МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

КАРПІВ Віталій Андрійович

Ймовірнісний аналіз стійкості системи захисту інформації методом цілочисельного розщеплення /Probabilistic Analysis of Information Security System Stability by Integer Splitting Method

спеціальність: 125 – Кібербезпека та захист інформації

освітньо-професійна програма –Кібербезпека

Кваліфікаційна робота

Виконав студент групи КБм -21
В.А. Карпів

Науковий керівник
д.т.н., професор М.М.Касянчук

Кваліфікаційну роботу допущено
до захисту:

«____» _____ ___2024 р.

Завідувач кафедри
_____ В.В.Яцків

ТЕРНОПІЛЬ – 2024

Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки
Освітній ступінь «магістр»
спеціальність: 125 – Кібербезпека та захист інформації
освітньо-професійна програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ В.В.Яцків
«____» _____ 2023 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
КАРПІВ ВІТАЛІЙ АНДРІЙОВИЧ

1. Тема кваліфікаційної роботи:
Ймовірнісний аналіз стійкості системи захисту інформації методом цілочисельного розщеплення / Probabilistic Analysis of Information Security System Stability by Integer Splitting Method

керівник роботи: д.т.н., професор М.М. Касянчук
затверджені наказом по університету від 12 грудня 2023 року № 753.
2. Строк подання студентом закінченої кваліфікаційної роботи 12 грудня 2024 р.

3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.

4. Основні питання, які потрібно розробити:
– формулювання необхідних основних понять, визначень, тверджень;
– представлення процедури цілочисельного розщеплення за відповідною базою;
– розробка алгоритмів процедури цілочисельного розщеплення та відновлення числа;
– розробка методу цілочисельного розщеплення з методами захисту інформації на основі модулярної арифметики;
– імовірнісний аналіз стійкості захисту інформації методом цілочисельного розщеплення;
– реалізація та ілюстрація роботи методу захисту інформації на основі цілочисельного розщеплення.

5. Перелік графічного матеріалу у роботі:
– блок-схема алгоритму цілісного розщеплення числа a по базі r при рівні розщеплення;
– кросовер "діагональ по діагоналі";

– порівняння традиційних, абсолютно стійких методів захисту з розщепленням;

– поведінка ймовірності несанкціонованого відновлення вихідного тексту за різних значень розміру простору гами;

– відновлений текст;

– ключ захисту;

– захищений текст у відповідності з ключем захисту.

6. Консультанти розділів кваліфікаційної роботи

	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 12 грудня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Аналіз сучасних підходів цілочисельного розщеплення	12.2023 р. – 03.2024 р.	
2	Алгоритмічне забезпечення процедури цілочисельного розщеплення	03.2024 р. – 06.2024 р.	
3	Реалізація та імовірнісний аналіз стійкості системи захисту інформації методом цілочисельного розщеплення	06.2024 р. – 11.2024 р.	

Студент _____ Карпів В.А.
(підпис)

Керівник роботи _____ д.т.н., професор М.М.Касянчук

АНОТАЦІЯ

Випускна кваліфікаційна робота на тему „Ймовірнісний аналіз стійкості системи захисту інформації методом цілочисельного розщеплення” на здобуття освітнього ступеня «Магістр» зі спеціальності 125 „Кібербезпека та захист інформації” освітньо-професійної програми «Кібербезпека» написана обсягом 81 сторінок і містить 27 ілюстрацій, 10 таблиць, 1 додаток та 33 джерела за переліком посилань.

Метою випускної кваліфікаційної роботи є ймовірнісний аналіз стійкості системи захисту інформації методом цілочисельного розщеплення.

Методи дослідження. Методи дослідження стійкості, статистичні методи, методи моделювання.

Результати дослідження. Здійснено аналіз сучасних підходів до захисту інформації методом цілочисельного розщеплення, що дало можливість обгрунтувати вибір відповідних алгоритмів захисту інформації та дослідити їх стійкість на основі імовірнісного аналізу. Розроблено алгоритмічне забезпечення для процедури цілочисельного розщеплення та відновлення числа, що дозволило здійснити порівняння методів захисту інформації на основі модулярної арифметики та цілочисельного розщеплення. Проведено імовірнісний аналіз стійкості захисту інформації методом цілочисельного розщеплення, що дозволило встановити його переваги та недоліки в порівнянні з існуючими цілочисельними методами захисту інформації. Виконана програмна реалізація методу захисту інформації на основі цілочисельного розщеплення, розроблено схему та інтерфейс роботи методу.

Результати роботи можуть успішно застосовуватися для захисту інформації на основі цілочисельного розщеплення.

КЛЮЧОВІ СЛОВА: ЦІЛОЧИСЕЛЬНЕ РОЗЩЕПЛЕННЯ, ЙМОВІРНІСТЬ, АНАЛІЗ СТІЙКОСТІ, ЗАХИСТ ІНФОРМАЦІЇ, ВІДНОВЛЕННЯ ЧИСЛА.

ABSTRACT

The graduate work on the topic „Probabilistic Analysis of Information Security System Stability by Integer Splitting Method” for Master’s degree on speciality 125 "Cybersecurity and information protection" is written on 81 pages and contains 27 illustrations, 10 tables, 1 suplement and 33 references.

The aim of graduate work is a probabilistic analysis of the stability of an information protection system using the integer splitting method.

Research methods. Methods of studying stability, statistical methods, modeling methods.

Results of the study. An analysis of modern approaches to information protection using the integer splitting method was carried out, which made it possible to justify the choice of appropriate information protection algorithms and to investigate their stability based on probabilistic analysis. Algorithmic support for the procedure of integer splitting and number recovery has been developed, which allowed to compare information protection methods based on modular arithmetic and integer splitting. A probabilistic analysis of the stability of information protection using the integer splitting method has been carried out, which allowed to establish its advantages and disadvantages in comparison with existing integer methods of information protection. A software implementation of the information protection method based on integer splitting has been performed, a scheme and interface of the method have been developed.

The results of the work can be successfully applied to information protection based on integer splitting.

Keywords: INTEGER SPLITTING, PROBABILITY, STABILITY ANALYSIS, INFORMATION PROTECTION, NUMBER RECOVERY.

ЗМІСТ

ВСТУП

В даний час арифметика в залишках активно застосовується в цифровій обробці сигналів [1-3], обробці зображень [4-5], у розподілених інфокомунікаційних системах [6-8], бездротових сенсорних мережах [9-11], засобах забезпечення множинного доступу з кодовим поділом каналів [12-15], виявлення та виправлення помилок [16-19], у системах інформаційної безпеки [20-23], хмарних обчисленнях [24-25] тощо.

Згідно з літературою [26-28], всі відомі симетричні алгоритми, такі як DES, AES, Rijndael, гамування, TEA, IDEA, ГОСТ 28147-89, MARS, RC6, Serpent, Twofish та ін., а також асиметричні алгоритми, наприклад: RSA, Рабіна, Ель-Гамаля, Мак-Еліса та ін. не передбачають якихось інших способів підвищения ступеня безпеки вказаних методів захисту у відношенні несанкціонованого доступу в каналах передачі та зберігання інформації.

На сьогоднішній день багато із відомих методів захисту даних грунтуються на операції ділення націло з остачею, таких як метод Цезаря, афінна система підстановок Цезаря, метод Хілла, метод Віженера тощо [29-31]. Однак у цих методах не розглядалося питання багатократного застосування цієї операції для кожного символу з метою підвищення рівня безпеки і створення додаткових труднощів для контролю повідомлень, що передаються зі сторони несанкціонованого користувача.

У відношенні математичних методів, які використовуються в даній роботі, випливає, що запропонований аналіз є розвитком відомих ймовірнісних підходів, розроблених після класичних досліджень К.Шеннона та інших спеціалістів по теорії інформації.

Подібні методи були розвинені із забезпеченням ефективної мети функціонування мереж і систем зв'язку, а також забезпечення роботи складних динамічних систем, в яких постає питання захисту як від незалежних зовнішніх впливів, так і від можливості стороннього втручання. Зокрема, питання захисту

інформації виникають в системах широкосмугової мобільної комунікації і в ідеяких задачах еволюційного розвитку технічних та біологічних систем.

Запропонований метод цілочисельного розщеплення забезпечує надійніший захист від різних криптоаналітичних атак, заснованих на підрахунку частот появи літер в захищеному тексті. Цей метод також слабо залежить також від розподілу ймовірностей літер у природній мові. Тому тема роботи є актуальною.

Мета роботи. Метою даної роботи є ймовірнісний аналіз стійкості системи захисту інформації методом цілочисельного розщеплення.

Для вирішення поставленої мети вирішуються наступні **завдання**:

– формулювання необхідних основних понять, визначень, тверджень;

– представлення процедури цілочисельного розщеплення за відповідною базою;

– розробка алгоритмів процедури цілочисельного розщеплення та відновлення числа;

– розробка методу цілочисельного розщеплення з методами захисту інформації на основі модулярної арифметики;

– імовірнісний аналіз стійкості захисту інформації методом цілочисельного розщеплення;

– реалізація та ілюстрація роботи методу захисту інформації на основі цілочисельного розщеплення.

Об’єкт дослідження. Процес дослідження стійкості системи захисту інформації методом цілочисельного розщеплення.

Предмет дослідження. Методи і засоби дослідження стійкості системи захисту інформації методом цілочисельного розщеплення.

Методи дослідження. Методи дослідження стійкості, статистичні методи, методи моделювання.

Наукова новизна одержаних результатів.

1. Здійснено аналіз сучасних підходів до захисту інформації методом цілочисельного розщеплення, що дало можливість обгрунтувати вибір

відповідних алгоритмів захисту інформації та дослідити їх стійкість на основі імовірнісного аналізу.

2. Розроблено алгоритмічне забезпечення для процедури цілочисельного розщеплення та відновлення числа, що дозволило здійснити порівняння методів захисту інформації на основі модулярної арифметики та цілочисельного розщеплення.

3. Проведено імовірнісний аналіз стійкості захисту інформації методом цілочисельного розщеплення, що дозволило встановити його переваги та недоліки в порівнянні з існуючими цілочисельними методами захисту інформації.

Практичне значення отриманих результатів. Виконана програмна реалізація методу захисту інформації на основі цілочисельного розщеплення, розроблено схему та інтерфейс роботи методу.

Публікації та апробація КР.

1. Карпів В., Момотюк О., Касянчук М. Математична модель захисту інформації на основі цілочисельного розщеплення. Збірник матеріалів науково - практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ-2024), Тернопіль, 2024. С.115-117 [32].

2. Карпів В., Крук О., Казьмірчук Н. Імовірнісний аналіз стійкості методу розщеплення для захисту інформації. Матеріали науково-практичного симпозіуму «Захист інформації». Тернопіль, 2024. С.89-92 [33].

1 АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ЦІЛОЧИСЕЛЬНОГО РОЗЩЕПЛЕННЯ

1.1 Основні визначення та поняття

Нехай дано два додатних цілих числа r і a , для яких виконується нерівність $0<a<r$. Цілочисельним розщепленням числа a за базою r називається подання числа a у вигляді послідовності чисел a_1, a_2, a_3, …, a_{k-1}, a_k, в якій виконуються такі рівності:

$$a_1=\delta^{(2)}, \text{ де } \delta^{(2)}=r \bmod a,$$

$$a_2=\delta^{(3)}, \text{ де } \delta^{(3)}=r \bmod q^{(2)},\ q^{(2)}=\left\lfloor \frac{r}{a} \right\rfloor,$$

$$a_3=\delta^{(4)}, \text{ де } \delta^{(4)}=r \bmod q^{(3)},\ q^{(3)}=\left\lfloor \frac{r}{q^{(2)}} \right\rfloor, \qquad (1.1)$$

…….

$$a_{k-1}=\delta^{(k)}, \text{ де } \delta^{(k)}=r \bmod q^{(k-1)},\ q^{(k-1)}=\left\lfloor \frac{r}{q^{(k-2)}} \right\rfloor,$$

$$a_k=q^{(k)}, \text{ де } q^{(k)}=\left\lfloor \frac{r}{q^{(k-1)}} \right\rfloor,$$

де $\delta^{(2)}$ – залишок при цілочисельному діленні r на a, а $q^{(i)}$ – ціла частина при такому діленні;

$\delta^{(i)}$ – залишок при цілочисельному діленні r на $q^{(i-1)}$;

символ $\lfloor\ \rfloor$ означає округлення до найближчого цілого в меншу сторону.

Натуральне число k називається рівнем розщеплення.

Цілочисельне розщеплення являє собою певне узагальнення відомої математичної операції ділення із залишком. Блок-схема цілочисельного розщеплення числа a за базою r при рівні розщеплення k представлена на рисунку 1.1.

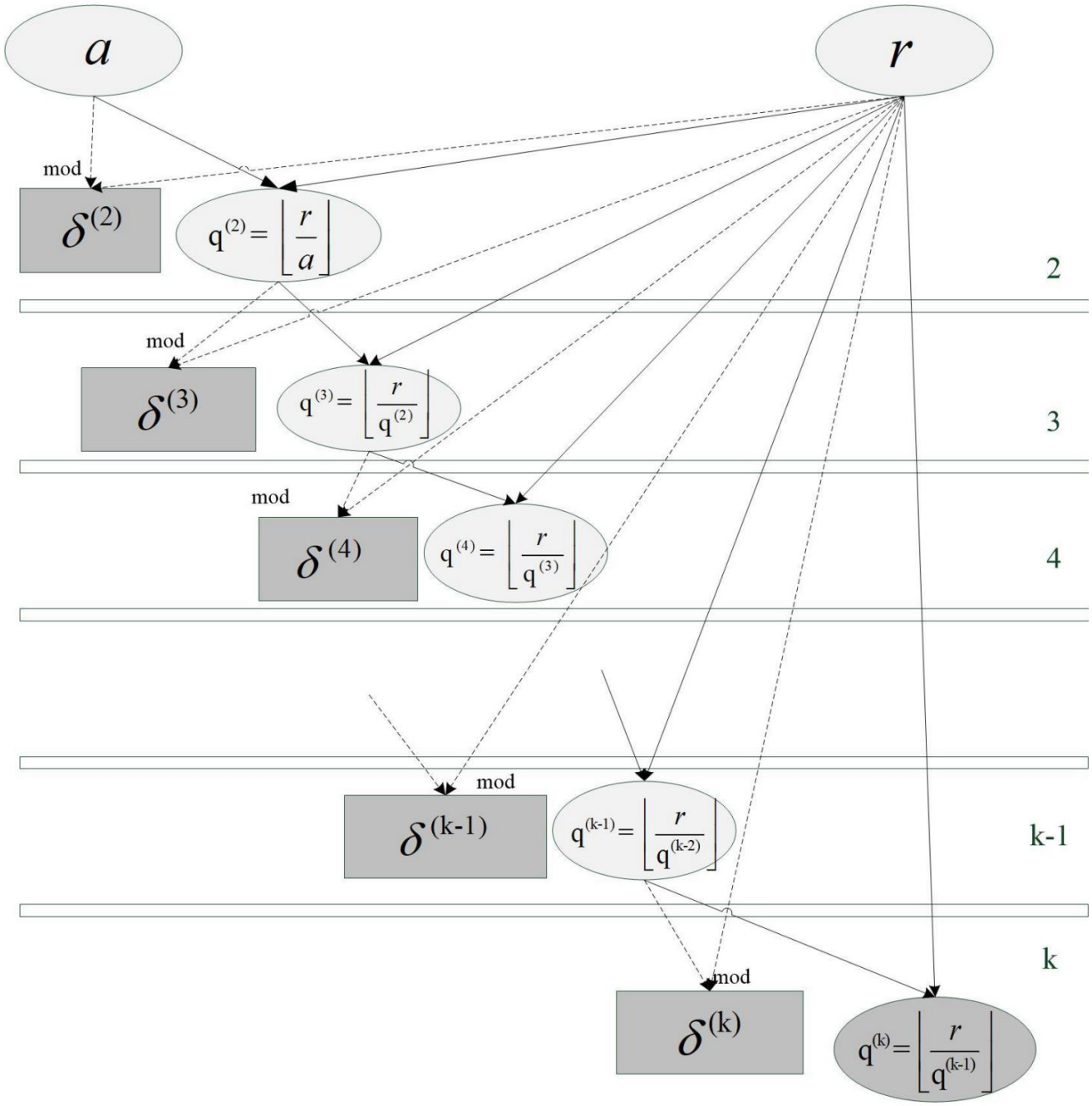

Рисунок 1.1 − Блок-схема цілочисельного розщеплення числа *a* за базою *r* при рівні розщеплення *k*

Функцією відображення $\Phi_k(a, r)$ називається результат цілочисельного розщеплення числа *a* за основою *r*.

Відповідно до (1.1), функція відображення $\Phi_k(a, r)$ при рівні розщеплення, що дорівнює *k*, задається наступним співвідношенням:

$$\Phi_k(a, r)=(\delta_a^{(2)}, \delta_a^{(3)}, \delta_a^{(4)}, \ldots, \delta_a^{(k-1)}, \delta_a^{(k)}, q_a^{(k)}). \quad (1.2)$$

Наприклад, відображення $\Phi_k(a, r)$ при рівні розщеплення k=3 визначається наступним співвідношенням: $\Phi_3(a, r)=(\delta_a^{(2)}, \delta_a^{(3)}, q_a^{(3)})$.

1.2 Формулювання основних тверджень та їх доведення

Зазначені вище визначення дозволяють сформулювати та представити доведення ряду тверджень.

Твердження 1. Нехай задана пара цілих чисел r і a, де $a\neq0$. Тоді існує єдине поєднання цілих чисел q і δ, які задовольняють співвідношенню $r=a\times q+\delta$, де $0\leq\delta<|a|$. Це є основною теоремою арифметики і її доведення наводиться в багатьох літературних джерелах з алгебри і теорії чисел.

Твердження 2. Цілочисленне розщеплення $\Phi_k(a, r)$ є ін'єктивним, тобто виконується така властивість:

$$\text{якщо } a\neq b, \text{ то маємо } \Phi_k(a, r)\neq \Phi_k(b, r). \quad (1.3)$$

Доведення.

Доведення твердження, коли k=2. При рівні розщеплення k=2 вірно:

$$\Phi_2(a, r)=(\delta_a^{(2)}, q_a^{(2)}); \quad (1.4)$$

$$\Phi_2(b, r)=(\delta_b^{(2)}, q_b^{(2)}). \quad (1.5)$$

Твердження (1.3) при k=2 задається наступною формулою:

$$\text{при } a\neq b \text{ маємо } \Phi_2(a, r)= \Phi_2(b, r). \quad (1.6)$$

Згідно (1.4) та (1.5) результат дії такого відображення (1.6), очевидно, є впорядкованою парою, і твердження 2 приводить до наступної формули:

$$\text{при } a \neq b \text{ маємо } (\delta_a^{(2)}, q_a^{(2)}) \neq (\delta_b^{(2)}, q_b^{(2)}). \quad (1.7)$$

Далі потрібно використати доведення від протилежного. Припустимо, що формула (1.7) неправильна. Це призводить до наступної формули:

$$\text{при } a \neq b \text{ маємо } (\delta_a^{(2)}, q_a^{(2)}) = (\delta_b^{(2)}, q_b^{(2)}). \quad (1.8)$$

З твердження 1 випливає, що ділення із залишком для будь-якого числа на інше число однозначне, тобто частка та залишок визначаються єдиним чином. З рівностей ($\delta_a^{(2)} = \delta_b^{(2)}$) і ($q_a^{(2)} = q_b^{(2)}$) слідує, що $a=b$ суперечить умові $a \neq b$. Отримана суперечність показує, що вихідне припущення (1.8) було невірним, і збіг двох пар ($\delta_a^{(2)}$, $q_a^{(2)}$) і ($\delta_b^{(2)}$, $q_b^{(2)}$) неможливо. І тому властивість $\Phi_2(a, r) \neq \Phi_2(b, r)$ досягнута. Твердження 2 доведено при $k=2$.

Доведення твердження у випадку, коли $k=n+1$.

