати отримувач В, це обернення ключа сеансу K. У зауваженні в кінці Розділу 5 вказано на загальний алгоритм обернення елементів $GF(p)$, розширений алгоритм Евкліда, який при будь-яких великих p дозволяє виконати обернення за скінченну кількість кроків і не вимагає багато ресурсів на виконання [5,6]. Для навчального прикладу з невеликим p ми не будемо його залучати, а скористаємося простішим, перебірним підходом.

Отже, вважатимемо, що сторони А та В (див. Рис.11) при параметрах $p = 83$ та $w = 5$ обмінялися відкритими ключами та утворили кожний у себе ключ сеансу $K = 37 \in GF(83)$. Нехай Відправник А бажає конфіденційно передати Отримувачеві В повідомлення з цифровим образом $m = 67$. Він утворює криптограму, відповідно до виразу (41)

$$c \equiv 67 * 37 \pmod{83} = 72. \qquad (43)$$

Криптограма $c = 72$ передається до отримувача через відкритий канал. Отримувач у попередньому сеансі узгодження ключа обчислив точно такий же $K = 37 \in GF(83)$. Зараз він мусить виконати обернення $K^{-1} \equiv 37^{-1} \in GF(83)$. Скористатися він може розширеним алгоритмом Евкліда, або таблицею цикла для степенів обраного первісного w^j, або перебірним підходом. Ми застосуємо останній і на основі визначення оберненого елемента поля GF(p), запишемо:

$$\begin{array}{l} K * K^{-1} \equiv 1 \pmod{p} \\ K * K^{-1} - t \bullet p = 1 \\ K * K^{-1} = 1 + t \bullet p \end{array} \quad , \quad \begin{array}{l} 37 * K^{-1} \equiv 1 \pmod{83} \\ 37 * K^{-1} - t \bullet 83 = 1 \\ 37 * K^{-1} = 1 + t \bullet 83 \end{array} \quad . \qquad (44)$$

Тоді шукане обернене до ключа сеансу має відповідати рівнянню в цілих числах де t - деяке ціле число. Перебором $1 \le t < p$ досягаємо першого цілого $K^{-1} \in GF(83)$, тобто $K^{-1} < 83$

$$K^{-1} = (1 + t \bullet p) / K \ , \qquad K^{-1} = (1 + t \bullet 83) / 37 , \qquad (45)$$

знаходимо ціле $K^{-1} = (1 + t \bullet 83) / 37 = 9$ при $t = 4$. Перевірка $37 * 9 \equiv 1 \bmod 83$ підтверджує цей результат.

І нарешті, останній акорд, застосовуємо вираз (42)

$$m \equiv 72 * 9 \ (\text{mod } 83) = 67 . \qquad (46)$$

Таким чином, цифровий образ $m = 67$ повідомлення M відновлено отримувачем В на своєму робочому місці, повідомлення M конфіденційно передано через відкритий канал, його цілісність збережено. Ніхто не міг за осяжний період часу спотворити, чи імітувати повідомлення M для В, оскільки ключі зашифрування і дешифрування K і $K^{(-1)}$ мають тільки легальні користувачі А та В, і більше ніхто. Криптостійкість алгоритма El-Gamal забезпечується проблемою дискретного логарифмування.

Звісно, існують певні загрози і механізми можливого втручання зловмисника за певного збігу обставин та умов, для обговорення яких потрібен окремий майданчик і відкриття нової теми - криптоаналіз. Нагадаємо, що мета даного матеріалу - ознайомити зацікавленого читача з першими підходами, моделями, алгоритмами, механізмами та Протоколами криптографічного захисту даних методами асиметричних криптоперетворень.

7.1. Контрольні запитання

7.1.1 Що таке алгоритм El-Gamal?

7.1.2 Що забезпечує криптостійкість алгоритма El-Gamal?

7.1.3 Яке призначення алгоритма El-Gamal?

7.1.4 Які механізми складають основу алгоритма El-Gamal?

7.1.5 Як формуються секретні ключі користувачів в El-Gamal?

7.1.6 Як формується ключ зашифрування в El-Gamal?

7.1.7 Як формується ключ дешифрування в El-Gamal?

