синтез и восприятие речи : пер. с англ. / Джеймс Фланаган; [под ред. Пирогова А. А.]. – М. : Связь, 1968. – 396 с. 7. Дозорський В. Обгрунтування математичної моделі фрикативного звуку у вигляді періодично корельованого випадкового процесу / Я. Драган, Є. Яворська, В. Дозорський // Вісник Тернопільського національного технічного університету ім. І. Пулюя. – Тернопіль : ТНТУ ім. І. Пулюя, 2010. – Т. 15, № 10. – С. 159–164. 8. Драган Я. П. Енергетична теорія лінійних моделей стохастичних сигналів : моногр. / Я. П. Драган. – Львів : Центр стратегічних досліджень еко-біо-технічних систем, 1997. – XVI+333 с. 9. Чорна Л. Б. Стохастична модель голосового сигналу для задачі діагностики ритміки серця людини : дис. ... канд. техн. наук : 01.05.02 / Л.Б. Чорна / Тернопільський держ. технічний ун-т ім. Івана Пулюя. – Т., 1999. – 162 с. – Бібліогр. : С. 149–161.

УДК 531.36+534

І. Дронюк[1], А. Шкодин[1], І. Барабаш[1], М. Закала[2]
Національний університет "Львівська політехніка",
[1]кафедра автоматизованих систем управління,
[2]кафедра прикладної лінгвістики

МЕТОД ШИФРУВАННЯ ІНФОРМАЦІЇ НА ОСНОВІ ATEB-ФУНКЦІЙ

Розроблено алгоритми та програмне забезпечення для шифрування інформації на основі теорії Ateb-функцій, що пропонується застосувати для захисту інформації. Шифрування здійснюється за допомогою числових значень Ateb-функцій на певному діапазоні. Для того, щоб збільшити надійність шифрування, розроблено алгоритм приховання ключа у файлі.

Ключові слова: шифрування, Ateb-функції, захист інформації

The algorithms and software for encoding information based on the theory Ateb-functions offered to apply for protection. Encryption by using numerical values Ateb-functions on a certain range. To increase the reliability of the encryption algorithm hides the key in the file.

Keywords: encryption, Ateb-functions, information security

1. Вступ

У процесі розвитку суспільства людство поступово переходить від традиційних форм збереження інформації (паперових документів) і цінних паперів (грошей, векселів) до їхніх електронних аналогів. Виникає потреба у захисті електронних документів від несанкціонованого доступу. Одним із методів, що може забезпечити захист, є шифрування документів. Алгоритми шифрування поділяють на симетричні, асиметричні та хеш-функції.

Симетричні криптосистеми – спосіб шифрування, в якому для шифрування і дешифрування застосовується однаковий криптографічний ключ [1]. Нині симетричні шифри – це блокові та потокові шифри. До асиметричних криптосистем належить криптографічна система з відкритим ключем. Перевага асиметричних шифрів над симетричними шифрами полягає у тому, що не треба передавати секретний ключ [2]. Крім симетричних та асиметричних криптосистем, широко застосовують хеш-функції. Хеш-функції використовують для перевірки цілісності й автентичності інформації.

Захист інформації в електронному вигляді є важливою проблемою. Розвиток комп'ютерної техніки спонукає до постійного оновлення методів та засобів шифрування інформації [1]. Тому вибрана тема є актуальною. У цій роботі наведено симетричний алгоритм шифрування інформації на основі теорії *Ateb*-функцій та реалізацію відповідного програмного забезпечення.

2. Основна частина

Пропонуємо застосовувати теорію *Ateb*-функцій для шифрування інформації. Для цього розроблено методи обчислення значень періодичних *Ateb*-функцій, які базуються на розкладах у ряди Тейлора та Фур'є.