Нехай, за припущенням індукції, твердження правильне при $k=n$. Твердження 2 визначається наступним співвідношенням при $k=n$:

$$\text{при } a \neq b \text{ маємо } \Phi_n(a, r) = \Phi_n(b, r). \quad (1.9)$$

І наступні послідовності не збігаються при $a \neq b$ згідно (1.3):

$$(\delta_a^{(2)}, \delta_a^{(3)}, \delta_a^{(4)}, \ldots, \delta_a^{(n-1)}, \delta_a^{(n)}, q_a^{(n)}) \neq (\delta_b^{(2)}, \delta_b^{(3)}, \delta_b^{(4)}, \ldots, \delta_b^{(n-1)}, \delta_b^{(n)}, q_b^{(n)}). \quad (1.10)$$

Далі використовується індукція по n:

1) при $k=2$ доведено вище;

2) нехай твердження справедливе при $k=n$. З рівняння (1.10) випливає, що якщо функція Φ_n є ін'єктивним відображенням, то, принаймні, один з компонентів не збігається, тобто:

$$\text{або } \delta_a^{(2)} \neq \delta_b^{(2)}; \tag{1.11}$$

$$\text{або } \delta_a^{(3)} \neq \delta_b^{(3)}; \tag{1.12}$$

$$\text{або } \delta_a^{(4)} \neq \delta_b^{(4)}; \tag{1.13}$$

……..

$$\text{або } \delta_a^{(n)} \neq \delta_b^{(n)}; \tag{1.14}$$

$$\text{або } q_a^{(n)} \neq q_b^{(n)}; \tag{1.15}$$

3) потрібно довести твердження при $k=n+1$:

$$\text{при } a \neq b \text{ маємо } \Phi_{n+1}(a, r) \neq \Phi_{n+1}(b, r). \tag{1.16}$$

Справді, при $a \neq b$ маємо:

$$(\delta_a^{(2)}, \delta_a^{(3)}, \delta_a^{(4)}, \ldots, \delta_a^{(n)}, \delta_a^{(n+1)}, q_a^{(n+1)}) \neq (\delta_b^{(2)}, \delta_b^{(3)}, \delta_b^{(4)}, \ldots, \delta_b^{(n)}, \delta_b^{(n+1)}, q_b^{(n+1)}). \tag{1.17}$$

При порівнянні двох рівнянь (1.11) та (1.10), можна відзначити, що компоненти від $\delta_a^{(2)}$ до $\delta_a^{(n)}$ збігаються для випадків $k=n$ і $k=n+1$, а також, компоненти від $\delta_b^{(2)}$ до $\delta_b^{(n)}$ збігаються для випадків $k=n$ і $k=n+1$. А лише останній компонент $q_a^{(n)}$ у нерівності (1.10) замінюється двома компонентами $q_a^{(n+1)}$ і $\delta_a^{(n+1)}$ в нерівності (1.17), а також останній компонент $q_b^{(n)}$ в нерівності (1.10) замінюється двома компонентами $q_b^{(n+1)}$ і $\delta_b^{(n+1)}$ у нерівності (1.17). Звідси для (1.17) маємо два варіанти:

а) або один або кілька компонентів від $\delta_a^{(2)}$ до $\delta_a^{(n)}$ не збігається з компонентами від $\delta_b^{(2)}$ до $\delta_b^{(n)}$, і тоді в силу рівнянь (1.11), (1.12), (1.13) і (1.14), це означає, що маємо $\Phi_{n+1}(a, r) \neq \Phi_{n+1}(b, r)$;

б) або компоненти від $\delta_a^{(2)}$ до $\delta_a^{(n)}$ збігаються з відповідними компонентами від $\delta_b^{(2)}$ до $\delta_b^{(n)}$. В цьому випадку в рівнянні (1.10) залишився один компонент $q_a^{(n)}$, який не збігається з компонентом $q_b^{(n)}$ через співвідношення (1.15), яке говорить, що $q_a^{(n)} \neq q_b^{(n)}$. Однак цей компонент при $k=n+1$ у рівнянні (1.17) замінений двома компонентами $q_a^{(n+1)}$, $\delta_a^{(n+1)}$ і $q_b^{(n+1)}$, $\delta_b^{(n+1)}$, тому в цій ситуації знову виникає два варіанти в рівнянні (1.17):

- інші компоненти $q_a^{(n+1)}$, $\delta_a^{(n+1}$ збігаються з $q_b^{(n+1)}$,

$$\text{тоді } q_a^{(n+1)} = q_b^{(n+1)} = q; \tag{1.18}$$

$$\text{а також } \delta_a^{(n+1)} = \delta_b^{(n+1)} = \delta. \tag{1.19}$$

Оскільки з формул (1.1), (1.10), (1.17), (1.18) та (1.19) випливає, що $r = q_a^{(n)} \cdot q_a^{(n+1)} + \delta_a^{(n+1)}$ і тоді $q_a^{(n)} = \dfrac{r - \delta_a^{(n+1)}}{q_a^{(n+1)}}$, то отримуємо

$$q_a^{(n)} = \frac{r - \delta}{q}. \tag{1.20}$$

Оскільки з (1.1), (1.10), (1.17), (1.18) та (1.19) випливає $r = q_b^{(n)} \cdot q_b^{(n+1)} + \delta_b^{(n+1)}$ і, отже $q_b^{(n)} = \dfrac{r - \delta_b^{(n+1)}}{q_b^{(n+1)}}$, то отримуємо

$$q_b^{(n)} = \frac{r - \delta}{q}. \tag{1.21}$$

З рівнянь (1.20) та (1.21) отримуємо, що $q_a^{(n)} = q_b^{(n)}$. Таким чином, цей варіант виключається, оскільки він не відповідає початковій умові в даному пункті, а саме $q_a^{(n)} \neq q_b^{(n)}$;

- якщо принаймні один із компонентів $q_a^{(n+1)}$, $\delta_a^{(n+1)}$ не збігається з компонентами $q_b^{(n+1)}$, $\delta_b^{(n+1)}$, то це означає, що

$$\Phi_{n+1}(a, r) \neq \Phi_{n+1}(b, r). \quad (1.22)$$

Вказані випадки призводять до того, що збіг послідовностей неможливий, тобто:

$$\text{якщо } a \neq b, \text{ то } \Phi_{n+1}(a, r) \neq \Phi_{n+1}(b, r). \quad (1.23)$$

Таким чином, згідно з принципом математичної індукції, з $a \neq b$ випливає, що нерівність $\Phi_k(a, r) \neq \Phi_k(b, r)$ справедлива для будь-якого натурального k. Отже, твердження 2 доведено.

Твердження 3. Нехай задана послідовність чисел $a_1, a_2, a_3, \ldots, a_{k-1}, a_k$, що задовольняє умовам $1 \leq a_k \leq r$ і $0 \leq a_i \leq r$, $i = 1, 2, \ldots, k\text{-}1$. Тоді існує таке ціле число a, $0 < a < r$, розщепленням якого є ця послідовність.

Доведення. Нехай задана послідовність:

$$a_1^{(2)}, a_2^{(3)}, a_3^{(4)}, \ldots, a_{k-2}^{(k-1)}, a_{k-1}^{(k)}, a_k^{(k)}. \quad (1.24)$$

Верхній індекс над кожним цілим числом у послідовності являє собою рівень розщеплення під час його створення. Крім того, нехай задано ціле число r, яке використовувалося під час розщеплення при створенні цієї послідовності.

З твердження 1 та визначення (1.1) маємо рівняння:

$$r = q_a^{(k-1)} \cdot a_k^{(k)} + a_{k-1}^{(k)}. \quad (1.25)$$

Співвідношення (1.25) призводить до наступного рівняння:

$$q_a^{(k-1)} = \frac{r - a_{k-1}^{(k)}}{a_k^{(k)}}. \quad (1.26)$$

Згідно (1.26), якщо замінити значення двох останніх цілих чисел $a_{k\text{-}1}{}^{(k)}$, $a_k{}^{(k)}$ значенням цілого числа $q_a{}^{(k\text{-}1)}$, то отримаємо нову послідовність чисел:

$$a_1{}^{(2)}, a_2{}^{(3)}, a_3{}^{(4)}, \ldots, a_{k\text{-}2}{}^{(k\text{-}1)}, a_{k\text{-}1}{}^{(k\text{-}1)}, \quad (1.27)$$

$$a_{k-1}^{(k-1)} = q_a^{(k-1)} = \frac{r - a_{k-1}^{(k)}}{a_k^{(k)}}. \quad (1.28)$$

Тим самим від k чисел у послідовності (1.24) можна перейти до k-1 числа. Діючи так k-1 разів, отримується число $a_1{}^{(1)}=a$.

Доведемо, що вихідна послідовність є розщепленням цього числа a. Спочатку доводиться твердження, коли k=2. При k=2 послідовність (1.24) матиме такий вигляд:

$$a_1{}^{(2)}, a_2{}^{(2)}. \quad (1.29)$$

Згідно (1.2) при рівні розщеплення k=2 випливає:

$$\Phi_2(a, r)=(\delta_a{}^{(2)}, q_a{}^{(2)}). \quad (1.30)$$

З твердження 1 та (1.1) маємо рівняння:

$$r=a\cdot q_a{}^{(2)}+\delta_a{}^{(2)}. \quad (1.31)$$

Співвідношення (1.31) призводить до наступного рівняння:

$$a = \frac{r - \delta_a^{(2)}}{q_a^{(2)}}. \quad (1.32)$$

В силу рівняння (1.28) отримаємо таке співвідношення:

$$a_1^{(1)} = \frac{r - a_1^{(2)}}{a_2^{(2)}}. \tag{1.33}$$

З (1.32), (1.33) та твердження 1 випливає, що частка та залишок визначаються єдиним чином. Це призводить до таких результатів:

$$(a_1{}^{(2)}=\delta_a{}^{(2)}); \tag{1.34}$$

$$(a_2{}^{(2)}=q_a{}^{(2)}). \tag{1.35}$$

Шляхом заміни цілих чисел $\delta_a{}^{(2)}$ і $q_a{}^{(2)}$ з (1.34) та (1.35) у рівнянні (1.32) отримується наступний вираз:

$$a = \frac{r - \delta_a^{(2)}}{q_a^{(2)}} = \frac{r - a_1^{(2)}}{a_2^{(2)}}. \tag{1.36}$$

Це означає, що ціле число a витягується з послідовності (1.29), коли k=2. Твердження 3 доведено при k=2.

Для доведення твердження у випадку, коли k>2 використовується індукція по n. При k=2 твердження 3 було доведено вище.

Нехай твердження справедливе при k=n. Тоді послідовність (1.24) матиме такий вигляд:

$$a_1{}^{(2)}, a_2{}^{(3)}, a_3{}^{(4)}, \ldots, a_{n-2}{}^{(n-1)}, a_{n-1}{}^{(n)}, a_n{}^{(n)}. \tag{1.37}$$

Нехай за припущенням індукції твердження 3 вірне при k=n. Це означає, що послідовність (1.37) буде відновлена до одного цілого числа a. З твердження 1 маємо рівняння:

$$r=N_1\cdot a_n^{(k-1)}\cdot a_n^{(n)}+N_2, \tag{1.38}$$

де N_1 та N_2, $0\le N_2<a_n^{(n)}$ можуть бути будь-якими позитивними числами. З (1.38) маємо:

$$a_n^{(n)}=\frac{r-N_2}{N_1}. \tag{1.39}$$

Тепер потрібно довести твердження при $k=n+1$. Тоді послідовність (1.24) матиме такий вигляд:

$$a_1^{(2)}, a_2^{(3)}, a_3^{(4)}, \ldots, a_{n-2}^{(n-1)}, a_{n-1}^{(n)}, a_n^{(n+1)}, a_{n+1}^{(n+1)}. \tag{1.40}$$

В силу рівняння (1.28) отримаємо такий вираз:

$$a_n^{(n)}=\frac{r-a_n^{(n+1)}}{a_{n+1}^{(n+1)}}. \tag{1.41}$$

З (1.39), (1.41) та твердження 1 випливає, що частка та залишок визначаються єдиним чином. Це призводить до наступного:

$$(N_2=a_n^{(n+1)}), \tag{1.42}$$

$$(N_1=a_{n+1}^{(n+1)}). \tag{1.43}$$

З (1.42) та (1.43) випливає:

$$a_n^{(n)}=\frac{r-N_2}{N_1}=\frac{r-a_n^{(n+1)}}{a_{n+1}^{(n+1)}}. \tag{1.44}$$

Відповідно до (1.44) шляхом заміни двох останніх цілих чисел $a_n^{(n+1)}$, $a_{n+1}^{(n+1)}$ в послідовності (1.40) на отримане ціле число $a_n^{(n)}$ буде сформована нова послідовність:

$$a_1^{(2)}, a_2^{(3)}, a_3^{(4)}, \ldots, a_{n-2}^{(n-1)}, a_{n-1}^{(n)}, a_n^{(n)}. \quad (1.45)$$

Послідовність (1.45) збігається з послідовністю (1.37), а послідовність (1.37), за припущенням індукції, може бути відновлена до єдиного цілого числа, що збігається з a. Через те, що послідовність (1.45) була отримана з послідовності (1.40), в результаті отримується, що за послідовністю (1.40) може бути відновлене ціле число a. Твердження 3 доведено при $k=n+1$.

Таким чином, згідно з принципом математичної індукції, вихідна послідовність є розщепленням одного числа a і це справедливо для будь-якого натурального k.Твердження 3 доведено.

1.3 Процедура цілочисельного розщеплення за відповідною базою

Нехай дані $r>a\geq 1$ і $a_1, a_2, a_3, \ldots, a_{k-1}, a_k$, тобто результат цілочисельного розщеплення a за базою r, тоді виконуються такі співвідношення: $1\leq a_i<r$, $i=1, 2, \ldots, k-1$ і $0\leq a_k\leq r$.

Для доведення використовується математична індукція за n. При $k=2$ послідовність матиме такий вигляд:

$$a_1, a_2. \quad (1.46)$$

З твердження 1 та (1.1) маємо рівняння:

$$a_1=r \bmod a \Rightarrow 0\leq a_1<|a|<r\Rightarrow 0\leq a_1<r. \quad (1.47)$$

Відповідно до (1.1) маємо рівняння:

$$a_2 = \left\lfloor \frac{r}{a} \right\rfloor. \tag{1.48}$$

$$r=a+N_2, \tag{1.49}$$

де $N_2 \geq 0$ може бути будь-яким позитивним числом.

Звідси маємо

$$\frac{r}{a} = \frac{a+N_2}{a}. \tag{1.50}$$

Шляхом застосування операції округлення до найближчого цілого числа з рівняння (1.50) випливає:

$$\left\lfloor \frac{r}{a} \right\rfloor = \left\lfloor \frac{a+N_2}{a} \right\rfloor = 1 + \left\lfloor \frac{N_2}{a} \right\rfloor. \tag{1.51}$$

Обговоримо значення цілого числа N_2 у рівнянні (1.51):

$$\text{якщо } N_2 > a, \text{ то } \left\lfloor \frac{r}{a} \right\rfloor = 1 + M_2, \text{ де } M_2 = \left\lfloor \frac{N_2}{a} \right\rfloor \Rightarrow \left\lfloor \frac{r}{a} \right\rfloor > 1; \tag{1.52}$$

$$\text{якщо } N_2 = a, \text{ то } \left\lfloor \frac{r}{a} \right\rfloor = 1+1 = 2; \tag{1.53}$$

$$\text{якщо } N_2 < a, \text{ то } \left\lfloor \frac{r}{a} \right\rfloor = 1+0 = 1 \Rightarrow \text{де } \left\lfloor \frac{r}{a} \right\rfloor = 1. \tag{1.54}$$

З (1.52), (1.53) та (1.54) отримаємо таку умову:

$$\left\lfloor \frac{r}{a} \right\rfloor \geq 1. \tag{1.55}$$

З початкової умови маємо:

$$r > a \geq 1 \Rightarrow \left\lfloor \frac{r}{a} \right\rfloor \leq r. \tag{1.56}$$

З (1.55) та (1.56) отримаємо таку умову:

$$1 \leq \left\lfloor \frac{r}{a} \right\rfloor \leq r. \tag{1.57}$$

З (1.48) та (1.57) отримаємо таку умову:

$$1 \leq a_2 \leq r. \tag{1.58}$$

З (1.47) та (1.58) отримаємо такі умови:

$$0 \leq a_1 \leq r \text{ і } 1 \leq a_2 \leq r. \tag{1.59}$$

Твердження 4 доведено при k=2.

Нехай твердження справедливе за k=n. Тоді послідовність матиме такий вигляд:

$$a_1, a_2, a_3, \ldots, a_{n-1}, a_n. \tag{1.60}$$

Нехай за припущенням індукції твердження 4 вірне при k=n. Це означає, що вірні такі умови:

$$0 \le a_i < r,\ i = 1, 2, \ldots, n\text{-}1; \tag{1.61}$$

$$1 \le a_n \le r. \tag{1.62}$$

Відповідно (1.2), при рівні розщеплення $k=n$ справедливо:

$$\Phi_n(a, r) = (\delta_a^{(2)}, \delta_a^{(3)}, \delta_a^{(4)}, \ldots, \delta_a^{(n-1)}, \delta_a^{(n)}, q_a^{(n)}). \tag{1.63}$$

Відповідно до (1.1) маємо рівняння:

$$a_n = q_a^n = \left\lfloor \frac{r}{q_a^{(n-1)}} \right\rfloor. \tag{1.64}$$

Тепер потрібно довести, що твердження 4 вірне при $k=n+1$. Тоді послідовність матиме такий вигляд:

$$a_1, a_2, a_3, \ldots, a_{n-1}, a_n, a_{n+1}. \tag{1.65}$$

Відповідно (1.2), при рівні розщеплення $k=n+1$ справедливо:

$$\Phi_{n+1}(a, r) = (\delta_a^{(2)}, \delta_a^{(3)}, \delta_a^{(4)}, \ldots, \delta_a^{(n-1)}, \delta_a^{(n)}, \delta_a^{(n+1)}, q_a^{(n+1)}). \tag{1.66}$$

З порівняння (1.63) і (1.66) помічаємо, що компоненти $\delta_a^{(2)}, \delta_a^{(3)}, \delta_a^{(4)}, \ldots, \delta_a^{(n-1)}, \delta_a^{(n)}$ збігаються в обох послідовностях. Тобто компоненти $a_1, a_2, a_3, \ldots, a_{n-1}$ теж збігаються в обох цих послідовностях.

За (2.61) виконуються такі умови:

$$0 \le a_i < r,\ i = 1, 2, \ldots, n\text{-}1. \tag{1.67}$$

Із твердження 1 та (1.1) маємо рівняння:

$$a_n=\delta_a^{(n+1)}=r \bmod q^{(n)} \Rightarrow 0\le a_n<|q^{(n)}|<r \Rightarrow 0\le a_n<r. \tag{1.68}$$

$$q^{(n)}=\left\lfloor \frac{r}{q^{(n-1)}} \right\rfloor. \tag{1.69}$$

Відповідно до (1.1) маємо рівняння:

$$q_{n+1}=\left\lfloor \frac{r}{q^{(n)}} \right\rfloor. \tag{1.70}$$

З (1.62), (1.64) та (1.69) видно, що:

$$\text{якщо } r\ge q^{(n)}\ge 1, \text{ то } r\ge q^{(n)}; \tag{1.71}$$

$$\text{якщо } r\ge q^{(n)}, \text{ то } r=q^{(n)}+N_n, \tag{1.72}$$

де $N_n\ge 0$ може бути будь-яким позитивним числом.

Шляхом ділення обох частин рівняння (1.72) на позитивне число $q^{(n)}>0$ маємо рівняння:

$$\frac{r}{q^{(n)}}=\frac{q^{(n)}+N_n}{q^{(n)}}. \tag{1.73}$$

Шляхом застосування операції округлення до найближчого цілого числа в рівнянні (1.73) отримуємо

$$\left\lfloor \frac{r}{q^{(n)}} \right\rfloor = \left\lfloor \frac{q^{(n)} + N_n}{q^{(n)}} \right\rfloor = 1 + \left\lfloor \frac{N_n}{q^{(n)}} \right\rfloor. \tag{1.74}$$

Обговоримо значення цілого числа N_n у рівнянні (1.74):

якщо $N_n > q^{(n)}$, то $\left\lfloor \frac{r}{q^{(n)}} \right\rfloor = 1 + M_n$, то $M_n = \left\lfloor \frac{N_n}{q^{(n)}} \right\rfloor \Rightarrow \left\lfloor \frac{r}{q^{(n)}} \right\rfloor > 1;$ (1.75)

якщо $N_n = q^{(n)}$, то $\left\lfloor \frac{r}{q^{(n)}} \right\rfloor = 1 + 1 = 2;$ (1.76)

якщо $N_n < q^{(n)}$, то $\left\lfloor \frac{r}{q^{(n)}} \right\rfloor = 1 + 0 = 1, \Rightarrow \left\lfloor \frac{r}{q^{(n)}} \right\rfloor = 1.$ (1.77)

З (1.75) , (1.76) та (1.77) отримаємо таку умову:

$$\left\lfloor \frac{r}{q^{(n)}} \right\rfloor \geq 1. \tag{1.78}$$

З (1.62), (1.64) та (1.69):

$$r \geq q^{(n)} \geq 1 \Rightarrow \left\lfloor \frac{r}{q^{(n)}} \right\rfloor \leq r. \tag{1.79}$$

З (1.78) та (1.79) отримаємо таку умову:

$$1 \leq \left\lfloor \frac{r}{q^{(n)}} \right\rfloor \leq r. \tag{1.80}$$

З (1.71), (1.72) та (1.80) отримаємо таку умову:

$$1 \le a_{n+1} < r. \qquad (1.81)$$

З (1.67), (1.68) та (1.81) отримуємо, що:

$$0 \le a_i < r,\ i = 1, 2, \ldots, n \quad \text{і} \quad 1 \le a_{n+1} \le r. \qquad (1.82)$$

Твердження 4 доведено при $k=n+1$. Таким чином, згідно з принципом математичної індукції, твердження 4 доведено для будь-якого натурального k.