7.1.8 Як виконують зашифрування повідомлення M в El-Gamal?

7.1.9 Як виконують дешифрування криптограми C в El-Gamal?

7.1.10 Як пов'язані ключі шифрування і дешифрування в El-Gamal?

7.2. Контрольні завдання

Передати алгоритмом El-Gamal конфіденційне повідомлення **m** за напрямком $\overline{V}$, AB – Відправник A, BA – Відправник B. Параметри комунікації обрати із Таблиці 7.2 за номером Завдання.

Таблиця 7.2 – El-Gamal, параметри Завдання

№	p	w	Xa	Xb	m	$\overline{V}$
7.2.1	103	12	31	101	96	AB
7.2.2	107	15	49	92	101	BA
7.2.3	131	2	32	105	112	AB
7.2.4	139	3	48	100	84	BA
7.2.5	149	8	89	91	50	AB
7.2.6	167	17	33	106	63	BA
7.2.7	173	19	47	99	75	AB
7.2.8	179	11	88	90	29	BA
7.2.9	191	19	34	107	154	AB
7.2.10	223	3	46	98	206	BA
7.2.11	227	13	87	159	188	AB
7.2.12	239	7	35	108	142	BA
7.2.13	263	5	45	97	214	AB
7.2.14	269	2	86	169	69	BA
7.2.15	283	3	36	109	128	AB
7.2.16	293	7	44	96	54	BA
7.2.17	311	17	85	179	62	AB
7.2.18	317	3	37	110	281	BA
7.2.19	347	5	43	95	327	AB
7.2.20	359	7	84	189	267	BA

Продовження Таблиці 7.2– El-Gamal, параметри Завдання

№	p	w	Xa	Xb	m	$\overline{V}$
7.2.21	103	12	41	111	61	AB
7.2.22	107	15	59	90	105	BA
7.2.23	131	2	42	105	125	AB
7.2.24	139	3	58	112	62	BA
7.2.25	149	8	99	91	104	AB
7.2.26	167	17	43	106	124	BA
7.2.27	173	19	57	113	63	AB
7.2.28	179	11	98	92	103	BA
7.2.29	191	19	44	107	123	AB
7.2.30	223	3	56	114	64	BA
7.2.31	227	13	97	129	102	AB
7.2.32	239	7	45	108	122	BA
7.2.33	263	5	55	115	65	AB
7.2.34	269	2	96	165	101	BA
7.2.35	283	3	46	109	121	AB
7.2.36	293	7	54	116	66	BA
7.2.37	311	17	95	143	100	AB
7.2.38	317	3	47	110	120	BA
7.2.39	347	5	53	117	67	AB
7.2.40	359	7	94	182	99	BA
7.2.41	367	10	38	112	171	AB
7.2.42	383	5	42	94	292	BA
7.2.43	389	3	83	199	301	AB
7.2.44	419	2	39	113	98	BA
7.2.45	431	7	41	93	67	AB
7.2.46	293	7	252	16	225	BA
7.2.47	311	17	295	43	287	AB
7.2.48	317	3	247	108	231	BA
7.2.49	347	5	253	37	224	AB
7.2.50	359	7	294	82	286	BA
7.2.51	367	10	238	62	232	AB
7.2.52	383	5	242	194	223	BA
7.2.53	389	3	283	97	285	AB
7.2.54	419	2	239	313	235	BA
7.2.55	431	7	241	193	221	AB

8. КРИПТОАЛГОРИТМ RSA

Опис RSA було опубліковано у 1977 році, Рональдом Райвестом, Аді Шаміром і Леонардом Ейделманом з Массачусетського технологічного інституту (MIT). Він працює у повній відповідності до моделей Рис. 4, Рис. 5, Рис. 6, Рис. 7, Рис. 8 і забезпечує у різних режимах розв'язок повного комплексу задач криптографічного захисту даних, наведеного у Розділі 1 [9].

На Рис. 12 представлено його варіант (що відповідає моделям Рис. 4 та Рис. 5) з прикладом для шифрування Відправником А повідомлення M з числовим образом $m_a = 78$ для відправки отримувачеві В [11].