Відомо [3], що обчислювати необхідно одну з *Ateb*-функцій. Обчислимо функцію *Ateb*-синуса $sa(n,m,\omega)$, що задається оберненням інтеграла:

$$\Phi(\omega)=\omega-\frac{n+1}{2}\int_0^{\omega}\frac{d\overline{v}}{(1-\overline{v}^{n+1})^{\frac{m}{m+1}}}. \qquad (1)$$

Для реалізації обчислень визначених інтегралів використано методи прямокутників, трапецій та парабол [4].

Існують різні методи обчислення нулів функції: метод золотого перерізу, метод Фібоначі, дихотомічний метод та інші [4]. Для знаходження нулів функції (1) застосовано метод поділу відрізка навпіл.

Розроблено алгоритм обчислення значення *Ateb*-синуса на основі використання розкладу у ряд Тейлора. Описаний метод реалізовано у розробленому програмному забезпеченні.

Будь-яку періодичну функцію $F(\omega)$ з періодом $2\Pi=[-\Pi,\ \Pi]$ можна розкласти на цьому відрізку в ряд Фур'є. Оскільки функція *Ateb*-синуса $sa(n,m,\omega)$ є непарною, то розклад у ряд Фур'є має вигляд

$$sa(n,m,\omega)=\sum_{k=1}^{\infty}b_k\sin\frac{k\pi\omega}{\Pi}, \qquad (2)$$

де

$$b_k=\frac{1}{\Pi}\int_{-\Pi}^{\Pi}sa(n,m,y)\ \sin\frac{k\pi y}{\Pi}dy=\frac{n+1}{2\Pi}\int_{-\Pi}^{\Pi}\sin\frac{k\pi y}{\Pi}\int_0^{-1\le y\le 1}\frac{d\overline{y}}{\left(1-\overline{y}^{n+1}\right)^{\frac{m}{m+1}}}dy. \qquad (3)$$

У [5] доведено, що ряд (2) є збіжним.

Використаємо формулу (2) для обчислення *Ateb*-синуса. Основна складність полягає в обчисленні коефіцієнтів розкладу в ряд Фур'є, заданих формулами (3). Як видно з виведених формул, b_k подано у вигляді подвійних інтегралів. У записаному виразі внутрішній інтеграл є невластивим, адже при $y\to 1$ для b_k підінтегральні вирази прямують до нескінченності.

Опишемо метод обчислення *Ateb*-функцій за допомогою розкладів у ряди Фур'є. На початковому етапі вводимо вхідні дані: крок ітерації та параметри *Ateb*-функцій n і m. Після цього перевіряємо умову періодичності [3], відтак обчислюємо період *Ateb*-функції $\Pi(m,n)$. Обчислення виконуємо на проміжку $\left[0,\frac{1}{2}\Pi(m,n)\right]$ із заданим кроком. За цим алгоритмом можна обчислювати довільну *Ateb*–функцію, опис подамо для *Ateb*-синуса. Отже, обчислюємо функцію *Ateb*-синуса згідно з формулою (2) за допомогою ряду Фур'є. Обчислення суми ряду виконуємо до заданої точності.

Після цього вибираємо наступну точку. Якщо вона належить проміжку, то повертаємось до обчислень, якщо функція обчислена на всьому проміжку, то виводимо результати. Окремим блоком виділено розрахунок коефіцієнтів b_k, для чого використано наближені методи обчислення подвійних інтегралів та дихотомічний метод пошуку нулів функції [4]. Так реалізовано метод обчислення періодичних *Ateb*-функцій на основі розкладу у ряди Фур'є.

На основі розроблених методів реалізовано комп'ютерну програму. Програма обчислює період $\Pi(m,n)$ та значення *Ateb*-функції із заданим кроком на проміжку $[-\Pi(m,n);\Pi(m,n)]$ за двома методами, використовуючи ряди Тейлора та Фур'є. Обчислені числові значення виводяться на екран та у файл. На їх основі будуються графіки *Ateb*-функцій. Побудовані обома методами графіки збігаються, оскільки розраховані значення відрізняються цифрами після 10^{-6} порядку.