Наслідок 1.2. Послідовність чисел $a_1, a_2, a_3, \ldots, a_{k-1}, a_k$, що виникають при цілісному розщепленні вихідного a, визначається єдиним чином.

Доведення випливає із тверджень 2 та 3. Твердження 2 говорить, що цілісне розщеплення є ін'єктивним, тобто два різних числа відображаються у вигляді двох нерівних упорядкованих послідовностей цілих чисел. Це означає, що кожне число розщеплюється єдиним чином. Упорядкованість тут розуміється як відображення очевидного порядку побудови компонентів розщеплення, аналогічно до того, як показана на рисунку 1.1. Доведення твердження 3 дає спосіб відновлення числа за його розщепленням.

Розглянемо наступні 2 приклади для цілісного розщеплення операції:

1) розщеплення символу $A=65$ за базою $r=302$. При $k=2$ отримуємо $\Phi_2(65, 302)=(42, 4)$. Функція відображення оборотна, дійсно $\frac{(302-42)}{4}=65$.

При $k=3$ отримуємо $\Phi_3(65,302)=(42, 2, 75)$. Функція відображення оборотна, дійсно $\frac{(302-42)}{\left(\frac{302-2}{75}\right)}=65$.

При $k=4$ отримуємо $\Phi_4(65,302)=(42, 2, 2, 4)$;

2) розщеплення символу $S=83$ за базою $r=205$.

При $k=2$ отримуємо $\Phi_2(83, 205)=(39, 2)$.

При $k=3$ отримуємо $\Phi_3(83, 205)=(39, 1, 102)$.

При $k=4$ отримуємо $\Phi_4(83, 205)=(39, 1, 1, 2)$.

2 АЛГОРИТМІЧНЕ ЗАБЕЗПЕЧЕННЯ ПРОЦЕДУРИ ЦІЛОЧИСЕЛЬНОГО РОЗЩЕПЛЕННЯ

2.1 Розщеплення по векторній базі

Усі теореми допускають природне узагальнення, зв'язане з динамікою, що виникає у застосунках. Зокрема, можна розглядати узагальнене розщеплення рівня *k* за векторною базою.

Розщеплення по векторній базі – це узагальнене розщеплення рівня *k* по векторній базі) $\vec{r} = (r_1, r_2, ..., r_l)$. В цьому випадку черговий (*i*-ий) крок процесу цілісного розщеплення виконується щоразу при новому значенні бази розщеплення.

Узагальненим цілим розщепленням числа *a* по векторній базі $\vec{r} = (r_1, r_2, ..., r_l)$, *l*=*k*-1, називається подання числа *a* у вигляді послідовності цілих чисел $a_1, a_2, a_3, \ldots, a_{k-1}, a_k$, у якій:

$$a_1=\delta^{(2)}, \text{ де } \delta^{(2)}=r_1 \bmod a,\ r_1>a,$$

$$a_2=\delta^{(3)}, \text{ де } \delta^{(3)}=r_2 \bmod q^{(2)},\ q^{(2)}=\left\lfloor \frac{r_1}{a} \right\rfloor,\ r_2>q^{(2)},$$

$$a_3=\delta^{(4)}, \text{ де } \delta^{(4)}=r_3 \bmod q^{(3)},\ q^{(3)}=\left\lfloor \frac{r_2}{q^{(2)}} \right\rfloor,\ r_3>q^{(3)}, \qquad (2.1)$$

……

$$a_{k-1}=\delta^{(k)}, \text{ де } \delta^{(k)}=r_{k-1} \bmod q^{(k-1)},\ q^{(k-1)}=\left\lfloor \frac{r_{k-2}}{q^{(k-2)}} \right\rfloor,\ r_{k-1}>q^{(k-1)},$$

$$a_k=q^{(k)},$$

де $q^{(k)}=\left\lfloor \frac{r_{k-1}}{q^{(k-1)}} \right\rfloor$.

Тут символи $\delta^{(i)}$ позначають залишки при цілочисельному діленні r_i на $q^{(i)}$.

Це визначення є узагальненням схеми математичного цілочисельного розщеплення.

Таке розщеплення виявляється найбільш корисним у застосунках, пов'язаних із захистом інформації, що передається.

Є багато способів, які можуть бути виконані для перевірки правильності вилучення відкритого тексту із зашифрованого з використанням процедури узагальненого розщеплення на стороні одержувача.

Один із цих способів, в яких обробляється символ за символом, можна пояснити так:

1) якщо значення перевіряє умову $r_i > q^{(i)}$, де i=2, 3, …, k-1, тобто використовують його у процесі шифрування;

2) якщо значення r_i не перевіряє умову $r_i > q^{(i)}$, де i=2, 3, …, k-1, то в процесі шифрування виконуються такі кроки:

- пропустити поточне значення r_i і використовувати наступне значення r_{i+1} у згенерованій послідовності гам;

- додати 0 ліворуч від результату залишку, який буде розрахований з використанням гами r_{i+1} (функція цього 0 не змінить значення залишку, але в процесі отримання відкритого тексту повідомить одержувача зашифрованого тексту про те, що в послідовності гам є невикористане пропущене значення r_i.

Передбачається, що зв'язок безшумний, тобто у каналі зв'язку відсутні перешкоди. Однак наявність перешкод можна грубо оцінити теоретично при передачі замість символу його розщеплення. У цій роботі буде всюди передбачатися, що канал зв'язку є безшумним, як і у випадку передачі даних між двома комп'ютерами виділеної лінії.

2.2 Алгоритми процедури цілочисельного розщеплення

Проста процедура цілісного розщеплення може бути описана, як показано в псевдокоді Алгоритму 2.1 та відповідній блок-схемі на рисунку 2.1.

Алгоритм 2.1.

Вихідні параметри: ціле число a, ціле число r рівень розщеплення k.

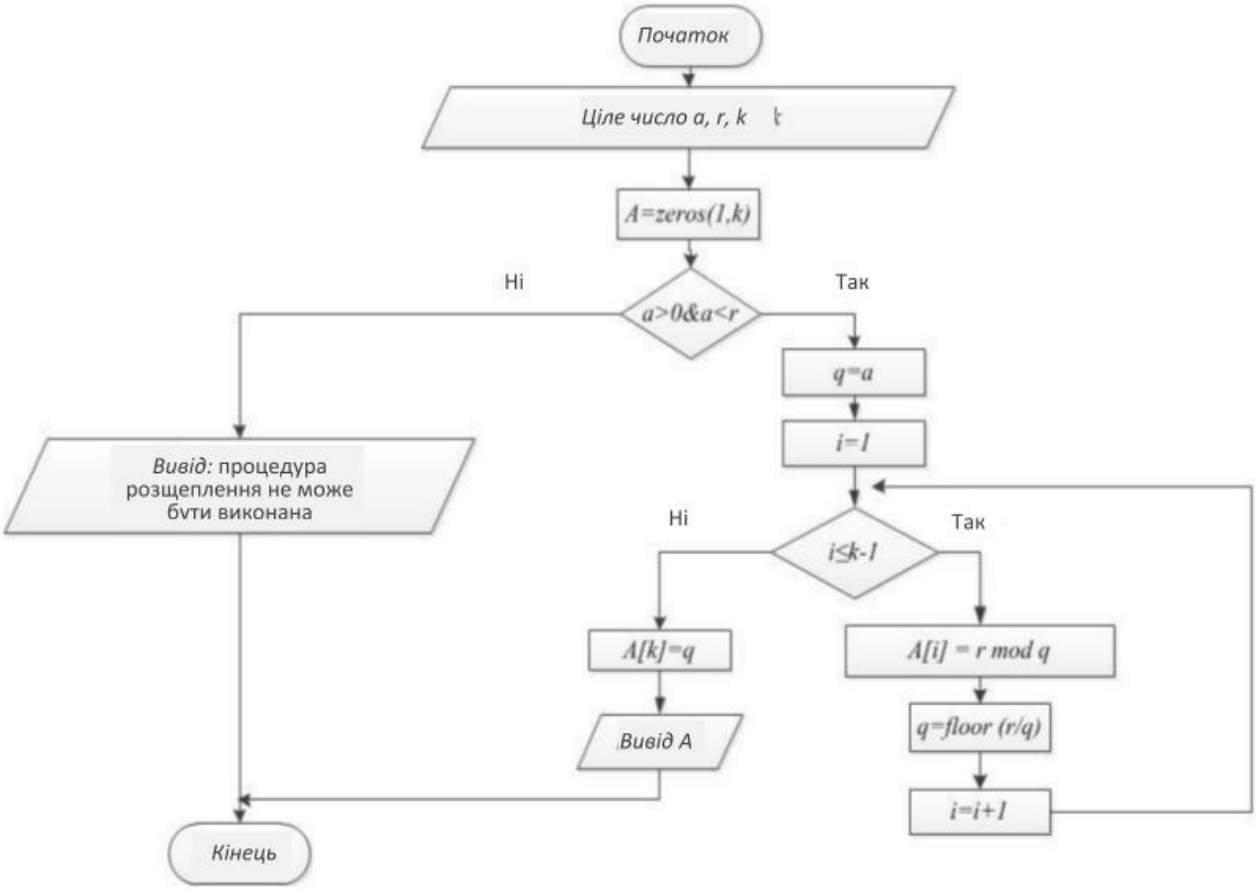

Рисунок 2.1 − Блок-схема алгоритму цілісного розщеплення числа *a* по базі *r* при рівні розщеплення *k*

Результат: вектор *A* з *k* елементів, що містить послідовність цілих чисел $a_1, a_2, a_3, \ldots, a_{k-1}, a_k$.

Якщо *a*>0 & *a*<, тоді

/* допоміжний вектор */

A=zeros (1, *k*);

/* допоміжний параметр */

q=*a*;

цикл *i*=1 до *k*-1 виконувати

A[*i*] *r* mod *q*;

q=floor (*r*/*q*);

кінець циклу

A[*k*]=*q*;

повернути *A*;

інакше

повернути висновок: процедура розщеплення не може бути застосована, тому що не виконується умова

кінець якщо

кінець

Алгоритм узагальненої процедури цілочисельного розщеплення може бути описаний, як показано в псевдокоді Алгоритму 2.2 та відповідній блок-схемі для цього алгоритму на рисунку 2.2.

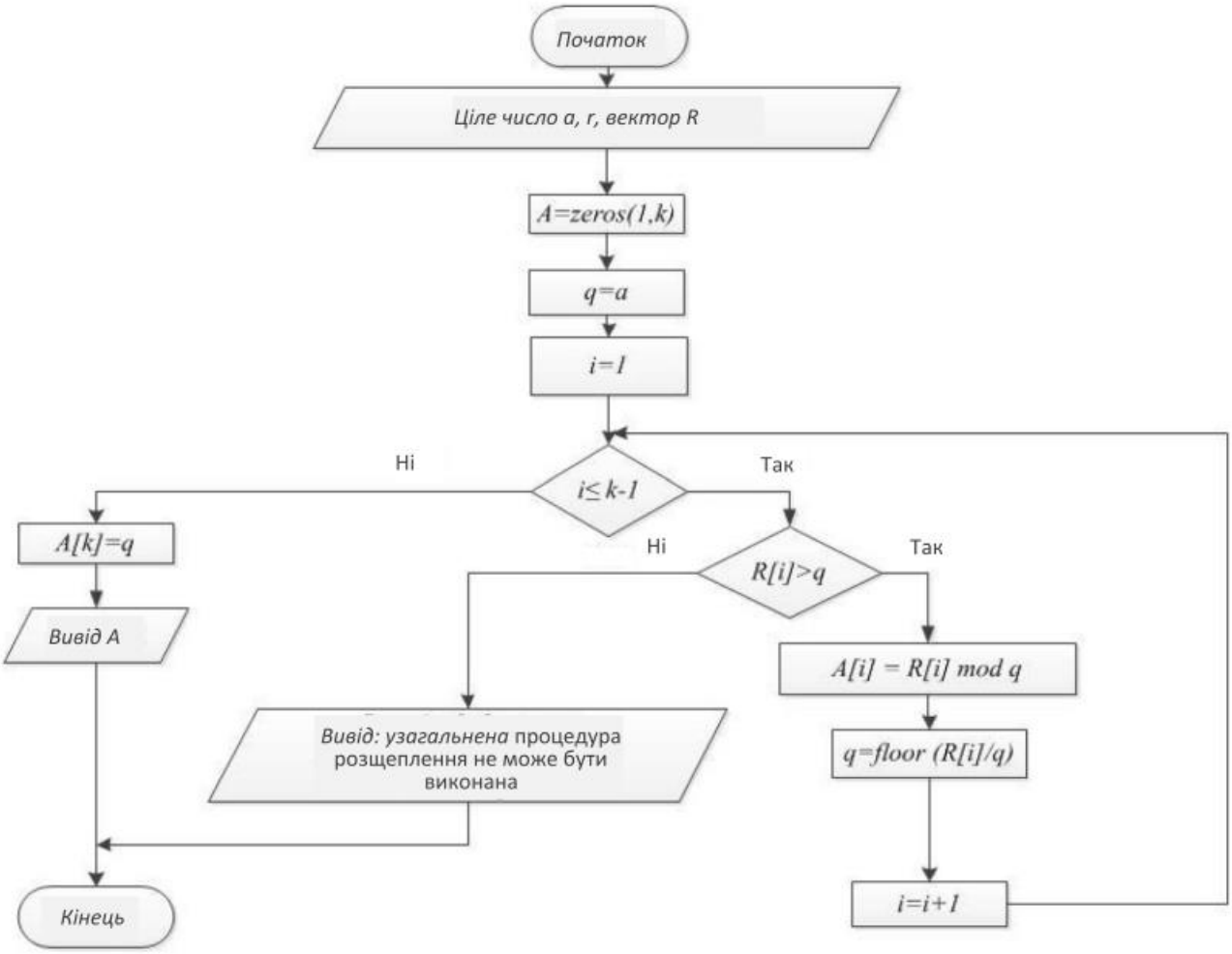

Рисунок 2.2 − Блок-схема алгоритму при використанні узагальненої процедури розщеплення

Алгоритм 2.2.

Вихідні параметри: ціле число a, вектор R з k-1 елементів, що містить послідовність цілих чисел r_1, r_2, r_3, …, r_{k-2}, r_{k-1}. Рівень розщеплення k.

Результат: вектор A з k елементів, що містить послідовність цілих чисел a_1, a_2, a_3, …, a_{k-1}, a_k.

/* допоміжний вектор */

A=zeros (1, k);

/* допоміжний параметр */

q=a;

цикл i=1 до k-1 виконувати

якщо $R[i]>q$ тоді

$A[i]=R[i] \bmod q$;

q=floor($R[i]/q$);

інакше

повернути узагальнена процедура розщеплення не може бути застосована, тому що не виконується умова

кінець

кінець якщо

кінець циклу

$A[k]=q$;

повернути A;

кінець

2.3 Алгоритми відновлення числа при цілочисельному розщепленні

Нижче наведено псевдокод алгоритму відновлення цілого числа a по базі r при рівні розщеплення k (Алгоритм 2.3). Блок-схема цього алгоритму показана на рисунку 2.3.

Алгоритм 2.3.

Вихідні параметри: вектор A з k елементів, що містить послідовність цілих чисел a_1, a_2, a_3, …, a_{k-1}, a_k, початкові умови та ціле число r.

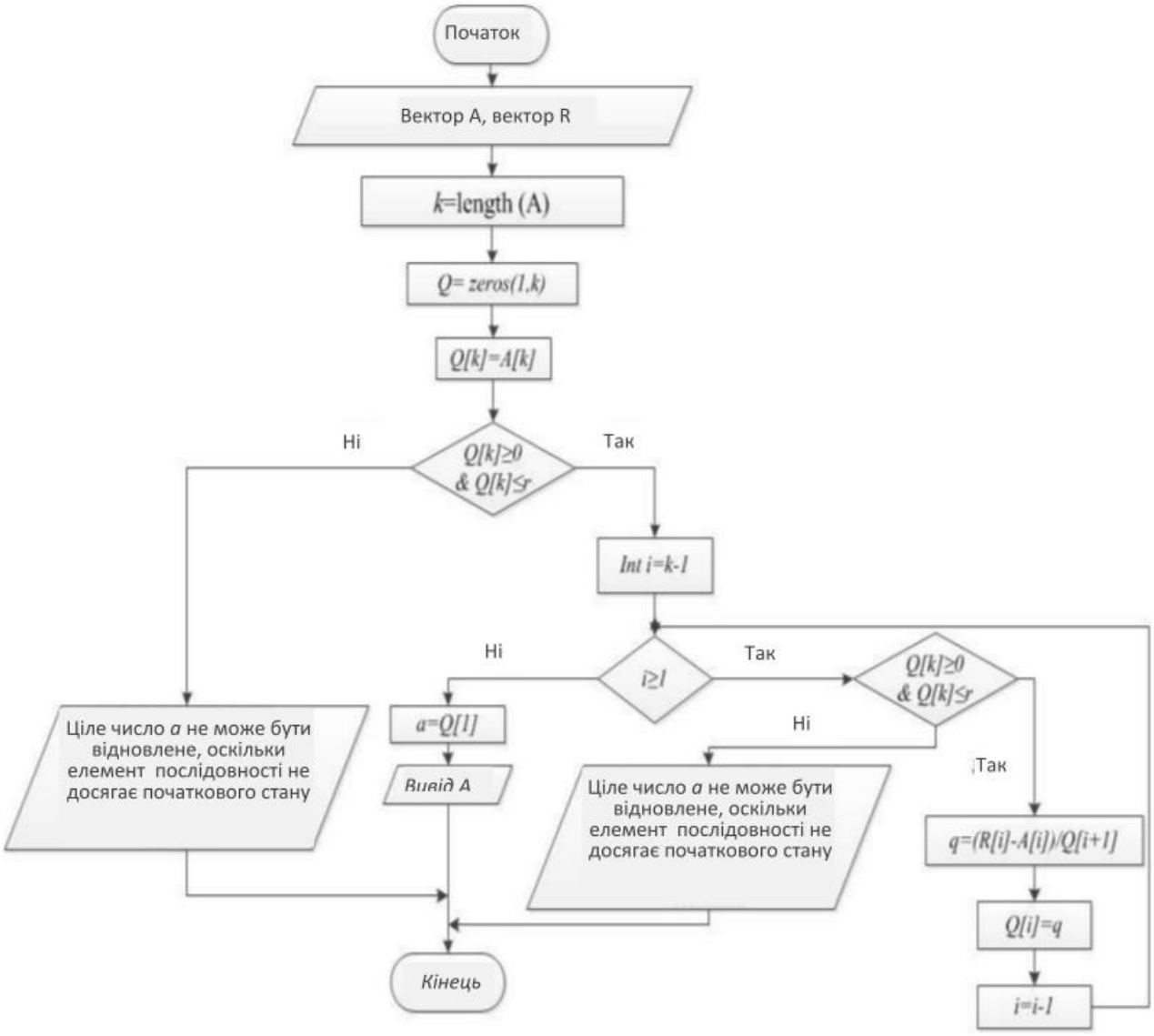

Рисунок 2.3 – Блок-схема алгоритму відновлення вихідного цілого числа

Результат: ціле число *a*.

/* рівень розщеплення */

k=length (*A*);

/* допоміжний вектор */

Q=zeros (1, *k*);

Q[k]=*A*[*k*];

якщо *Q*[*k*]≥1& *Q*[*k*]≤*r*, тоді

цикл *i*=*k*-1 до 1 виконувати

якщо *A*[*i*]≥0 & *A*[*i*]<*r* тоді

q(*r*-*A*[*i*])/*Q*[*i*+1];

$Q[i]=q$;

інакше

повернути ціле число a не може бути відновлено з послідовності, оскільки елемент послідовності не досягає початкового стану

кінець

кінець якщо

кінець циклу

$a=Q[1]$;

повернути a;

інакше

повернути ціле число a не може бути відновлено з послідовності, оскільки елемент послідовності не досягає початкового стану

кінець якщо

кінець

Нижче наведено псевдокод алгоритму відновлення цілого числа a по базі r при використанні узагальненої процедури розщеплення (Алгоритм 2.4). Блок-схема цього алгоритму показана на рисунку 2.4.