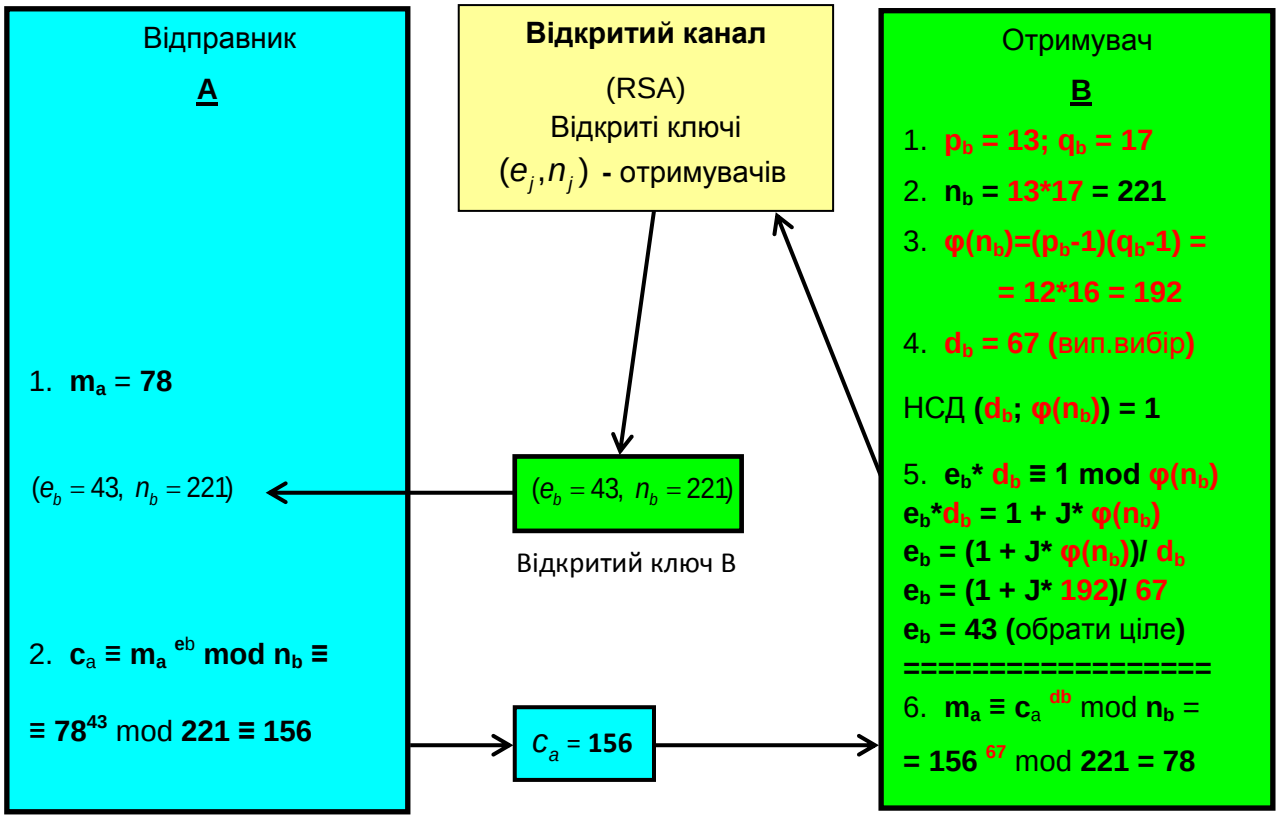

Рисунок 12 - Алгоритм шифрування RSA (модель Рис. 4 та 5)

Згідно алгоритма (Рис. 4 та 5), кожен учасник готує, або отримує від Довіреної третьої сторони власну пару ключів. На Рис. 12 показано процес підготовки пари ключів користувачем В, який забезпечує для себе таким чином можливість отримувати конфіденційні повідомлення від будь-якого учасника

середовища спільного доступу (наприклад, мережа). В даному прикладі - від користувача А.