Щоб визначити ефективність обчислень за допомогою кожного з цих методів, порівняно результати моделювання для значень параметрів $n = m = 1$, що відповідає випадку тотожності *Ateb*-функції зі звичайним тригонометричним синусом. Значення звичайного синуса вибрано за точні значення у формулах обчислення відносної похибки (див. табл. 1). У табл. 1 подано вибіркові результати обчислень значень *Ateb*-синуса $sa(1, 1, \omega)$ на проміжку $\left[0, \frac{1}{2}\Pi(1, 1)\right]$ з кроком $\frac{1}{10}\Pi(1, 1)$ за допомогою рядів Тейлора і Фур'є, а також відповідні відносні похибки обчислень.

На основі табл. 1 проаналізовано відносні похибки обчислень значень *Ateb*-синуса sa(1,1,ω). Із показаних значень випливає, що порядок максимальної відносної похибки обчислень у обох випадках дорівнює 10^{-3}, що свідчить про високу ефективність запропонованих методів.

Отже, на практиці для випадку періодичних *Ateb*-функцій рекомендується застосовувати моделювання як на основі рядів Тейлора, так і на основі рядів Фур'є. Використаємо знайдені значення *Ateb*-функцій для шифрування інформації.

Таблиця 1

Оцінка результатів моделювання Ateb-синуса за розкладами у ряди Тейлора та ряду Фур'є (вибіркові дані)

Ітерація, i	ω_i	Синус $\sin(\omega_i)$	*Ateb*-синус $sa(1,1,\omega_i)$, за рядом Тейлора	*Ateb*-синус $sa(1,1,\omega_i)$, за рядом Фур'є	Відносна похибка за рядом Тейлора, %	Відносна похибка за рядом Фур'є, %
1	0,0785398163	0,0784590957	0,0784590957	0,0784626165	0,0000000000	0,0044874224
5	0,7068583471	0,6494480483	0,6494480483	0,6494525784	0,0000000043	0,0006975270
9	1,4922565105	0,9968616740	0,9969073337	0,9969029228	0,0045803458	0,0041378685

Опишемо алгоритм шифрування інформації на основі *Ateb*-функцій. Реалізацію методу опишемо на прикладі *Ateb*-синуса. Задаємо параметри *Ateb*-синуса *n*, *m* та крок обчислення *h*, де $0<h<0{,}1$. Значення $\langle n, m, h\rangle$ будуть ключем шифрування. Перевіряємо умову періодичності, якщо умова не виконується, генеруємо інший ключ. За заданими параметрами ключа обчислюємо *Ateb*-синус методом розкладу в ряд Тейлора в межах від 0 до $\Pi(m,n)$ із заданим кроком h та визначеною кількістю знаків після коми. Отриману послідовність використовуємо для шифрування вхідних даних із файла. Для шифрування у роботі вибрано операцію побітового додавання за модулем 2 "XOR". Також замість розкладу в ряд Тейлора можна використати розклад в ряд Фур'є.

Функція шифрування матиме вигляд:

$$Crypt(Ateb(n,m,x_i), Input),$$

де *Input* – вхідні значення, $x_i = i \cdot h$ – поточна точка обчислення, $i = 0, \ldots, P$; $P = \frac{\Pi(n,m)}{h}$.

Нехай

$$\langle n, m, h\rangle \qquad (4)$$

ключ шифрування. Це унеможливлює знаходження ключа методом підбору, оскільки діапазон можливих значень дуже великий. У формулі (4) n, m – параметри *Ateb*-синуса, h – крок обчислень, $h \in (0;\ 0,\ 1)$.

Обчислюємо значення *Ateb*-синуса з точністю до 10^{-10}. Нехай вхідне значення дорівнює $Input = 123$ і $Ateb(n,m,x_i) = 0{,}3245214735$. Тоді шифрування виконують так:

Результат = 123 XOR $G(Ateb(n,\ m,\ x_i)) = 123$ XOR 52147 = 52168,

де функція $G(Ateb(n,\ m,\ x_i))$ виконує перетворення значення *Ateb*-синуса з позиції 10^{-3} до 10^{-8} після коми до цілого числа. У такий спосіб послідовно шифруємо всю інформацію у вихідному файлі. Позиції цифр значень *Ateb*-синуса у алгоритмі шифрування можна змінювати.