Алгоритм 2.4.

Вихідні параметри: вектор A з елементів k, що містить послідовність цілих чисел a_1, a_2, a_3, …, a_{k-1}, a_k. Вектор R з k-1 елементів, що містить послідовність цілих чисел r_1, r_2, r_3, …, r_{k-2}, r_{k-1}.

Результат: ціле число a.

/* рівень розщеплення */

k=length (A);

/* допоміжний вектор */

Q=zeros (1, k);

$Q[k]=A[k]$;

цикл $i=k$-1 до 1 виконувати

$q=(R[i]-A[i])/Q[i+1]$;

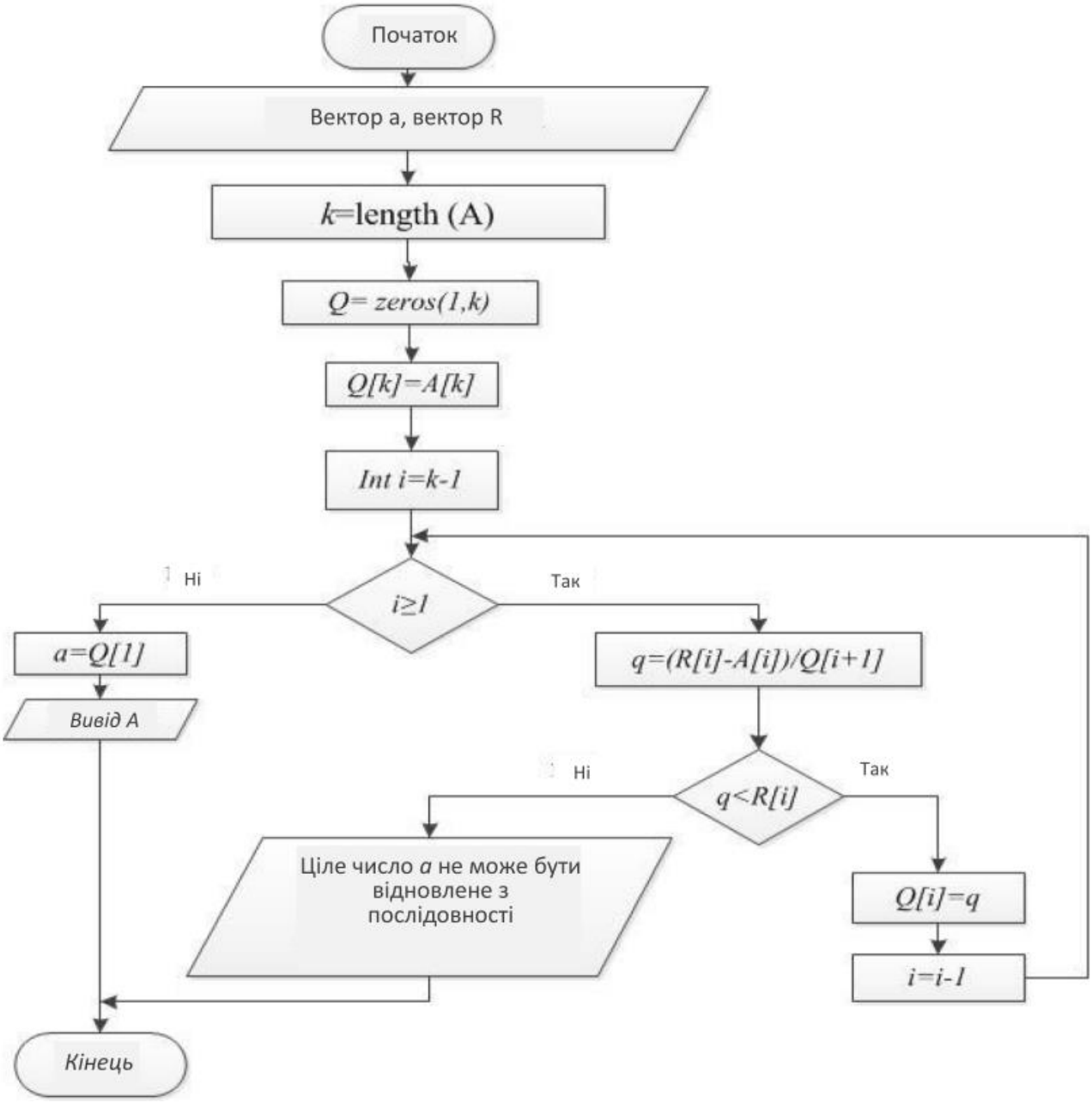

Рисунок 2.4 − Блок-схема алгоритму відновлення вихідного цілого числа при використанні узагальненої процедури розщеплення

якщо $q<R[i]$ тоді

$Q[i]=q$;

інакше

повернути ціле число a не може бути відновлено із послідовності

кінець

кінець якщо

$Q[i]=q$;

кінець циклу

$a=Q[1]$;

Повернути a;

кінець

2.4 Зв'язок між еволюцією та процедурою розщеплення

На рисунку 1.1 рівень розщеплення відповідає рівню еволюційного розвитку. При цьому кожен рівень є новим поколінням.

Початкове покоління: a – значення символу у вибраній кодовій таблиці символів, r – псевдовипадкове число, що перевищує максимальне значення вибраної кодової таблиці символів.

Еволюція в процедурі розщеплення проявляється, починаючи з другого покоління.

Нове покоління у вигляді пари чисел $\delta^{(i)}$, $q^{(i)}$ є результатом цілісного розщеплення для особини $q^{(i-1)}$ з використанням псевдовипадкового числа r, загального для всіх поколінь a.

В узагальненому цілочисельному розщепленні псевдовипадкове число у кожному поколінні генерується заново, що зближує процес з мутацією в біологічних системах.

Відбір особини у нове покоління здійснюється відповідно до особини попереднього покоління як результат неповної частки ділення із залишком $q^{(i-1)}$. Вибір неповної частки ділення гарантує безперервність процесу еволюції.

Процес народження виконується з використанням математичної операції ділення із залишком $\delta^{(i)}=r \bmod q^{(i-1)}$, $q^{(i)}=\left\lfloor \frac{r}{q^{(i-1)}} \right\rfloor$, $i=2, 3, \ldots, k$, тоді як попередня особина $q^{(i-1)}$ гине.

Критерій зупинки процесу еволюції при розщепленні: досягнення певної кількості поколінь k.

Еволюцією числа a на основі процедури цілочисельного розщеплення називається розщеплення a на k поколінь з використанням арифметичної операції ділення із залишком. Натуральне число k тут визначає загальну кількість поколінь.

Перевага використання процедури розщеплення у сфері захисту інформації у порівнянні з традиційними методами еволюції на основі генетичного алгоритму можна сформулювати в такий спосіб.

У процедурі розщеплення немає необхідності використовувати деякі традиційні операції еволюції, які властиві генетичній еволюції, такі, як визначення значення цільової функції для всіх особин, визначення точок кросовера, застосування кросовера, визначення точок мутації, застосування мутації тощо.

Замість цих традиційних еволюційних операцій процедура розщеплення створює покоління шляхом повторного використання математичної операції ділення із залишком для кожного покоління. Це спосіб зменшення часу виконання, тобто процедура розщеплення працює швидше, ніж традиційні методи еволюції на основі генетичного алгоритму.

2.5 Порівняння деяких синхро-струмових методів захисту з методом розщеплення

Метод цілочисельного розщеплення знімає серйозну проблему, що виникає при реалізації методу Вернама, і пов'язана з необхідністю доставки одержувачу такої ж послідовності ключів, як і у відправника, або з необхідністю безпечного зберігання ідентичних послідовностей ключів у відправника та одержувача.

Ця проблема вирішена при захисті інформації методом цілочисельного розщеплення за допомогою ключа захисту, який генерує ті ж гами у відправника та одержувача. Тому замість передачі або зберігання великих гам, що необхідно у методі Вернама, у запропонованому методі достатньо передати

(або зберегти) невеликий обсяг інформації, який називається нами ключем захисту.

Метод цілочисельного розщеплення також знімає досить серйозну проблему, що виникає при реалізації методу гамування, яка пов'язана з необхідністю генерування гам, у яких період має бути достатньо великим. Справа в тому, що цілочисельне розщеплення за допомогою ДГА та ГПВЧ буде створювати гами, які є дійсно більш випадковими за кількома відомими критеріями.

Відмінності методу цілочисельного розщеплення від відомих методів захисту гамування та методу Вернама представлені в таблиці 2.1.

Таблиця 2.1 - Порівняння деяких синхро-потокових (синхронізаційних) методів захисту із розщепленням

	Метод Вернама	Метод гамування	Метод цілочисельного розщеплення
Період гами	Відсутня одноразова гама	Є	Істотно збільшений
Необхідність збереження гами	Так	Ні	Ні
Необхідність доставки отримувачу такої ж гами, як у відправника	Так	Ні	Ні
Абсолютна стійкість	Так	Ні	Асимптотична стійкість

Метод розщеплення вирішує проблему ненадійності, яка існує в потокових методах захисту даних через повторне використання гами.

2.6 Порівняння відомих абсолютно стійких методів захисту з методом розщеплення

Є дві переваги методу цілочисельного розщеплення порівняно з традиційними, абсолютно стійкими методами захисту інформації.

Перше: метод цілочисельного розщеплення є практичним і не дуже дорогим за необхідними ресурсами в порівнянні з іншими способами забезпечення стійкості шифрів, оскільки не потрібне виконання умови про використання кожної гами лише один раз.

Друге: метод цілочисельного розщеплення приховує для порушника інформацію про довжину вихідного повідомлення, що визначається наступним чином: $c=k\times l$, де c – довжина захищеного тексту, k – рівень розщеплення, l – довжина вихідного тексту, тоді як k – невідоме.

Відмінності даного методу цілочисельного розщеплення від відомих, абсолютно стійких алгоритмів захисту представлені в таблиці 2.2.

Таблиця 2.2 - Порівняння традиційних, абсолютно стійких методів захисту з розщепленням

Властивості	Відомі, абсолютно стійкі, алгоритми захисту	Захист методом цілочисельного розщеплення
Використання кожної гами тільки один раз	Так	Ні
Інформація довжини вихідного тексту повідомлення	Показана інформація про довжину вихідного тексту повідомлення	Інформація про довжину вихідного тексту повідомлення прихована
Необхідність зберігання гами	Так	Ні

2.7 Порівняння методу цілочисельного розщеплення з методами заміни, заснованими на операції модульної арифметики

Відзначаються дві відмінності методу цілочисельного розщеплення від відомих алгоритмів захисту, що застосовують операції модульної математики.

Перше - операція із застосуванням модуля використовується в традиційних методах лише один раз для кожного символу. У запропонованому методі цілочисельного розщеплення ця операція використовується k-1 раз.

Друге – величини модулів, що використовуються у всіх інших способах захисту інформації (Цезаря, Віженера, афінному, Хілла тощо), заснованих на операціях модульної арифметики, збігаються з розміром відповідного алфавіту, тоді як в алгоритмі цілочисельного розщеплення, величина модуля не пов'язана із загальним розміром алфавіту. Перелічені особливості, зокрема, ускладнюють семантичне відновлення вихідного тексту несанкціонованим користувачем, тобто відновлення тексту за його змістом.

При застосуваннях розщеплення та китайської теореми про залишки передбачено можливість відновлення цілого числа за множиною його залишків від ділення. Однак у китайській теоремі про залишки це досягається завдяки умові, що множина використовуваних чисел є сукупністю попарно взаємно простих чисел. Ця вимога не виникає в запропонованому методі розщеплення.

Щодо китайської теореми про залишки слід зазначити, що вона використовується в алгоритмах шифрування та в завданнях розділення секрету (sharing secret), що ґрунтуються на використанні односторонніх функцій. Для розкриття інформації в таких системах потрібне вирішення класичних проблем факторизації та пошуку взаємно простих чисел, на яких базується КТЗ.

У методі розщеплення не використовуються взаємно прості числа, а на етапі спроб відкриття факторизація не може бути використана у зв'язку з особливостями запропонованого методу.

2.8 Покращення рівня випадковості деяких генераторів псевдовипадкових чисел на основі генетичного алгоритму

Запропонований генетичний алгоритм використовує та застосовує наступні оператори:

1) “Хромосома” у запропонованому методі є бінарною, тобто її компоненти – 0 та 1;

2) довжина хромосоми повинна бути задана в ключі захисту;

3) розмір популяції хромосом також має бути визначений у ключі захисту;

4) генетичні перетворення, використовуючи наступні операції кросовера та мутації:

- тип кросовера – одноточний;

- мутація досягається інвертуванням детерміновано вибраних деяких «генів», 0 замінюється на 1 або навпаки.

Заданими вважаються наступні параметри: тип генератора, початкове значення генератора, розмір генерації L, довжина хромосоми M, кількість поколінь N генерації, потім виконуються такі дії:

1) генерується послідовність випадкових чисел довжини L на основі обраного ГПВЧ при обраному початковому значенні;

2) значення кожного числа в отриманій послідовності з L випадкових чисел конвертуються в двійкове подання. Після такого перетворення утворюватимуться вектори з різною довжиною, тому у кожному цьому векторі або потрібно додати біти від 0 до довжини хромосоми M і, відповідно, видалити додаткові біти, що перевищують довжину хромосоми M. В результаті отримується послідовність векторів з однаковою довжиною M, яка становить множину хромосом;

3) відбираються перші дві хромосоми;

4) визначається тип кросовера;

5) застосовується оператор кросовера на вибраних двох хромосомах;

6) визначити, чи потрібно використовувати генетичний оператор мутації. Якщо оператор мутації потрібен, то перейти до кроку 7 і виконати мутацію, інакше перейти до кроку 8;

7) конвертуються значення деяких визначених генів від 0 до 1;

8) послідовно відбираються наступні дві хромосоми;

9) повторити кроки від 4 до 8 до кінця розміру генерації L;

10) в результаті сформується покоління хромосом №1;

11) змінюється початкове значення генератора за визначеним правилом;

12) за допомогою ГПВЧ генерується нова послідовність випадкових чисел на основі нового отриманого початкового значення генератора довжини L;

13) кроки від 3 до 9 циклічно повторюються, щоб отримати нове покоління хромосом;

14) кроки від 11 до 13 повторюються до досягнення максимальної кількості поколінь N, тобто до виконання умов зупинки.

У запропонованому способі використовуються такі п'ять типів кросоварів:

1) кросовер "діагональ по діагоналі" використовує діагонально першу частину першої хромосоми та другу частину другої хромосоми. Друга частина першої хромосоми замінюється першою частиною другої хромосоми, як показано рисунку 2.5.

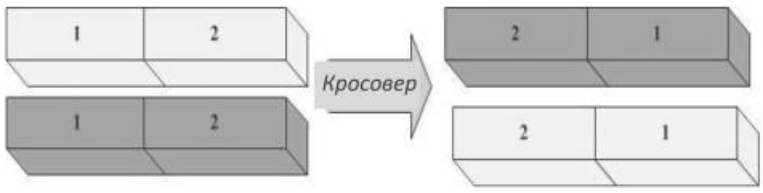

Рисунок 2.5 - Кросовер "діагональ по діагоналі"

2) кросовер "вертикально праворуч" діє вертикально: друга частина першої хромосоми обмінюється з другою частиною другої хромосоми, як показано рисунку 2.6.

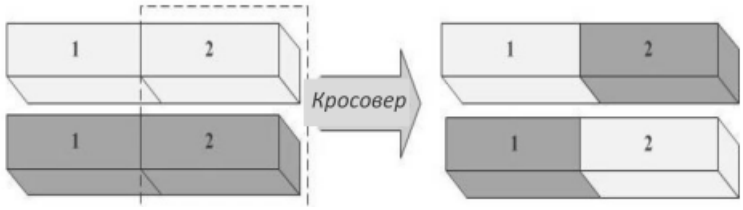

Рисунок 2.6 – Кросовер “вертикально праворуч”

3) кросовер "вертикально ліворуч": перша частина першої хромосоми обмінюється з першою частиною другої хромосоми, як показано рисунку 2.7.

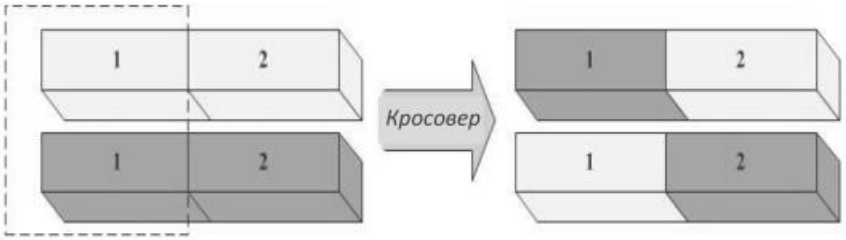

Рисунок 2.7 – Кросовер “вертикально ліворуч”.

4) кросовер "діагонально праворуч": друга частина першої хромосоми обмінюється з першою частиною другої хромосоми, як показано рисунку 2.8.

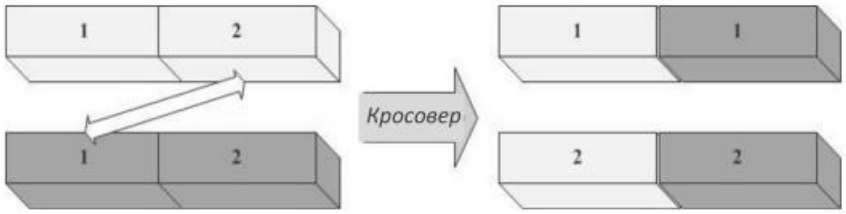

Рисунок 2.8 – Кросовер “діагонально праворуч”.

5) кросовер "діагонально ліворуч": перша частина першої хромосоми обмінюється з другою частиною другої хромосоми, як показано рисунку 2.9.

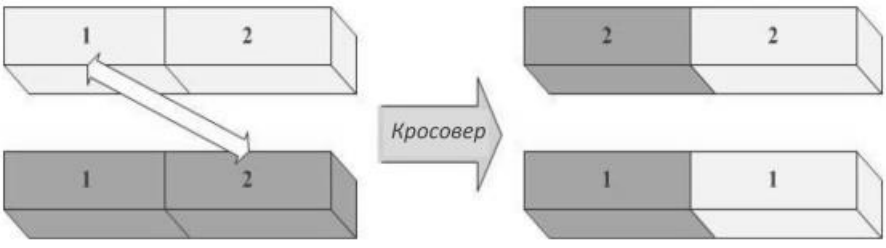

Рисунок 2.9 – Кросовер “діагонально ліворуч”

Алгоритм розроблений, щоб він не був передбачуваним (що містить період), але може бути відтворений. Тому запропонований детермінований генетичний алгоритм розроблено так, щоб використовувати всі типи кросовера у довільній послідовності для відсутності періоду. Це досягається за допомогою наступного рівняння:

тип кросовера = (порядок хромосоми 1 + порядок хромосоми 2 + порядок покоління);

- якщо тип кросовера =1, то застосувати кросовер "діагональ по діагоналі";

- якщо тип кросовера =2, то застосувати кросовер "діагонально ліворуч";

- якщо тип кросовера =3, то застосувати кросовер "діагонально праворуч";

- якщо тип кросовера =4, то застосувати: кросовер “вертикально ліворуч”;

- якщо тип кросовера =0, то застосувати кросовер "вертикально праворуч".

Генетичний алгоритм з перерахованими властивостями називається детермінованим генетичним алгоритмом (ДГА).

3 РЕАЛІЗАЦІЯ ТА ІМОВІРНІСНИЙ АНАЛІЗ СТІЙКОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ МЕТОДОМ ЦІЛОЧИСЕЛЬНОГО РОЗЩЕПЛЕННЯ

3.1 Імовірнісний аналіз стійкості захисту інформації методом цілочисельного розщеплення

Прийнятий тут підхід будується значною мірою по аналогії з відповідними роботами К. Шеннона, що належать до принципів дії «секретних систем зв'язку».

Перш, ніж нагадати основний результат К. Шеннона, що відноситься до захисту інформації методом Вернама, слід зазначити, що ймовірнісний аналіз досі міцно увійшов у практику дослідників, які працюють у різних галузях. Як приклад можна вказати недавню публікацію [6], в якій вивчається час відгуку системи, що спирається на хмарні обчислення.