Підготовка пари ключів, на прикладі користувача В, полягає в наступному (Рис. 12, червоним шрифтом позначено секретні дані, які жодним чином не можна публікувати, чи допускати їх потрапляння до рук зловмисника). Крок 1, суб'єкт В обирає два великих простих числа $p_b = 13$ та $q_b = 17$. На Кроці 2 обчислюється потужність множини алфавіту $n_b = 13 \bullet 17 = 221$. На Кроці 3 обчислюється число Ейлера для $n_b = 221$

$$\varphi(n_b) = \varphi(221) = (p-1) \bullet (q-1) = 12 \bullet 16 = 192 \ .$$

Крок 4, користувач В вибирає випадкове число $d_b = 67$, взаємно-просте із $\varphi(n_b) = 192$, це таке число, для якого найбільший спільний дільник НСД (d_b, $\varphi(n_b)$) = НСД (67,192) = 1 дорівнює одиниці. В даному випадку це виконується. Число $d_b = 67$ є унікальним елементом алфавіту $A_b = \{0,1,2,3,\ldots,220\}$, тому йому призначаємо роль приватного ключа $k_{prb} = d_b = 67$. На Кроці 5 суб'єкт В обчислює елемент $e_b \in A_b$, мультиплікативно обернений до приватного ключа d_b за модулем $\varphi(n_b)$, шляхи такого обчислення ми вже обговорювали вище в Розділі 5 і наприкінці Розділу 7. В даному навчальному прикладі (за невеликого n_b) ми повторимо процедуру переборного типу згідно виразів (44) та (45). У пункті 5 Рис. 12 ця процедура розписана у подібному ж порядку. Перебором цілих $1 \le J < n$ знаходимо ціле $e_b = 43$. Перевіримо оберненість e_b до d_b: $e_b * d_b \equiv 1 \pmod{\varphi(n_b)}$, або ж $43 * 67 \equiv 1 \pmod{192}$. Відкритим ключем суб'єкта В є пара $k_{pbb} = (e_b = 43,\ n_b = 221)$, яка відправляється на сервер відкритих ключів через відкритий канал і у певний момент потрапляє до відправника А на його запит. Нехай, відправник А бажає конфіденційно передати Отримувачу В повідомлення M з числовим образом $m_a = 78$. Він у пункті 2 Рис. 12 обчислює криптограму c_a

$$c_a \equiv m_a^{e_b} \bmod n_b = 78^{43} \bmod 221 = 156,$$

і передає $c_a = 156$ через відкритий канал отримувачеві В. Отримувач В відновлює m_a допіднесенням c_a у степінь свого приватного ключа k_{prb} за $(\bmod n_b)$

$$m_a \equiv c_a^{d_b} \bmod n_b = 156^{67} \bmod 221 = 78.$$

Таким чином, повідомлення M з числовим образом $m_a = 78$ конфіденційно передано через відкритий канал, і забезпечено його цілісність, оскільки ніхто, крім отримувача В не має приватного ключа $k_{prb} = d_b = 67$ і не може за осяжний час його розшифрувати для модифікації.

Алгоритм RSA забезпечує автентифікацію у повній відповідності до моделі Рис. 6, при відповідному порядку застосування ключів. Якщо користувач В зашифрує згідно цій моделі своє повідомлення $m_b = 45$ на приватному ключі $k_{prb} = d_b$, то він отримає криптограму $c_b \equiv m_b^{d_b} \bmod n_b = 45^{67} \bmod 221 = 124$, яку передає до користувача А через відкритий канал. Користувач А може розшифрувати c_b використовуючи публічний ключ k_{pbb}

$$m_b \equiv c_b^{e_b} \bmod n_b = 124^{43} \bmod 221 = 45.$$

Якщо відновлений таким чином текст M є «читабельним», то А може робити висновки про автентичність, і цілісність текста. Конфіденційність тут не забезпечується, оскільки пересвідчитися в автентичності M може і Криптоаналітик, отримавши публічний ключ В, разом з тим він і прочитає M.

Алгоритм RSA забезпечує і інші режими роботи криптосистеми згідно моделей Рис. 6 та Рис. 7 [5,6]. У відповідні кроки додаються процедури хешування і додаткове шифрування/дешифрування (на Рис. 8 - Шифратор

1/Дешифратор 1) з відповідними висновками до цих моделей, що були наведені в Розділі 4.

8.1. Контрольні запитання

8.1.1 Що таке алгоритм RSA?