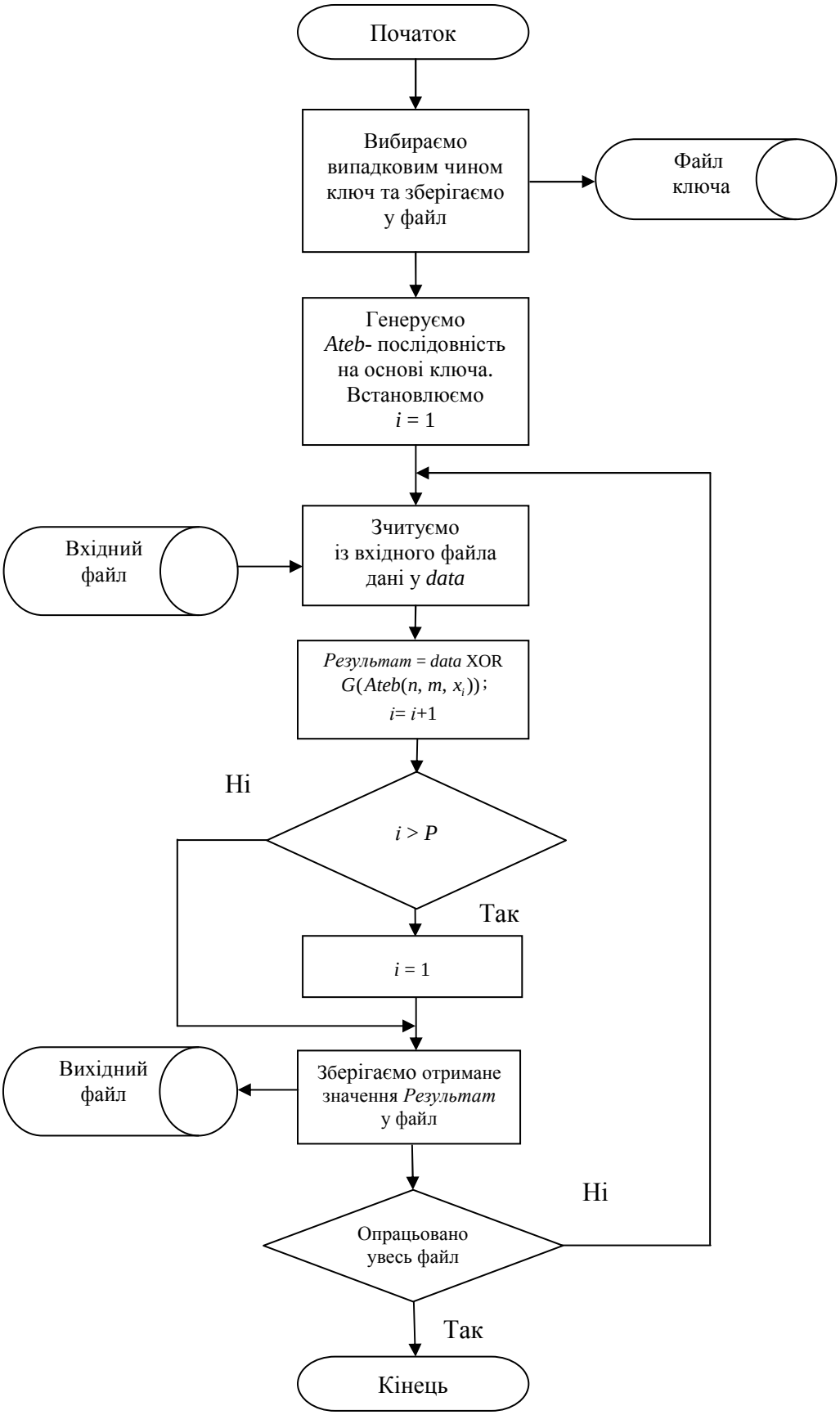

Рис. 1. Загальний алгоритм роботи програми шифрування

Кожне з чисел ключа $\langle n,\ m,\ h\rangle$ задається у програмі з подвійною точністю. Отже, розмір кожного параметра ключа – 4 байти, а всього ключа – 12 байтів. У загальному випадку можна задавати у ключ ще одне ціле значення (1 байт), яке визначає тип *Ateb*-функцій. Тоді ключ запишемо у вигляді:

$$\langle n, m, h, t\rangle, \tag{5}$$

де n, m – параметри довільної періодичної Ateb-функції, h – з формули (4), t, $t = 1, ..., 6$ – визначає тип *Ateb*-функції: 1 – *Ateb*-синус; 2 – *Ateb*-косинус; 3 – *Ateb*-тангенс; 4 – *Ateb*-котангенс; 5 – *Ateb*-секанс; 6 – *Ateb*-косеканс [3]. Ключ у вигляді (5) займає всього 13 байтів. Можна залишити ключ у вигляді (4), але змінювати тип функцій Ateb-синуса, Ateb-косинуса і т.д. за домовленістю.

На рис. 1 подано алгоритм методу шифрування, який описаний вище та реалізований у програмному забезпеченні. Для дешифрування необхідно передати ключ $\langle n,\ m,\ h\rangle$, який є комбінацією трьох раціональних чисел. Для того, щоб підвищити надійність передавання ключа, розроблено алгоритм та програму приховання ключа у деякий файл.

Приховування виконується окремо із кожним параметром ключа. Нехай для прикладу $n = 0,68943$. Розглянемо випадок, коли параметр не перевищує 1 та має п’ять знаків після коми. Проте у загальному випадку він може бути довільним раціональним числом.

1. Виділяємо ціле значення:

$$0,68943 \to 68943.$$

2. Перетворюємо отримане число у двійково-десятковий код:

$$68943_{10} \to 0110\ \ 1000\ \ 1001\ \ 0100\ \ 0011_{2-10}.$$