У роботі [47] наводяться основні теореми та алгоритми розрахунку імовірнісних характеристик для цілого ряду моделей так званих мультисервісних мереж. Іншим прикладом може бути публікація [167]. У ній особливо підкреслюється потреба розглядати стохастичні явища як зовнішні по відношенню до системи, але як притаманні самій системі. У роботі вивчаються відомі процеси «народження-загибелі». Особливо важливим є те, що запропонований у статті [167] метод дозволяє організувати «правильне поєднання детермінованих та стохастичних явищ» в системі. Стаття [192] присвячена дослідженню асимптотики ймовірностей шляхів у деякому марківському процесі на тривимірному графі Юнга. Відразу потрібно підкреслити, що подібне поєднання детермінованих та ймовірнісних явищ у єдиній системі є також однією з найбільш характерних рис системи, що вивчається розщепленням, запропонованим нами раніше.

Позначимо через C захищений текст, отриманий в результаті застосування методу розщеплення кожного символу вихідного тексту M.

Доцільно зауважити, що C через роботу ГПВЧ представляється хакеру як набір випадкових чисел із невідомими йому імовірнісними властивостями.

Тому останній спробує відновити M по цих числах, застосовуючи процедуру повного перебору чи пошуку.

Позначимо через $\Pr(M|C, k)$ ймовірність успішного відновлення вихідного тексту M, спираючись на доступний хакеру захищений текст C і невідомий йому рівень розщеплення k.

Порушнику відомі математичні моделі розщеплення та відновлення символу, але невідомий ключ, який використовується під час передачі. Теорема про асимптотичну стійкість доведена за цієї умови.

Крім того, порушник має доступ до інформації, що передається каналом зв'язку. Йому невідомо, чи використовується просте розщеплення, чи узагальнене.

У таблиці 3.1 наведено числові значення для ймовірності несанкціонованого відновлення вихідного тексту за різних значень k. Також на рисунку 3.1 показано графік поведінки ймовірності для тих самих рівнів розщеплення.

Таблиця 3.1 - Ймовірність несанкціонованого відновлення вихідного тексту за різних значень рівнів розщеплення

Рівень розщеплення k	Ймовірність несанкціонованого відновлення $\Pr(M\|C, k)$, $\times 10^{-8}$
2	8,77914
3	8,74030
4	8,73773
5	8,73755
6	8,73738
7	8,73737
8	8,73736

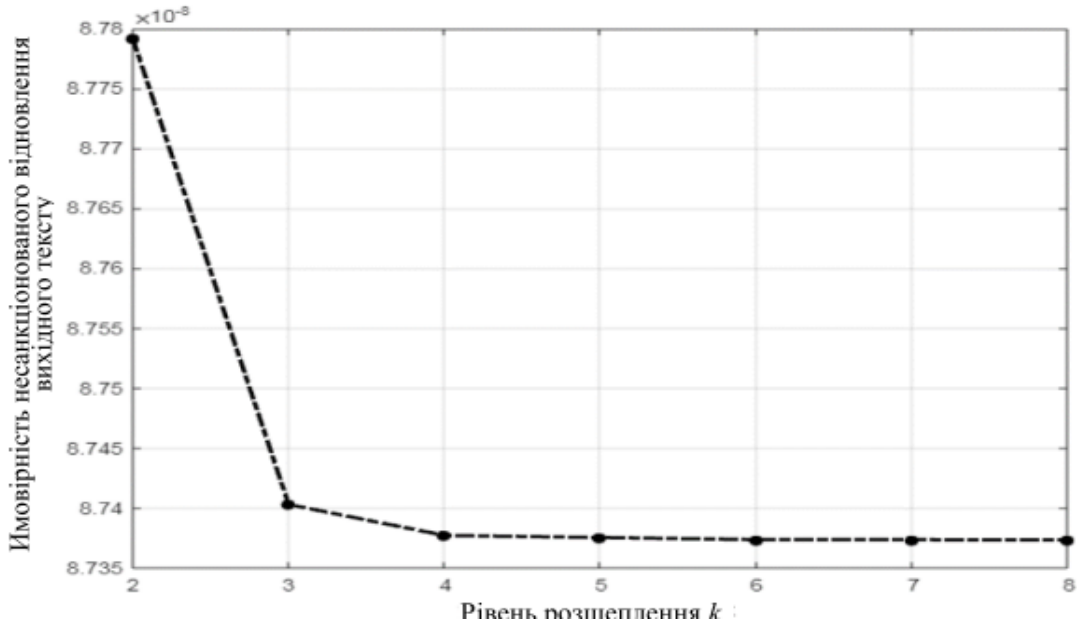

Рисунок 3.1 − Поведінка ймовірності несанкціонованого відновлення вихідного тексту за різних значень рівнів розщеплення *k*

Ймовірність несанкціонованого відновлення вихідного тексту *M* за результатом розщеплення *C* експоненційно зменшується зі зростанням розміру захищеного тексту *N*. У таблиці 3.2 наведено числові значення для ймовірності несанкціонованого відновлення вихідного тексту за різних значень розміру захищеного тексту *N*, а на рисунку 3.2 - їх графічна залежність.

Таблиця 3.2 - Ймовірність несанкціонованого відновлення вихідного тексту при різних значеннях розміру захищеного тексту

Розмір тексту *N*, який захищається	Ймовірність несанкціонованого відновлення Pr(*M*|*C*, 4)
5	0,00392
10	$1{,}31066\times10^{-6}$
15	$5{,}82676\times10^{-9}$
20	$1{,}73412\times10^{-12}$
25	$7{,}70719\times10^{-15}$
30	$2{,}28366\times10^{-18}$
35	$1{,}01496\times10^{-20}$

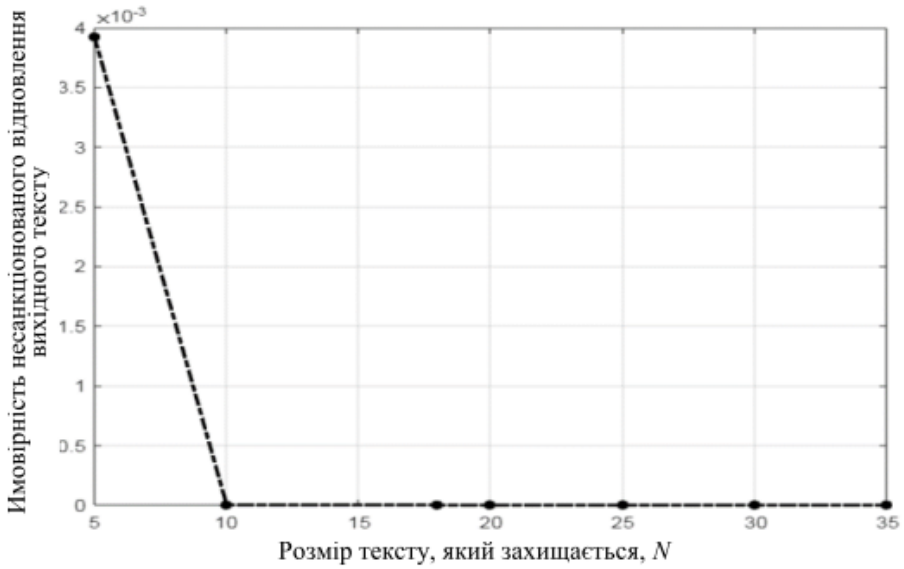

Рисунок 3.2 − Поведінка ймовірності несанкціонованого відновлення вихідного тексту при різних значеннях розміру тексту *N*, що захищається

Ймовірність несанкціонованого відновлення вихідного тексту *M* за результатом розщеплення *C* експоненційно зменшується зі зростанням числа всіх перебірних подій (виходів) *L* в просторі створеної ним гами з випадкових чисел. Приклад: якщо вибираються значення параметрів *k*=4 і *N*=35, то отримується таблиця 3.3.

Таблиця 3.3 - Ймовірність несанкціонованого відновлення вихідного тексту за різних значень розміру простору гами *L*

Розмір простору гами *L*	Ймовірність несанкціонованого відновлення Pr(*M*|*C*, 4)
10	$9{,}9999\times10^{-18}$
15	$1{,}01496\times10^{-20}$
20	$7{,}62939\times10^{-23}$
25	$1{,}71799\times10^{-24}$
30	$7{,}74352\times10^{-26}$
35	$5{,}63434\times10^{-27}$
40	$5{,}82077\times10^{-28}$

У таблиці 3.3 наведено числові значення для ймовірності несанкціонованого відновлення вихідного тексту при k=4, N=35 та різних значеннях розміру простору для гами L. На рисунку 3.3 показана графічна залежність ймовірнсті несанкціонованого відновлення вихідного тексту для тих же різних значень розміру простору гами L.

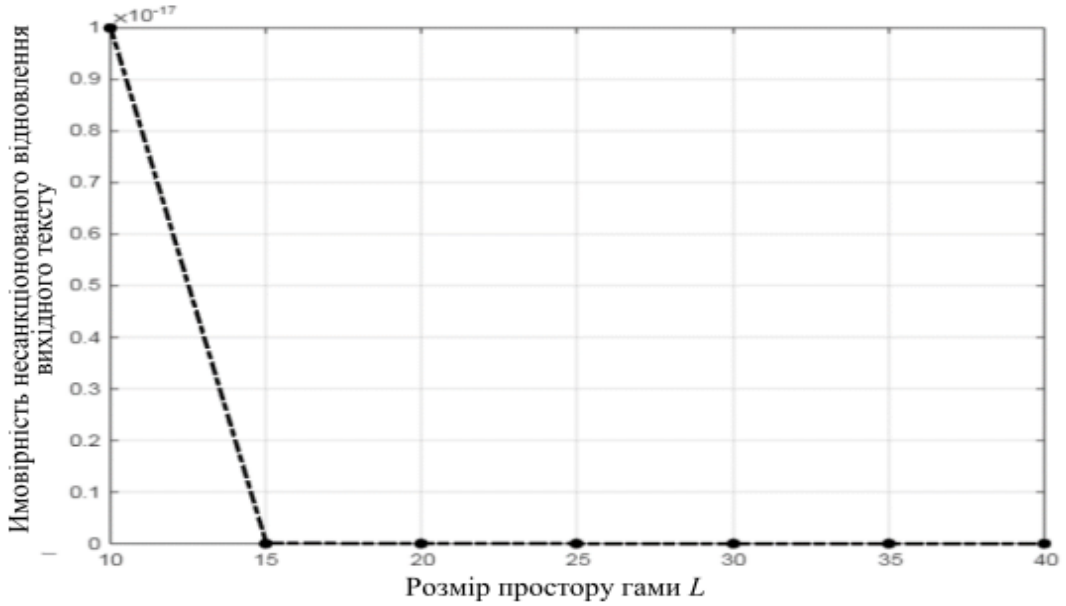

Рисунок 3.3 − Поведінка ймовірності несанкціонованого відновлення вихідного тексту за різних значень розміру простору гами L

У таблиці 3.4 наведено числові значення для ймовірності несанкціонованого відновлення вихідного тексту при різних значеннях k. На рисунку 3.4 показаний графік ймовірності для таких же самих рівнів розщеплення.

У таблиці 3.5 наведено числові значення для ймовірності несанкціонованого відновлення вихідного тексту для різних значень розміру захищеного тексту N. На рисунку 3.5 показаний графік ймовірності несанкціонованого відновлення вихідного тексту для тих же значень розмірів тексту, що захищається.

Таблиця 3.4 - Ймовірність несанкціонованого відновлення вихідного тексту за різних значень рівнів розщеплення

Рівень розщеплення k	Ймовірність несанкціонованого відновлення $\Pr(A\|C, k)$
2	$8{,}77915\times10^{-8}$
3	$3{,}88358\times10^{-10}$
4	$2{,}43798\times10^{-11}$
5	$2{,}29460\times10^{-11}$
6	$1{,}61230\times10^{-12}$
7	$1{,}61227\times10^{-12}$
8	$1{,}61183\times10^{-12}$

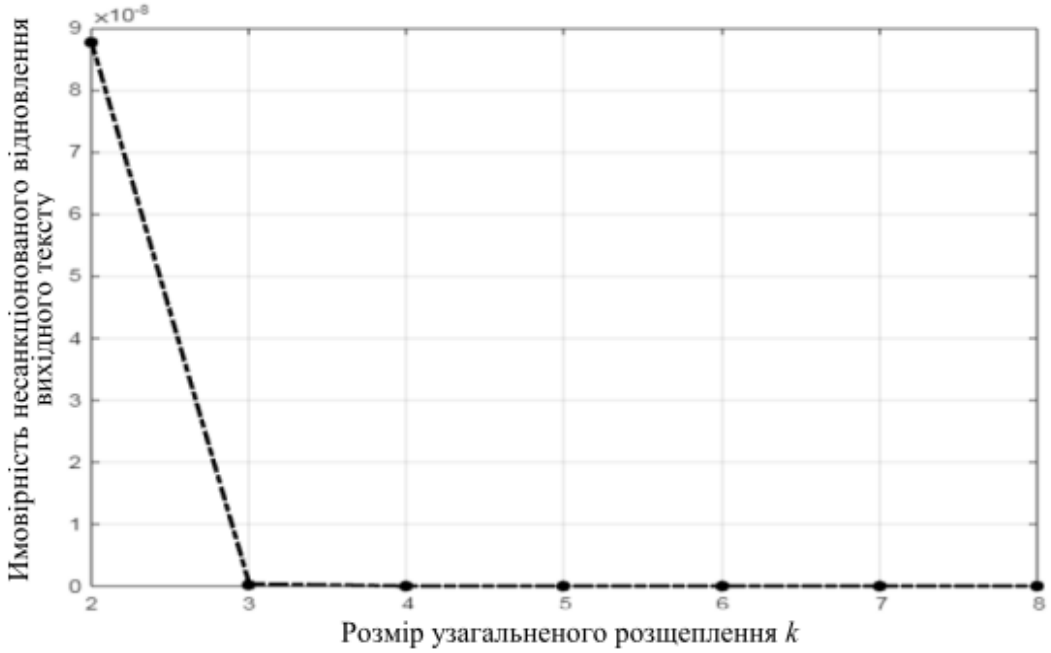

Рисунок 3.4 − Поведінка ймовірності несанкціонованого відновлення вихідного тексту за різних значень рівнів узагальненого розщеплення k

Таблиця 3.5 - Ймовірність несанкціонованого відновлення вихідного тексту при різних значеннях розміру захищеного тексту

Розмір тексту N, який захищається	Ймовірність несанкціонованого відновлення $\Pr(A\|C, 4)$
5	$2{,}61144\times10^{-4}$
10	$4{,}24798\times10^{-8}$
15	$1{,}62532\times10^{-12}$
20	$2{,}28298\times10^{-18}$
25	$6{,}73645\times10^{-22}$
30	$1{,}87955\times10^{-25}$
35	$5{,}91403\times10^{-29}$

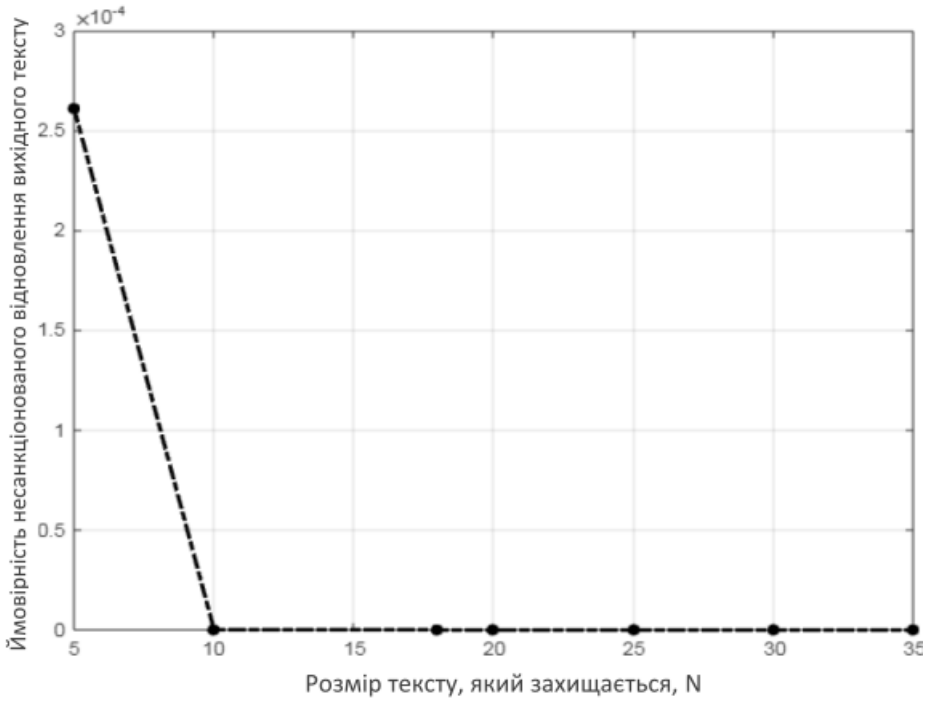

Рисунок 3.5 − Поведінка ймовірності несанкціонованого відновлення вихідного тексту при різних значеннях розміру тексту, що захищається

У таблиці 3.6 наведено числові значення для ймовірності несанкціонованого відновлення вихідного тексту за різних значень розміру

простору гами L. А на рисунку 3.6 показаний графік поведінки ймовірності несанкціонованого відновлення вихідного тексту за тих же різних значень розміру простору гами L.

Таблиця 3.6 - Ймовірність несанкціонованого відновлення вихідного тексту за різних значень розміру простору гами L

Розмір простору гами L	Ймовірність несанкціонованого відновлення $\Pr(A\|C, 4)$
10	$9{,}90099\times10^{-25}$
15	$5{,}91403\times10^{-29}$
20	$5{,}94560\times10^{-32}$
25	$2{,}81025\times10^{-34}$
30	$3{,}53678\times10^{-36}$
35	$8{,}75009\times10^{-38}$
40	$3{,}55049\times10^{-39}$

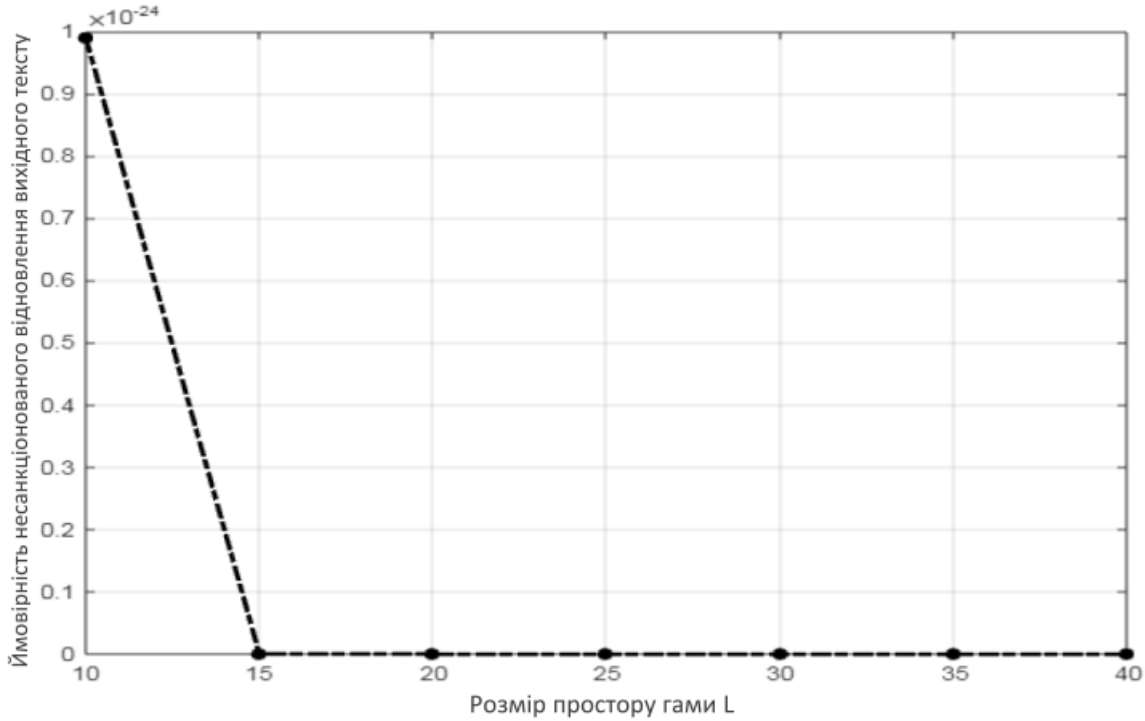

Рисунок 3.6 − Поведінка ймовірності несанкціонованого відновлення вихідного тексту за різних значень розміру простору гами

3.2 Метод захисту інформації в системі з цілочисельним розщепленням

Метод розщеплення суттєво ускладнює відновлення вихідного тексту несанкціонованим користувачем, що спирається на семантичний зміст. На відміну від ізольованого гамування, в результаті його застосування після процедури розщеплення досягається підвищена стійкість навіть за використання традиційного ГПВЧ. Це відбувається завдяки додатковому захисту даних в результаті розщеплення, оскільки замість символів тексту в каналі зв'язку або при захищеному зберіганні, будуть знаходитися символи, що не входять до звичайного алфавіту природної мови у вибраній кодовій таблиці. Крім того, внаслідок розщеплення у каналі можуть виникати символи, що належать алфавіту, але не мають жодного смислового змісту. Тому поширені методи несанкціонованого розкриття тексту, що базуються на семантичному виявлення регулярностей при передачі інформації, взагалі кажучи, перестають діяти.