8.1.2 Що забезпечує криптостійкість алгоритма RSA?

8.1.3 Яке призначення алгоритма RSA?

8.1.4 Які механізми складають основу алгоритма RSA?

8.1.5 Як формується алфавіт користувача в RSA?

8.1.6 Як формується ключ дешифрування в RSA

8.1.7 Як формується ключ зашифрування в RSA?

8.1.8 Як зашифрувати повідомлення M в RSA?

8.1.9 Як дешифрувати криптограму C в RSA?

8.1.10 Як пов’язані ключі шифрування і дешифрування в RSA?

8.1.11 Що таке число Ейлера і його роль в алгоритмі RSA?

8.1.12 Яким алгоритмом знаходять публічний ключ в алгоритмі RSA?

8.1.13 Які дані є публічним ключем в алгоритмі RSA?

8.1.14 Які дані є приватним ключем в алгоритмі RSA?

8.1.15 Які дані в алгоритмі RSA зберігають в секреті від сторонніх?

8.2. Контрольні завдання

Алгоритм RSA та його робочі режими. Забезпечити виконання наступних задач в телекомунікаційній підсистемі ІС, відповідно до типу Завдання:

1 – Конфіденційність **m**;

2- Цілісність + Автентичність **m**;

3 – Конфіденційність + Цілісність + Автентичність **m**.

Параметри Завдання обирати із Таблиці 8.1 за номером варіанта.

Таблиця 8.1 – Варіанти Завдань з робочих режимів алгоритма RSA.

№	Користувач **A**			Користувач B			Direction	Повідомл.	Тип
Вар	n	e	d	n	e	d	V	m	Завдання
1	391	31	159	377	313	73	BA	289	**1**
2	667	331	67	391	31	159	AB	296	**2**
3	667	295	71	391	327	183	BA	385	**3**
4	667	481	73	391	345	201	AB	149	**1**
5	667	39	79	391	157	213	BA	301	**2**
6	667	475	83	391	307	219	AB	212	**3**
7	667	353	89	391	101	237	BA	145	**1**
8	667	489	97	391	41	249	AB	354	**2**
9	667	61	101	391	323	267	BA	237	**3**
10	667	311	103	391	75	291	AB	187	**1**
11	667	403	107	391	79	303	BA	98	**2**
12	667	373	109	391	221	309	AB	215	**3**
13	377	263	23	667	227	19	AB	324	**1**
14	377	121	25	667	333	37	BA	89	**2**
15	377	197	29	667	601	41	AB	119	**3**
16	377	271	31	667	417	65	BA	246	**1**
17	377	109	37	667	367	47	AB	373	**2**
18	377	211	43	667	93	53	BA	281	**3**
19	377	317	53	667	355	59	AB	138	**1**
20	377	131	59	667	101	61	BA	93	**2**
21	377	325	61	667	331	67	AB	334	**3**
22	377	305	65	667	295	71	BA	297	**1**
23	377	331	67	667	481	73	AB	195	**2**
24	377	313	73	667	39	79	BA	151	**3**
25	377	319	79	667	475	83	AB	263	**1**
26	391	79	303	377	233	137	AB	317	**2**
27	391	221	309	377	307	139	BA	107	**3**
28	391	193	321	377	221	149	AB	211	**1**
29	391	183	327	377	247	151	BA	76	**2**
30	391	27	339	377	229	157	AB	259	**3**
31	391	251	115	377	235	163	BA	344	**1**
32	391	147	91	377	311	215	AB	168	**2**
33	391	71	119	377	101	173	BA	182	**3**
34	391	163	203	377	107	179	AB	361	**1**
35	391	73	217	377	299	227	BA	146	**2**

9. ПІСЛЯМОВА

У Навчальному посібнику «Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах», Частина 1, висвітлено ряд вибраних важливих тем з групи дисциплін із інформаційної стійкості комп'ютерних технологій та мереж, захисту інформації та інформаційної безпеки у мережах, проектування комплексних систем захисту інформації зокрема, моделі криптосистем, математичні засади криптоперетворень, сучасні асиметричні криптоалгоритми.