У таблиці 3.7 наводиться декілька прикладів для символу, який передається по мережі, при одиночному гамуванні та при гамуванні після розщеплення.

Таблиця 3.7 - Результат захисту тексту в системі з розщепленням для вихідного символу *S*

Рівень розщеплення *k*	Результат системи з розщепленням	Відповідні символи
1	279	Ì
2	322277	ÅÌ
3	322279685	ÅÌê
4	322279713710	ÅÌêŒ
5	322279713708291	ÅÌŢå

Вихідні псевдовипадкові числа були створені за допомогою лінійного конгруентного генератора з наступними параметрами: початкове значення − 3, модуль − 500, множник − 3, збільшення − 8. Крім того, використовувався детермінований генетичний алгоритм, у якому розмір генерації – 40, кількість поколінь – 3, довжина хромосоми – 10.

Видно, що багато символів, які виникають ще до застосування гамування є або недрукованими, або не виправданими з погляду змісту, тобто семантики тексту.

У каналі зв'язку або у файлі, що зберігається, наприклад, у хмарі використовується бінарне кодування. У таблиці 3.7 наведено результати кодування та «символи», які можуть бути відновлені інтелектуальним агентом, спираючись на відому властивість процедури XOR. Таким чином, при розщепленні можуть непередбачуваним чином з'являтися «осмислені» символи, які насправді ніяк не пов'язані із змістом тексту. Слід зазначити, що відкидати «недруковані» символи без попередніх відомостей про зміст переданого матеріалу не можна

Крім того, на відміну від XOR, пропонований метод цілочисельного розщеплення не допускає поцілочисельного застосування гамування при відновленні вихідного тексту. Тому наведені у таблиці 3.7 дані отримані за допомогою досить громіздкої процедури відновлення. Для порівняння з процедурою розщеплення корисно навести зведення різних систем, у яких застосовується модульна арифметика.

У таблиці 3.8 представлені деякі математичні моделі для методів захисту даних на основі операцій модульної арифметики для порівняння з математичною моделлю цілочисельного розщеплення.

Крім того, відзначаються дві суттєві відмінності представленого методу цілочисельного розщеплення від перерахованих відомих методів захисту інформації, що застосовують операції модулярної арифметики. Вони полягають у тому, що операція із застосуванням модуля в запропонованому методі

розщеплення використовується k-1 раз і вона не пов'язується з розміром алфавіту.

Перелічені властивості ускладнюють семантичне відновлення вихідного тексту, тобто відновлення несанкціонованим користувачем за змістом. Можна зробити висновок, що все це ускладнює семантичне відновлення вихідного тексту несанкціонованим користувачем.

Таблиця 3.8 - Деякі математичні моделі методів заміни, засновані на операціях модульної арифметики

	Метод захисту Цезаря	Метод захисту Віженера	Афінний шифр	Метод захисту Хілла
Математична модель захисту	$c=(m+k) \bmod n$	$c_i=(m_i+k_i) \bmod n$	$E(m)=(am+b) \bmod n$	$C=(K\times M) \bmod n$
Математична модель відновлення	$m=(c-k) \bmod n$	$m_i=(c_i-k_i) \bmod n$	$D(c)=a^{-1}(c-b) \bmod n$	$M=(K^{-1}\times C) \bmod n$
Примітка	Модуль n – розмір алфавіту			

Метод цілочисельного розщеплення застосовується в роботі до окремих символів вихідного тексту.

3.3 Ілюстрація роботи методу захисту інформації на основі цілочисельного розщеплення

Розглянемо хід роботи методу захисту інформації на основі цілочисельного розщеплення

а) нехай рівень цілочисельного розщеплення k=1. Для експерименту було обрано вихідний текст, що складається з одного символу "S". При виборі лінійного конгруентного генератора на основі ключа захисту (ключ показаний на рисунку 3.7), побудована гама (r), показана на рисунку 3.8.

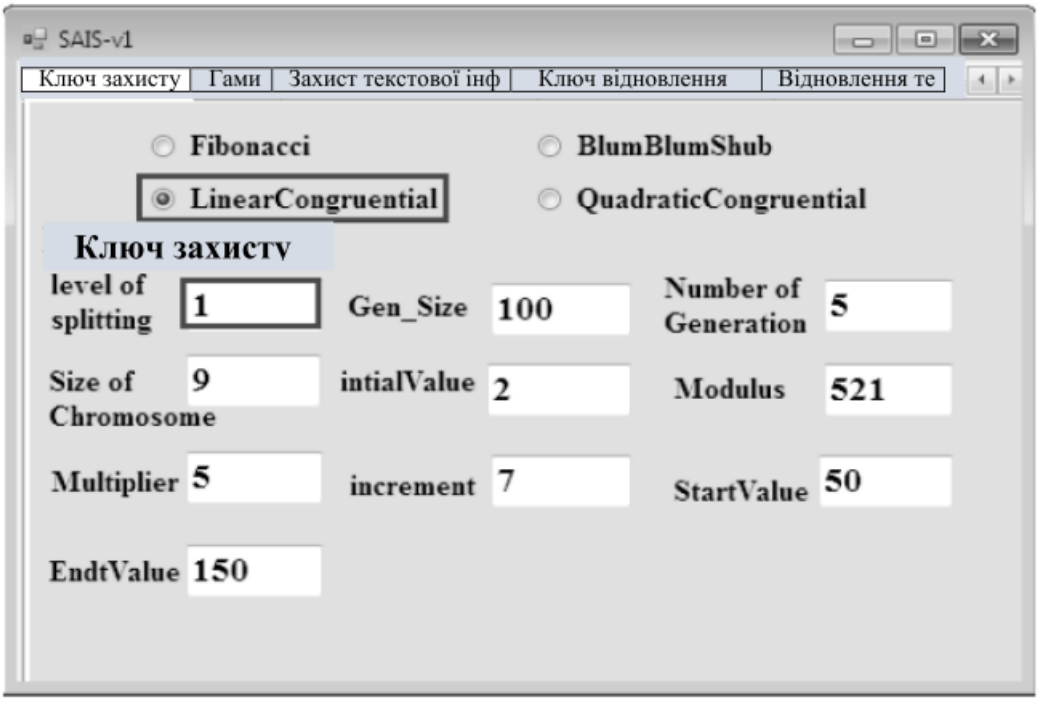

Рисунок 3.7 – Ключ захисту (рівень цілочисельного розщеплення k=1)

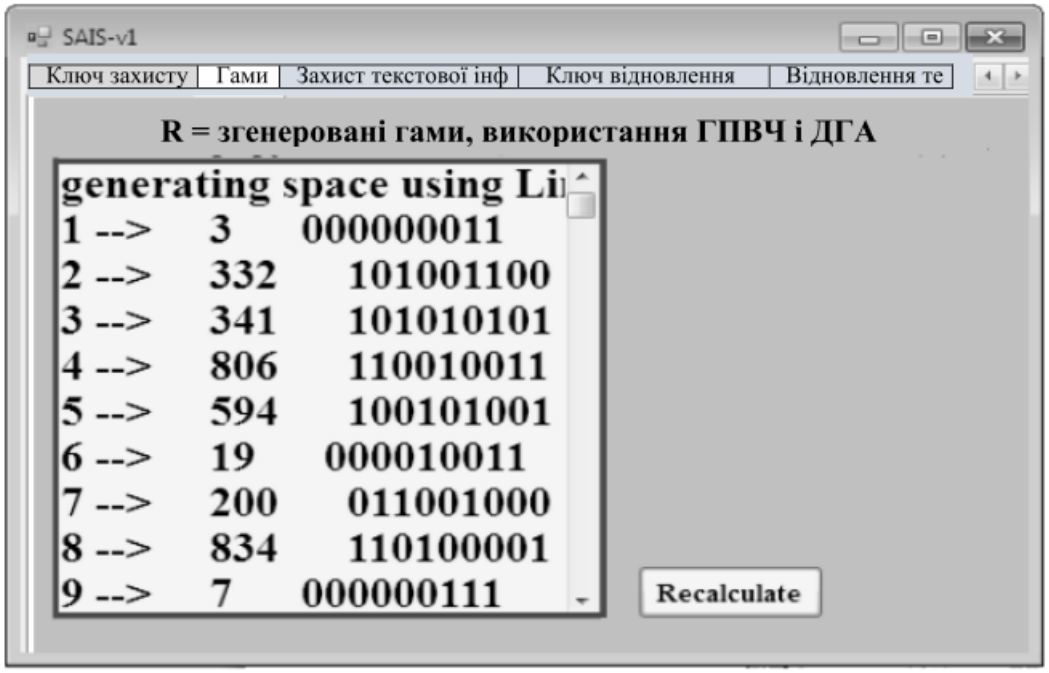

Рисунок 3.8 − Гама (r) (рівень цілочисельного розщеплення k=1)

Захищений текст буде обчислений і становить 81, як це показано на рисунку 3.9.

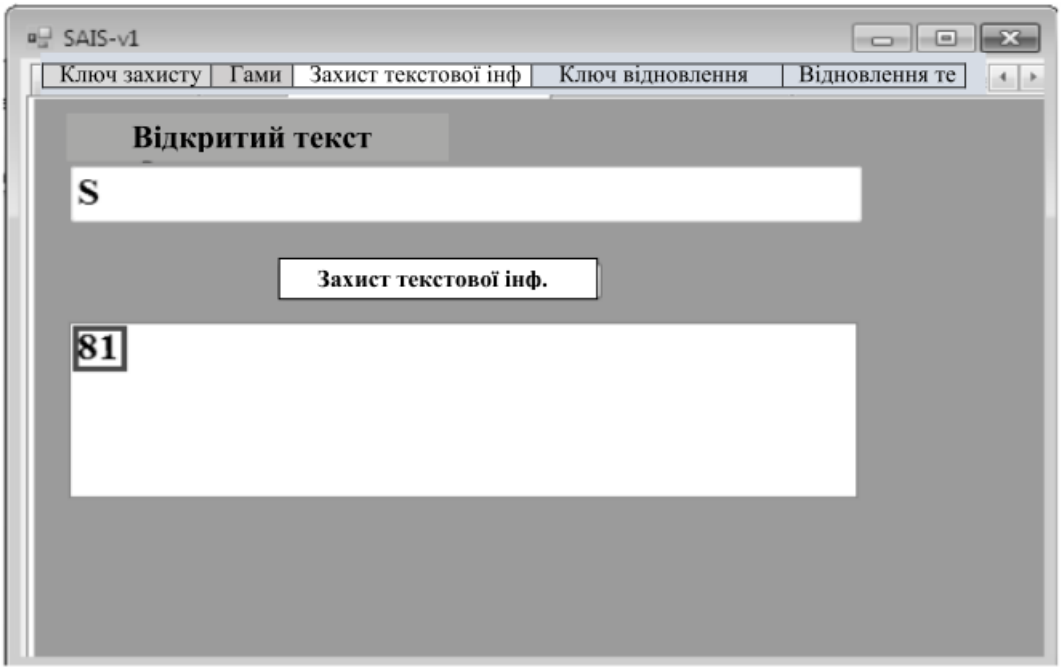

Рисунок 3.9 − Процесс захисту текстової інформації (рівень цілочисельного розщеплення *k*=1)

В процесі відновлення, якщо ввести ключ відновлення, як показано на рисунку 3.10, отримується вихідний текст="S", як показано на рисунку 3.11.

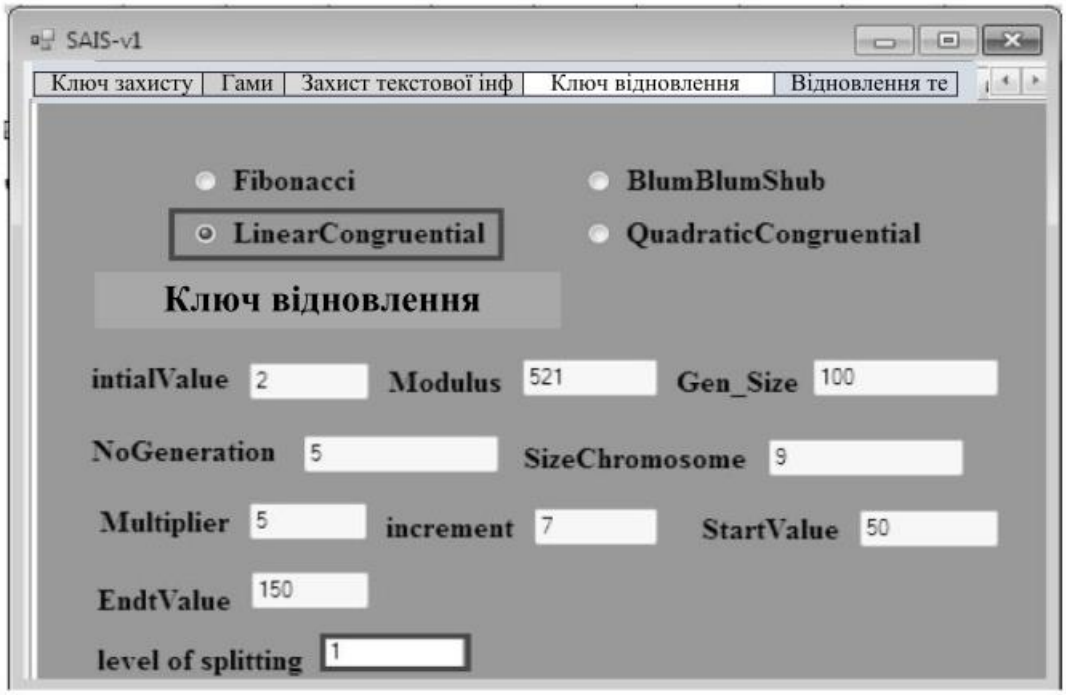

Рисунок 3.10 − Ключ відновлення (рівень цілочисельного розщеплення *k*=1)

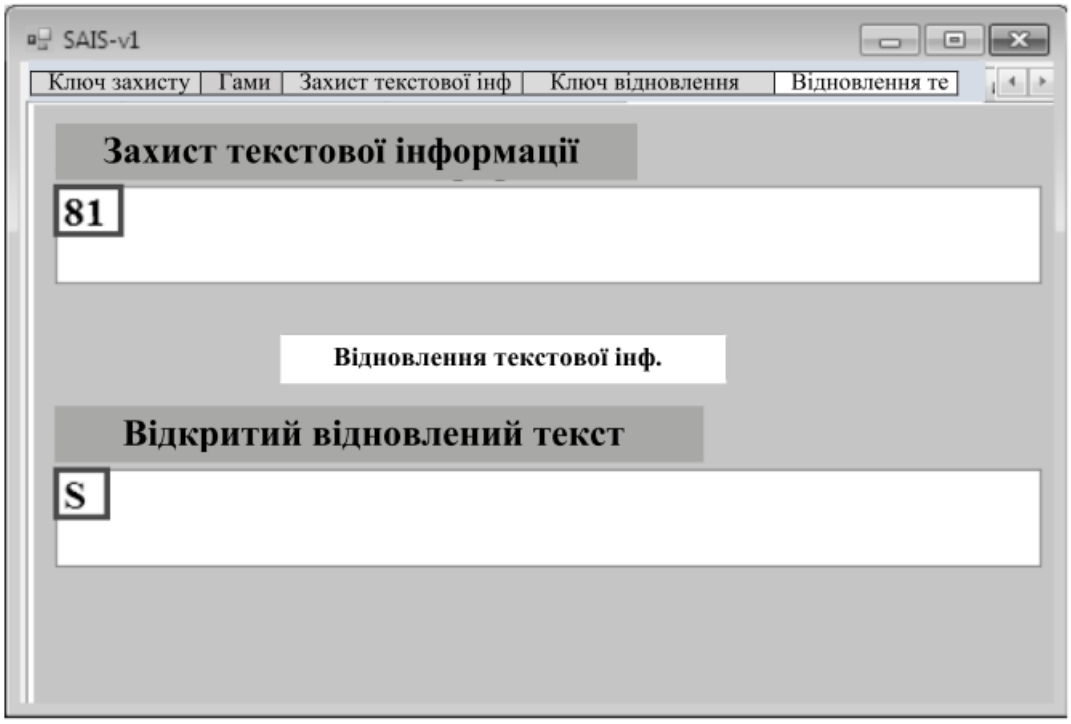

Рисунок 3.11 – Відновлений текст (рівень цілочисельного розщеплення k=1)

б) нехай рівень цілочисельного розщеплення k=2. Тоді для ключа захисту, як показано на рисунку 3.12, отримається захищений текст = {481 385} рисунок 3.13.

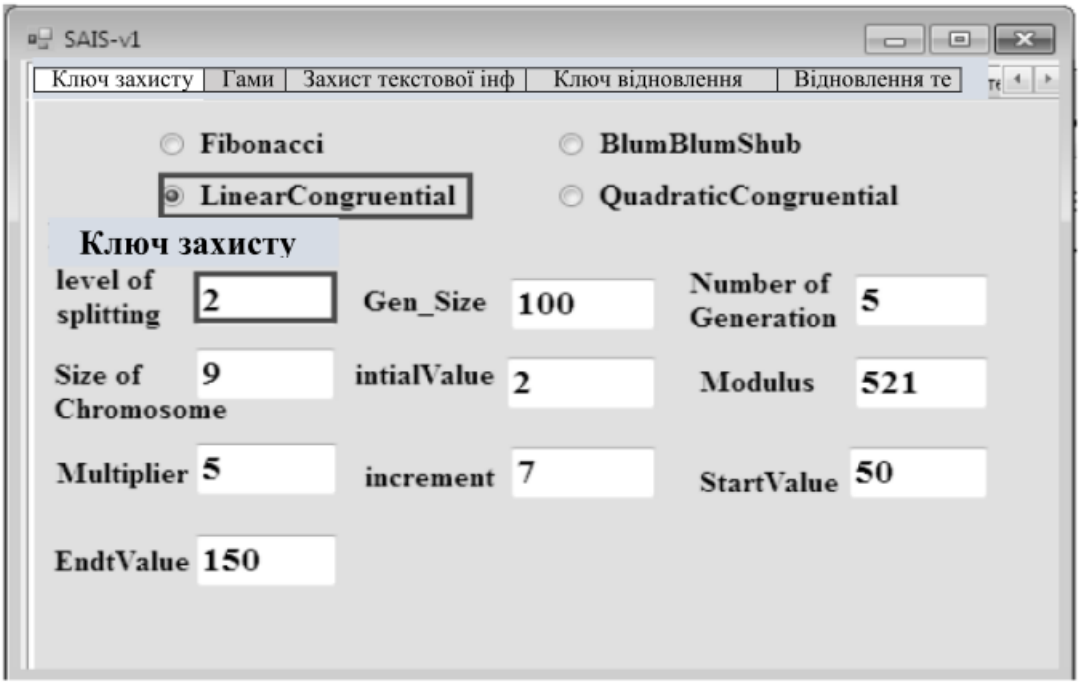

Рисунок 3.12 − Ключ захисту (рівень цілочисельного розщеплення k=2)

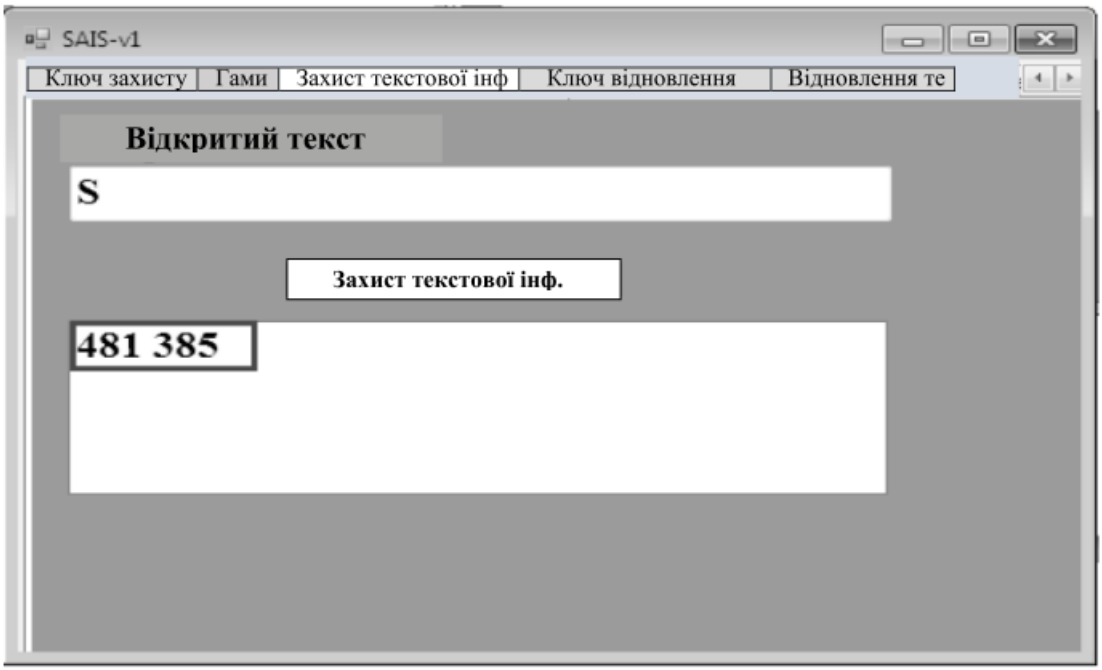

Рисунок 3.13 − Захищений текст у відповідності з вказаним ключем захисту (рівень цілочисельного розщеплення k=2)

в) Нехай рівень цілочисельного розщеплення для ключа захисту k=3 (рисунок 3.14), отримається захищений текст = {481 386 1144}, як показано на рисунку 3.15.

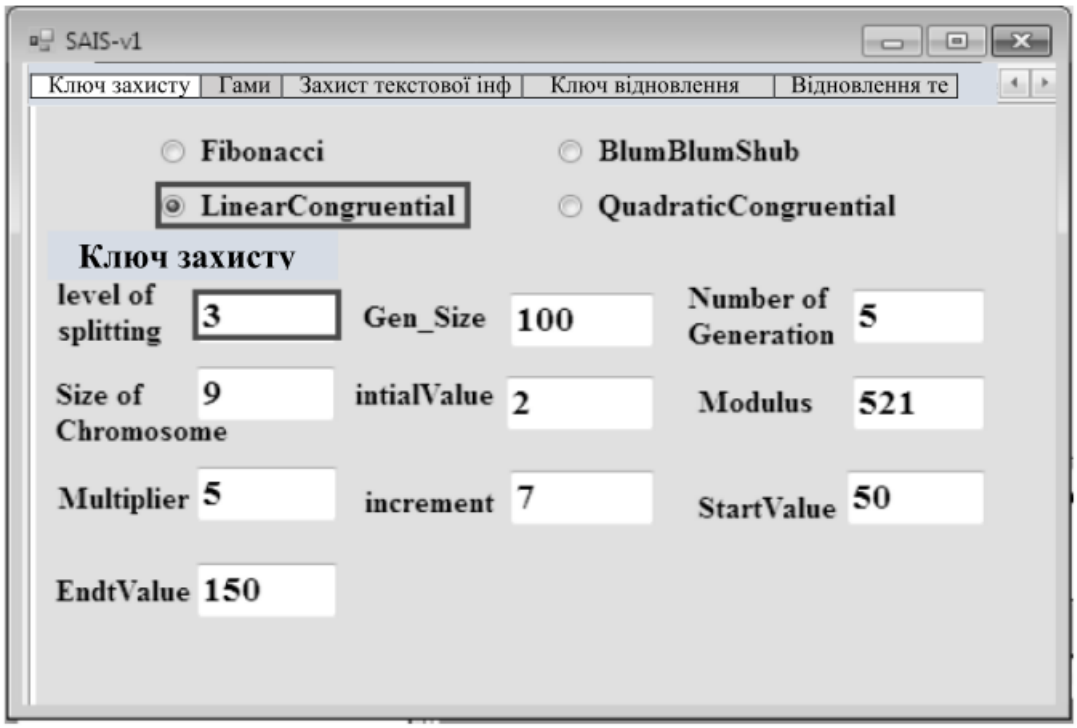

Рисунок 3.14 − Ключ захисту (рівень цілочисельного розщеплення k=3)

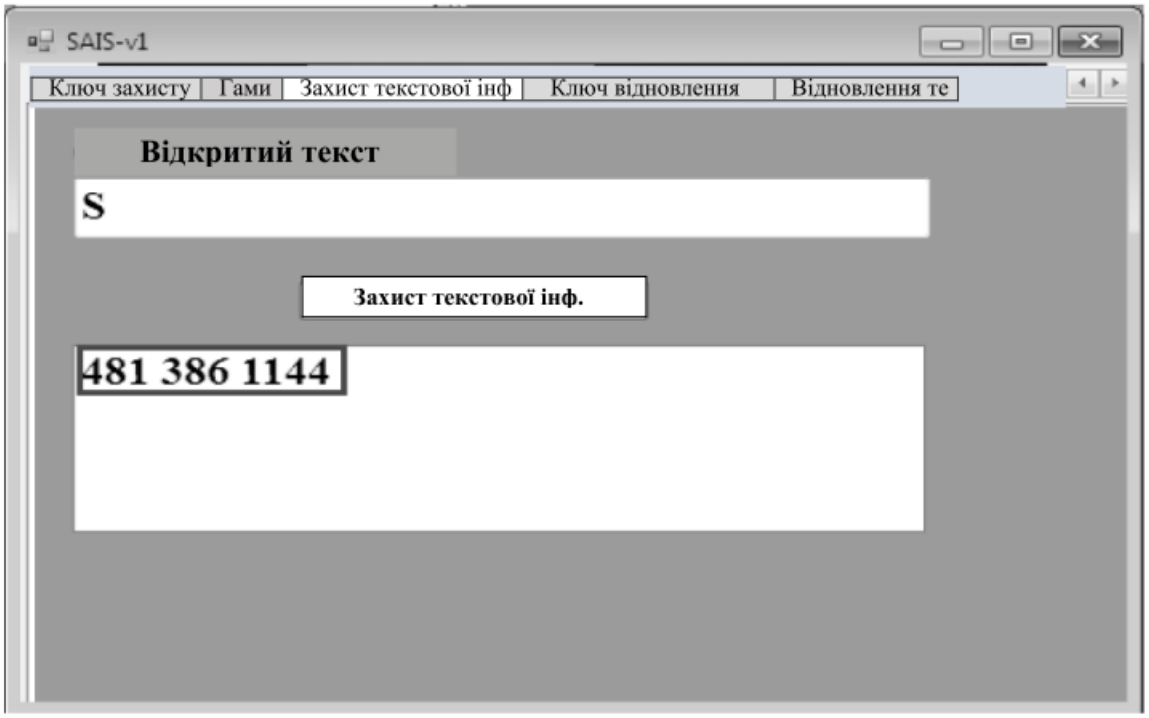

Рисунок 3.15 − Захищений текст у відповідності з вказаним ключем захисту (рівень цілочисельного розщеплення k=3)

г) нехай рівень цілочисельного розщеплення для ключа захисту k=4 (рисунок 3.16). Тоді отримається захищений текст = {481 386 1070 382} (рисунок 3.17).

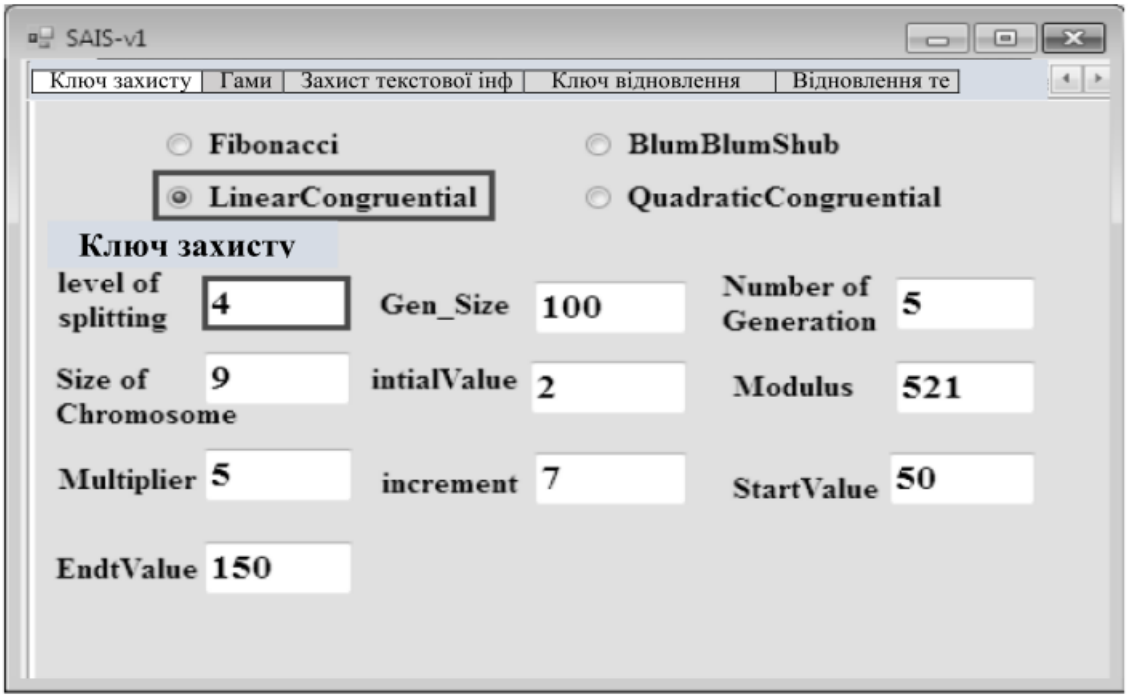

Рисунок 3.16 − Ключ захисту (рівень цілочисельного розщеплення k=4

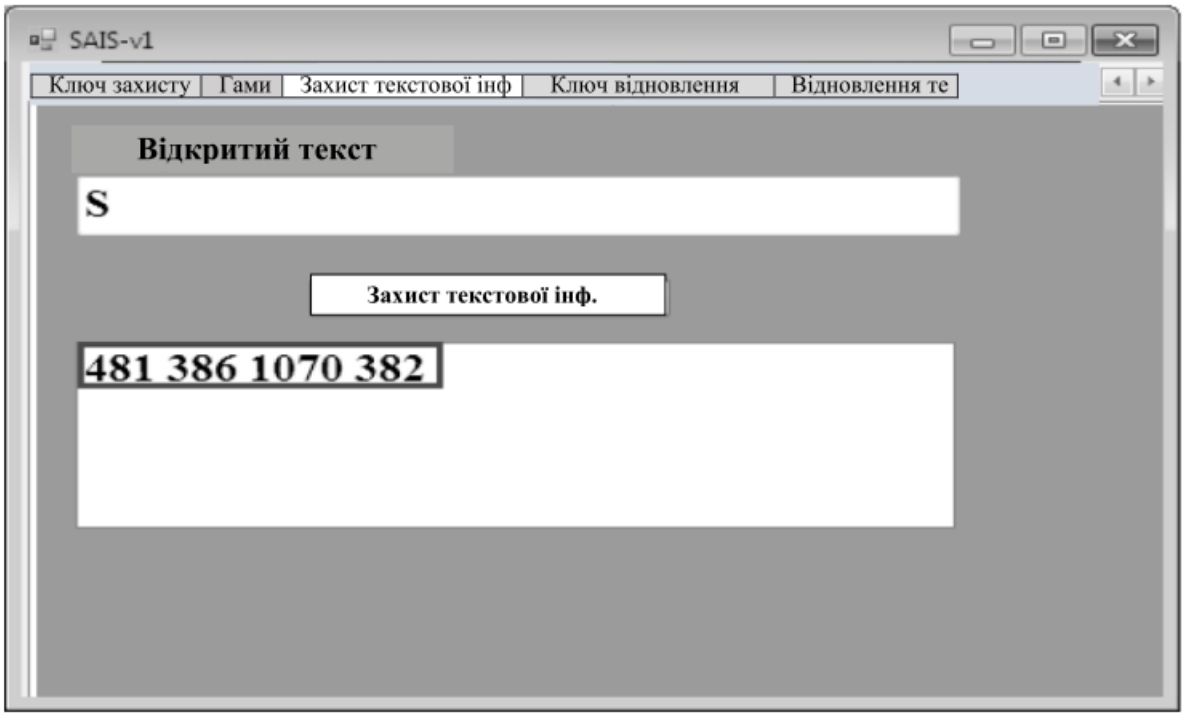

Рисунок 3.17 − Захищений текст у відповідності з ключем захисту (рівень цілочисельного розщеплення k=4

Отже, створений і реалізований математичний апарат, що базується на використанні модульної арифметики на додаток до дослідження нової процедури, яка називається цілочисленним розщепленням. Згідно з нею ціле число представляється унікальним чином у вигляді послідовності k цілих чисел. Розщеплення нагадує китайську теорему про залишки, відрізняючись від неї кардинальним чином за математичними властивостями. Згідно теоретичних викладок реалізовано відповідну програмну систему.

ВИСНОВКИ

1. Здійснено аналіз сучасних підходів до захисту інформації методом цілочисельного розщеплення, що дало можливість обгрунтувати вибір відповідних алгоритмів захисту інформації та дослідити їх стійкість на основі імовірнісного аналізу.

2. Розроблено алгоритмічне забезпечення для процедури цілочисельного розщеплення та відновлення числа, що дозволило здійснити порівняння методів захисту інформації на основі модулярної арифметики та цілочисельного розщеплення.

3. Проведено імовірнісний аналіз стійкості захисту інформації методом цілочисельного розщеплення, що дозволило встановити його переваги та недоліки в порівнянні з існуючими цілочисельними методами захисту інформації.

4. Виконана програмна реалізація методу захисту інформації на основі цілочисельного розщеплення, розроблено схему та інтерфейс роботи методу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Roy R., Datta D., Bhagat S., Saha S., Sinha A. Comparative Study and Analysis of Performances among RNS, DBNS, TBNS and MNS for DSP Applications. Journal of Signal and Information Processing. 2015. Vol. 6. P. 49-65.

2. Kundu P., Bandyopadhyay O., Sinha A. An Efficient Architecture of RNS Based Wallace Tree Multi- plier for DSP Application. Circuits and Systems. 2008. Vol. 48. P. 221-224.

3. Cardarilli G.C., Nannarelli A., Re A. Residue Number System for low-power DSP applications. Signals, Systems and Computers: Proceedings of the 41st Asilomar Conference. 2007. P. 1412–1416.

4. Wnuk M. Remarks on hardware implementation of image processing algorithms. International Journal of Applied Mathematics and Computer Science. 2008. Vol.18(1). P. 105–110.

5. Wang W., Swamy M.N.S., Ahmad M.O. RNS application for digital image processing. System-on-Chip for Real-Time Applications (IWSOC'04): Proceedings of the 4th IEEE International Workshop, Banff, Alberta, Canada. 2004. P. 77–80.

6. Piestrak S.J., Berezowski K. Architecture of efficient RNS-based digital signal processor with very low-level pipelining. IET Irish Signals and Systems Conference (ISSC 2008): Proceedings of the International Conference, Galway, Republic of Ireland. 2008. P. 127–132.

7. Николайчук Я.М. Теорія цифрових перетворень мультибазисного супершвидкодіючого процесора. Искусственный интеллект. 2008. №4. С. 387-394.

8. Николайчук Я.М., Возна Н.Я., Пітух І.Р. Проектування спеціалізованих комп'ютерних систем. Тернопіль: ТзОВ: Терн граф, 2010. 392 с.

9. Яцків В.В. Теоретичні основи створення і структурна організація компонентів безпровідних сенсорних мереж підвищеної ефективності: дис. д-ра техн. наук: 05.13.05. Львів: НУ «ЛП», 2016. 327 с.

10. Яцків В.В. Метод підвищення надійності передачі даних в безпровідних сенсорних мережах на основі системи залишкових класів. Радіоелектроніка та інформатика. 2010. №2. С.32–35.

11. Hu Zhengbing, Yatskiv V., Sachenko A. Increasing the Data Transmission Robustness in WSN Using the Modified Error Correction Codes on Residue Number System. Elektronika ir Elektrotechnika. 2015. Vol 21(1). P. 76-81.

12. Pikh V., Kimak V., Krulikovskyi B. Synthesis of High-performance Components of Spectral Analyzers and Special Processors for Data Encryption in Rademacher-Krestenson's Theoretical-numerical Basis. Experience of Designing and Application of CAD Systems in Microelectronics (CADSM-2015): Proceedings of the 13th International Conference. 2015. P.182-184.

13. Vozna N., Nykolaichuk Ya., Zastavnyy O., Pikh V. System complexity criteria and synthesis of high-performance multifunctional parallel ADC in Rademacher's and Haar-Krestenson's theoretical and numerical bases. Experience of Designing and Application of CAD Systems in Microelectronics (CADSM-2017): Proceedings of the 14th International Conference. 2017. P. 218-221.

14. Vergos H. On the design of efficient modular adders. J. Circuits, Syst. and Comput. 2005. Vol. 14 (5). P. 965–972.

15. Anitha K., Arulananth T.S., Karthik R., Bhaskara P. Reddy Design and Implementation of Modified Sequential Parallel RNS Forward Converters. International Journal of Applied Engineering Research. 2017. Vol. 12 (16). P. 6159-6163.

16. Яцків В.В. Виявлення та виправлення багатократних помилок на основі модулярних коректуючих кодів. Інформаційні технології та комп'ютерна інженерія. 2015. Том 33, №2. С.77-82. 88.

17. Яцків В.В., Цаволик Т.Г. Двовимірні коректуючі коди на основі модулярної арифметики. Вісник Хмельницького національного університету. Технічні науки. 2015. № 4 (227). С.144-148.

18. Xiao H., Garg H., Hu J., Xiao G. New Error Control Algorithms for Residue Number System Codes. Electronics and Telecommunications Research Institute. 2016. Vol. 38 (2). P.326-336.

19. Lo H., Lin T. Parallel Algorithms for Residue Scaling and Error Correction in Residue Arithmetic. Wireless Eng. Technol. 2013. Vol. 4 (4). P. 198–213.

20. Patel R A., Benaissa M., Powell N., Boussakta S. Novel power-delay-area-efficient approach to generic modular addition. IEEE Transactions on Circuits and Systems. 2007. V.54. P. 1279-1292.

21. Perin G., Imbert L. Electromagnetic analysis on RSA algorithm based on RNS. Euromicro Conference on Digital System Design (DSD): Proceedings. 2013. Vol.1. P. 345–352.

22. Laurent I., Jean-Claude B. A Full RNS Implementation of RSA. Transactions on computers. 2004. Vol.53 (5). P. 1-6.

23. Nobuhiro T., Teruki I. Design of High-Speed RSA Encryption Processor Based on the Residue Table for Redundant Binary Numbers. Systems and Computers in Japan. 2002. Vol. 33(5). P. 423-432.

24. Singh N. An overview of Residue Number System. Devices, Circuits & Communication: Proceedings of the National Seminar. 2008. P. 132-135.

25. Hema V., Ganaga Durga M. Data Integrity Checking Based On Residue Number System and Chinese Remainder Theorem In Cloud. International Journal of Innovative Research in Science, Engineering and Technology. 2014. Vol.3 (3). P. 2584-2588.

26. Hoffstein J., Pipher J., Silverman J. An Introduction to Mathematical Cryptography. Springer Science+Business Media, LLC, 2008. 524 p.

27. Jeffrey H., Jill P., Joseph H. An Introduction to Mathematical Cryptography. Berlin: Springer, 2008. 540 p.

28. Задірака В.К., Олексюк О.С. Комп’ютерна криптологія. Тернопіль, Київ, 2002. 504 с.

29. Shoup V. A Computational Introduction to Number Theory and Algebra. Cambridge University Press, 2005. 517 p.

30. Stillwell J. Elements of Number Theory. Springer, 2010. 256 p.

31. Hardy G.H., Wright E.M., Wiles A. An Introduction to the Theory of Numbers. Oxford University Press, 2008. 656 p.

32. Карпів В., Момотюк О., Касянчук М. Математична модель захисту інформації на основі цілочисельного розщеплення. Збірник матеріалів науково - практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ-2024), Тернопіль, 2024. С.115-117.