У цю частину не ввійшли такі теми, як Схеми постановки та верифікації Електронного цифрового підпису (ЕЦП), Схема ЕЦП Ель-Гамаль, Схема ЕЦП RSA, Схема ЕЦП DSA, Стандарт ЕЦП DSS, Сертифікати публічних (відкритих) ключів, Протокол X.509 та життєвий цикл Сертифікатів публічних ключів, Криптографія на еліптичних кривих ECC. Вони складуть основний зміст навчального посібника «Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах», Частина 2, який автор планує укласти надалі.

На завершення Частини 1 варто згадати думку знаного експерта в галузі криптографії Б. Шнайєра [5]. Жоден криптоалгоритм сам по собі нікого і ні від чого не захищає. Кожен з них має свої переваги і недоліки, свої сильні і слабкі сторони. Тому гарна, стійка криптосистема має вигляд процедури, складеної із багатьох дій і кроків, де ті чи інші криптоалгоритми можуть бути лише простим кроком у послідовності захисних дій. Така криптосистема набуває назви Протокол. У Протоколі, сильними сторонами одних криптоалгоритмів, або спеціальними діями чи обмеженнями, прикривають слабкі сторони інших криптоалгоритмів. Питання у такій постанові наближаються до залучення криптоаналіза до дослідження методів і засобів захисту інформації. Але це вже тема для окремого теоретичного і практичного матеріалу.

ПЕРЕЛІК ПОСИЛАНЬ

1. Полторак В.П. Теорія інформації та кодування: Підручник / Жураковський Ю.П., Полторак В.П. - К. : Вища школа, 2001. - 255 с. : іл.

2. ДСТУ 2392-94 Інформація та документація. Базові поняття.

3. Про Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.1999 № 1229/99, редакція від 04.05.2008. - Електронні текстові дані (1 файл: 16 Кбайт). – Київ : Верховна Рада України, 2020. - Назва з екрана. Доступ : http://zakon2.rada.gov.ua/laws/show/1229/99

4. Скляр Бернард. Цифровая связь. Теоретические основы и практическое применение, 2-е издание: Пер. с англ. / Б. Скляр. - М. : Издательский дом «Вильямс», 2003. - 1104 с. : ил.

5. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на С. / Б. Шнайер. – М. : Изд-во ТРИУМФ, 2002. – 816 с. : ил.

6. Тилборг ван Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник. / Х.К.А. ван Тилборг. – М. : Мир, 2006. – 471 с. : ил.

7. Модель. [Електронний ресурс]. - Назва з екрана. Доступ : https://uk.wikipedia.org/wiki/Модель

8. Горбенко И.Д. О новом украинском стандарте шифрования. / Р. Олейников, И.Д. Горбенко. [Електронний ресурс]. - Назва з екрана. Доступ: https://ko.com.ua/o_novom_ukrainskom_standarte_shifrovaniya_110863

9. Полторак В.П. Криптографічний захист даних в цифрових інформаційних системах. (Ч. 1) / В.П. Полторак // Телеком. Військовий зв'язок. hi-Tech.ua, спец. випуск, №2 : Военная связь. – Київ: СофтПресс, 2018/10. – С. 98–104.

10. Полторак В.П. Криптографічний захист даних в цифрових інформаційних системах. (Ч. 2) / В.П. Полторак // Телеком. Військовий зв'язок. hi-Tech.ua, спец. випуск, №1 : Военная связь. – Київ: СофтПресс, 2019/4. – С. 81–85.

11. Полторак В.П. Криптографічний захист даних в цифрових інформаційних системах. (Ч. 3) / В.П.Полторак // Телеком. Військовий зв'язок. hi-Tech.ua, спец. випуск, №2: Военная связь. – Київ: СофтПресс, 2019/10. – С. 64–67.

Додаток А

Таблиця А.1 - Перші прості числа до 1000

2	**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**

Електронне мережне навчальне видання

Полторак Вадим Петрович

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ЗАХИСТ ДАНИХ В КОМП'ЮТЕРНИХ ТЕХНОЛОГІЯХ І МЕРЕЖАХ

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Свідоцтво про державну реєстрацію: серія ДК №5354 від 25.05.2017 р.
просп. Перемоги, 37,
м. Київ, 03056