33. Карпів В., Крук О., Казьмірчук Н. Імовірнісний аналіз стійкості методу розщеплення для захисту інформації. Матеріали науково-практичного симпозіуму «Захист інформації». Тернопіль, 2024. С.89-92.

ДОДАТОК А Копії публікацій



ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»
ГАЛИЦЬКИЙ ФАХОВИЙ КОЛЕДЖ ІМ. В'ЯЧЕСЛАВА ЧОРНОВОЛА

КІБЕРБЕЗПЕКА ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ (КБКІТ – 2024)

науково-практична конференція
молодих вчених, аспірантів та студентів

26–28 серпня 2024
Тернопіль

Збірник матеріалів науково-практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ - 2024), Тернопіль, 2024. - 160 с.

Адреса редакції:
Західноукраїнський національний університет, кафедра кібербезпеки,
вул. Олени Теліги 8, м. Тернопіль 46003
Контакти:
*e-mail:*conferencekb@gmail.com

УДК 004.056.2

Віталій КАРПІВ, Олег МОМОТЮК, Михайло КАСЯНЧУК

Західноукраїнський національний університет

МАТЕМАТИЧНА МОДЕЛЬ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ЦІЛОЧИСЕЛЬНОГО РОЗЩЕПЛЕННЯ

Вступ. В даний час арифметика в залишках активно застосовується в цифровій обробці сигналів, обробці зображень, у розподілених інфокомунікаційних системах, бездротових сенсорних мережах, засобах забезпечення множинного доступу з кодовим поділом каналів, виявлення та виправлення помилок, у системах інформаційної безпеки, хмарних обчисленнях тощо [1].

Для асиметричної криптографії на операції ділення націло з остачею грунтується переважна більшість відомих методів, зокрема, метод Цезаря, афінна система підстановок Цезаря, метод Хілла, метод Віженера тощо [2].

Однак у цих методах не розглядалося питання багатократного застосування такої операції для кожного символу з метою підвищення рівня безпеки і створення додаткових труднощів для контролю повідомлень, що передаються зі сторони несанкціонованого користувача. Тому тема роботи є актуальною.

Мета: розробити математичну модель захисту інформації на основі цілочисельного розщеплення.

1. Математична модель захисту інформації на основі цілочисельного розщеплення

Нехай дано два додатних цілих числа r і a , для яких виконується нерівність $0<a<r$. Цілочисельним розщепленням числа a за базою r називається подання числа a у вигляді послідовності чисел a_1, a_2, a_3, …, a_{k-1}, a_k, в якій виконуються такі рівності:

$$
\begin{aligned}
&a_1=\delta^{(2)}, \text{ де } \delta^{(2)}=r \bmod a,\\
&a_2=\delta^{(3)}, \text{ де } \delta^{(3)}=r \bmod q^{(2)},\ q^{(2)}=\left\lfloor \frac{r}{a} \right\rfloor,\\
&a_3=\delta^{(4)}, \text{ де } \delta^{(4)}=r \bmod q^{(3)},\ q^{(3)}=\left\lfloor \frac{r}{q^{(2)}} \right\rfloor,\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \ldots\ldots\ldots\ldots \qquad (1)\\
&a_{k-1}=\delta^{(k)}, \text{ де } \delta^{(k)}=r \bmod q^{(k-1)},\ q^{(k-1)}=\left\lfloor \frac{r}{q^{(k-2)}} \right\rfloor,\\
&a_k=q^{(k)}, \text{ де } q^{(k)}=\left\lfloor \frac{r}{q^{(k-1)}} \right\rfloor,
\end{aligned}
$$

де $\delta^{(2)}$ – залишок при цілочисельному діленні r на a, а $q^{(i)}$ – ціла частина при такому діленні; $\delta^{(i)}$ – залишок при цілочисельному діленні r на $q^{(i-1)}$; символ $\lfloor\ \rfloor$ означає округлення до найближчого цілого в меншу сторону.

Натуральне число k називається рівнем розщеплення. Цілочисельне розщеплення є певним узагальненням математичної операції ділення із залишком.

Блок-схема цілочисельного розщеплення числа a за базою r при рівні розщеплення k показана на рисунку 1.

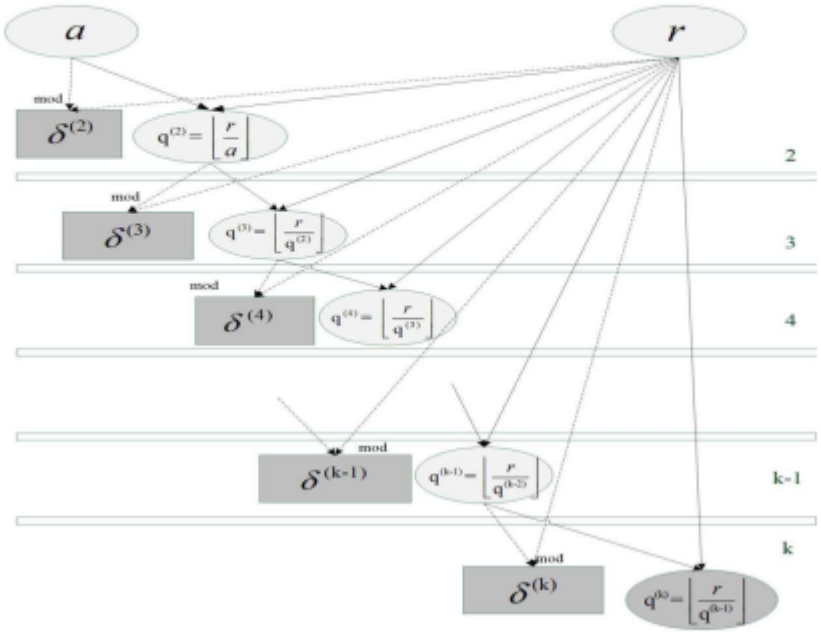

Рисунок 1 - Блок-схема цілочисельного розщеплення числа a за базою r при рівні розщеплення k

Функцією відображення $\Phi_k(a, r)$ називається результат цілочисельного розщеплення числа a за основою r.

Відповідно до (1), функція відображення $\Phi_k(a, r)$ при рівні розщеплення, що дорівнює k, задається наступним співвідношенням:

$$\Phi_k(a, r)=(\delta_a^{(2)}, \delta_a^{(3)}, \delta_a^{(4)}, \ldots, \delta_a^{(k-1)}, \delta_a^{(k)}, q_a^{(k)}). \quad (2)$$

Наприклад, відображення $\Phi_k(a, r)$ при рівні розщеплення k=3 визначається наступним співвідношенням:

$$\Phi_3(a, r)=(\delta_a^{(2)}, \delta_a^{(3)}, q_a^{(3)}).$$

2. Розщеплення по векторній базі

Усі теореми допускають природне узагальнення, зв'язане з динамікою у застосунках. Зокрема, можна розглядати узагальнене розщеплення рівня k за векторною базою. Розщеплення по векторній базі - це узагальнене розщеплення рівня k по векторній базі $\vec{r}=(r_1, r_2, \ldots, r_l)$. Причому черговий ($i$-ий) крок процесу цілочисельного розщеплення виконується щоразу при новому значенні бази розщеплення.

Узагальненим цілим розщепленням числа a по векторній базі

$$\vec{r}=(r_1, r_2, \ldots, r_l),\ l=k-1,$$

називається подання числа a у вигляді послідовності цілих чисел $a_1, a_2, a_3, \ldots, a_{k-1}, a_k$, у якій:

$$a_1=\delta^{(2)}, \text{ де } \delta^{(2)}=r_1 \bmod a,\ r_1>a,$$

$$a_2=\delta^{(3)}, \text{ де } \delta^{(3)}=r_2 \bmod q^{(2)},\ q^{(2)}=\left\lfloor \frac{r_1}{a} \right\rfloor,\ r_2>q^{(2)},$$

$$a_3=\delta^{(4)}, \text{ де } \delta^{(4)}=r_3 \bmod q^{(3)},\ q^{(3)}=\left\lfloor \frac{r_2}{q^{(2)}} \right\rfloor,\ r_3>q^{(3)},$$

$$\ldots\ldots\ldots\ldots \qquad (3)$$

$$a_{k-1}=\delta^{(k)}, \text{ де } \delta^{(k)}=r_{k-1} \bmod q^{(k-1)},\ q^{(k-1)}=\left\lfloor \frac{r_{k-2}}{q^{(k-2)}} \right\rfloor,\ r_{k-1}>q^{(k-1)},$$

$$a_k=q^{(k)}, \text{ де } q^{(k)}=\left\lfloor \frac{r_{k-1}}{q^{(k-1)}} \right\rfloor.$$

Тут символи $\delta^{(i)}$ позначають залишки при цілочисельному діленні r_i на $q^{(i)}$. Це визначення є узагальненням схеми математичного цілочисельного розщеплення. Таке розщеплення виявляється найбільш корисним у застосунках, пов'язаних із захистом інформації, що передається.

Є багато способів, які можуть бути виконані для перевірки правильності вилучення відкритого тексту із зашифрованого з використанням процедури узагальненого розщеплення на стороні одержувача.

Один із цих способів, в яких обробляється символ за символом, можна пояснити так:

1) якщо значення перевіряє умову $r_i>q^{(i)}$, де i=2, 3, …, k-1, тобто використовують його у процесі шифрування;

2) якщо значення r_i не перевіряє умову $r_i>q^{(i)}$, де i=2, 3, …, k-1, то в процесі шифрування виконуються такі кроки:

- пропустити поточне значення ri і використовувати наступне значення ri+1 у згенерованій послідовності гам;
- додати 0 ліворуч від результату залишку, який буде розрахований з використанням гами r_{i+1} (функція цього 0 не змінить значення залишку, але в процесі отримання відкритого тексту повідомить одержувача зашифрованого тексту про те, що в послідовності гам є невикористане пропущене значення r_i.

Передбачається, що зв'язок безшумний, тобто у каналі зв'язку відсутні перешкоди. Однак наявність перешкод можна грубо оцінити теоретично при передачі замість символу його розщеплення. У цій роботі буде всюди передбачатися, що канал зв'язку є безшумним, як і у випадку передачі даних між двома комп'ютерами виділеної лінії.

Висновок. Розроблено математичну модель захисту інформації на основі цілочисельного розщеплення.

Перелік використаних джерел.

1. Samuel S., Wagstaff Jr. Cryptanalysis of Number Theoretic Ciphers. RC Press, 2019. 336c.

2. Rubin F. Secret Key Cryptography: Ciphers, from Simple to Unbreakable. Manning, 2022. 344c.

ГРОМАДСЬКА ОРГАНІЗАЦІЯ
«КІБЕРБЕЗПЕКА І АВТОМАТИЗАЦІЯ»

Матеріали
науково-практичного симпозіуму
«ЗАХИСТ ІНФОРМАЦІЇ»

30 листопада 2024
Тернопіль

У збірнику опубліковано матеріали науково-практичного симпозіуму «Захист інформації», Тернопіль, 2024. - 130с.

Технічний редактор: Давлетова А.Я.

Адреса редакції:
Громадська організація «Кібербезпека і автоматизація»
м. Тернопіль
Контактний телефон: (066)043-42-10
e-mail: conferencekb@gmail.com

УДК 004.056.2

Віталій КАРПІВ, Олег КРУК, Назар КАЗЬМІРЧУК

Західноукраїнський національний університет

ІМОВІРНІСНИЙ АНАЛІЗ СТІЙКОСТІ МЕТОДУ РОЗЩЕПЛЕННЯ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ

Вступ. В сучасних умовах розвитку інформаційних технологій і комп'ютеризації роль інформації як одного із найбільш цінних і важливих активів в різних сферах неупинно зростає. Дослідження проблем розробки, удосконалення та застосування методів і засобів захисту інформації в процесі її передачі та зберігання набуло особливої важливості [1].

Для дослідження захищеності інформації використовуються різні ймовірності методи. Це дозволяє забезпечити ефективне функціонування мереж і систем зв'язку, а також забезпечення роботи складних динамічних систем, в яких поставало питання захисту як від незалежних зовнішніх впливів, так і від можливості втручання посторонніх осіб та систем [2]. Тому тема роботи є актуальною.

Мета: провести імовірнісний аналіз стійкості методу розщеплення для захисту інформації.

1. Імовірнісний аналіз стійкості методу розщеплення

Позначимо через C захищений текст, отриманий в результаті застосування методу розщеплення кожного символу вихідного тексту M, а через $\Pr(M|C,\ k)$ - ймовірність успішного відновлення вихідного тексту M, спираючись на доступний хакеру захищений текст C і невідомий йому рівень розщеплення k.

Порушнику відомі математичні моделі розщеплення та відновлення символу, але невідомий ключ, який використовується під час передачі. Порушник має доступ до інформації, що передається каналом зв'язку. Йому невідомо, чи використовується просте розщеплення, чи узагальнене. У таблиці 1 наведено числові значення для ймовірності несанкціонованого відновлення вихідного тексту за різних значень k.

Таблиця 1 - Ймовірність несанкціонованого відновлення вихідного тексту за різних значень рівнів розщеплення

Рівень розщеплення k	**Ймовірність несанкціонованого відновлення $\Pr(M\|C, k)$, $\times 10^{-8}$**
2	8,77914
3	8,74030
4	8,73773
5	8,73755
6	8,73738
7	8,73737
8	8,73736

На рисунку 1 показано графік поведінки ймовірності рівнів розщеплення.

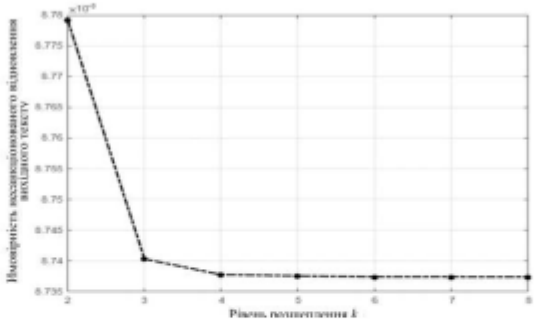

Рисунок 1 - Поведінка ймовірності несанкціонованого відновлення вихідного тексту за різних значень рівнів розщеплення k

Ймовірність несанкціонованого відновлення вихідного тексту M за результатом розщеплення C експоненційно зменшується зі зростанням розміру захищеного тексту N. У таблиці 2 наведено числові значення для ймовірності несанкціонованого відновлення вихідного тексту за різних значень розміру захищеного тексту N, а на рисунку 2 - їх графічна залежність.

Таблиця 2 - Ймовірність несанкціонованого відновлення вихідного тексту при різних значеннях розміру захищеного тексту

Розмір тексту N, який захищається	**Ймовірність несанкціонованого відновлення $\Pr(M\|C, 4)$**
5	0,00392
10	$1{,}31066\times10^{-6}$
15	$5{,}82676\times10^{-9}$
20	$1{,}73412\times10^{-12}$
25	$7{,}70719\times10^{-15}$
30	$2{,}28366\times10^{-18}$
35	$1{,}01496\times10^{-20}$

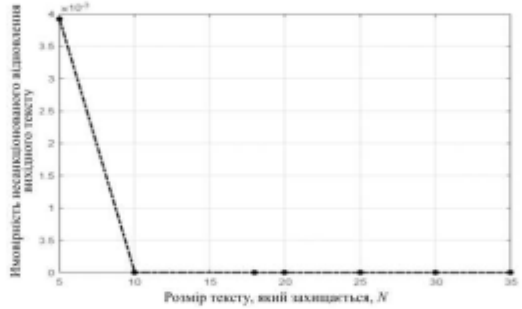

Рисунок 2 - Поведінка ймовірності несанкціонованого відновлення вихідного тексту при різних значеннях розміру тексту N, що захищається

Ймовірність несанкціонованого відновлення вихідного тексту M за результатом розщеплення C експоненційно зменшується зі зростанням числа всіх перебірних подій (виходів) L в просторі створеної ним гами з випадкових чисел.

Приклад: якщо вибираються значення параметрів k=4 і N=35, то отримується таблиця 3.

Таблиця 3 - Ймовірність несанкціонованого відновлення вихідного тексту за різних значень розміру простору гами L

Розмір простору гами *L*	**Ймовірність несанкціонованого відновлення Pr(*M*|*C*, 4)**
10	$9{,}9999\times10^{-18}$
15	$1{,}01496\times10^{-20}$
20	$7{,}62939\times10^{-23}$
25	$1{,}71799\times10^{-24}$
30	$7{,}74352\times10^{-26}$
35	$5{,}63434\times10^{-27}$
40	$5{,}82077\times10^{-28}$

У таблиці 3 наведено числові значення для ймовірності несанкціонованого відновлення вихідного тексту при k=4, N=35 та різних значень розміру простору гами L.

На рисунку 3 показано графічна залежність ймовірнсті несанкціонованого відновлення вихідного тексту для тих же різних значень розміру простору гами L.

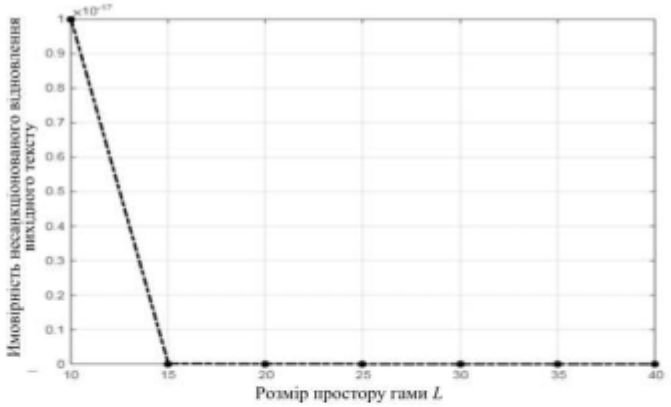

Рисунок 3 - Поведінка ймовірності несанкціонованого відновлення вихідного тексту за різних значень розміру простору гами L

У таблиці 4 наведено числові значення для ймовірності несанкціонованого відновлення вихідного тексту за різних значень k.

На рисунку 4 показано графік ймовірності для тих самих рівнів розщеплення.

Метод розщеплення суттєво ускладнює відновлення вихідного тексту несанкціонованим користувачем, що спирається на семантичний зміст.

Таблиця 4 - Ймовірність несанкціонованого відновлення вихідного тексту за різних значень рівнів розщеплення

Рівень розщеплення k	**Ймовірність несанкціонованого відновлення $\Pr(A\|C, k)$**
2	$8{,}77915\times10^{-8}$
3	$3{,}88358\times10^{-10}$
4	$2{,}43798\times10^{-11}$
5	$2{,}29460\times10^{-11}$
6	$1{,}61230\times10^{-12}$
7	$1{,}61227\times10^{-12}$
8	$1{,}61183\times10^{-12}$

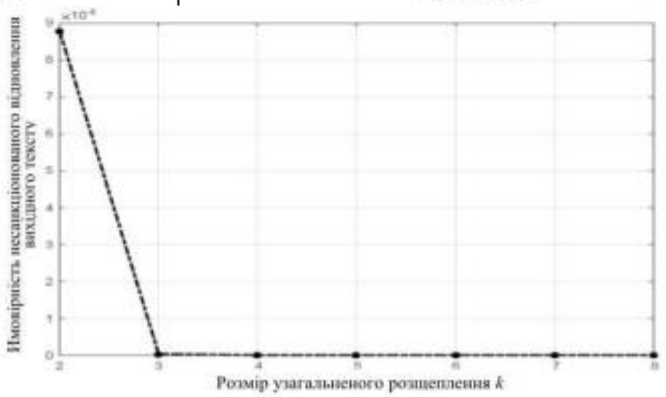

Рисунок 4 - Поведінка ймовірність несанкціонованого відновлення вихідного тексту за різних значень рівнів узагальненого розщеплення k

На відміну від ізольованого гамування, в результаті його застосування після процедури розщеплення досягається підвищена стійкість навіть за використання традиційного ГПВЧ. Це відбувається завдяки додатковому захисту даних в результаті розщеплення, оскільки замість символів тексту, будуть знаходитися символи, що не входять до звичайного алфавіту природної мови у вибраній кодовій таблиці.

Крім того, внаслідок розщеплення у каналі можуть виникати символи, що належать алфавіту, але не мають жодного смислового змісту. Тому методи несанкціонованого розкриття тексту, що базуються на семантичному виявлення регулярностей при передачі інформації перестають діяти.

Висновок. Проведено імовірнісний аналіз стійкості методу розщеплення для захисту інформації.

Перелік використаних джерел.

1. Simpson M.T., Antill Hands N. On Ethical Hacking and Network Defense. Cengage Learning, 2016. 512 p.

2. Samuel S., Wagstaff Jr. Cryptanalysis of Number Theoretic Ciphers. RC Press, 2019. 336 p.