3. Кожен біт із вищеподаного перетворення заносимо першою наймолодшою позицією кожного байта, що зчитується за певним принципом. Можна вибирати варіанти з кінця, парний, непарний, кожен *n*-й і т.д. з файла, у який приховуємо ключ. Такий спосіб приховування ключа дає змогу ускладнити його виокремлення статистичними методами.

Щоб отримати прихований ключ відповідно до вибраного принципу зберігання ключа, що описано у пункті 3, зчитуються потрібні байти, виділяються з них молодші біти накладанням маски, формуються з отриманих значень двійково-десяткові коди і здійснюються перетворення, зворотні до описаних вище пунктів 2 та 1. На рис. 2 показано файл зображення перед і після приховування ключа. Як видно з рисунків, вони однакові.

а *б*

Рис. 2. Зображення перед і після приховування ключа:
а – перед; б – після приховування ключа

Дешифрування відбувається аналогічно до алгоритму шифрування. Відповідно до ключа програма генерує значення *Ateb*-синуса, виділяє з нього ціле значення, здійснює операцію побітового додавання за модулем 2 “XOR” та відновлює початкову інформацію.

Опишемо програмну реалізацію розробленого методу шифрування. На основі описаного методу створено ужиток, що виконує операції шифрування та дешифрування довільного вхідного потоку. Програма реалізована в середовищі Borland C++ Builder 6.0 мовою C++. На рис. 3 показано інтерфейс програми. Для початку роботи треба вказати шлях до джерела (*From*), шлях до вихідного файла (*To*) та шлях до ключа (*KeyFile*). Для виконання шифрування необхідно вибрати опцію *Crypt File*, а для розшифрування *UnCrypt File*. У полі *Input* виводяться дані з файла до шифрування, а у *Output* – після шифрування.

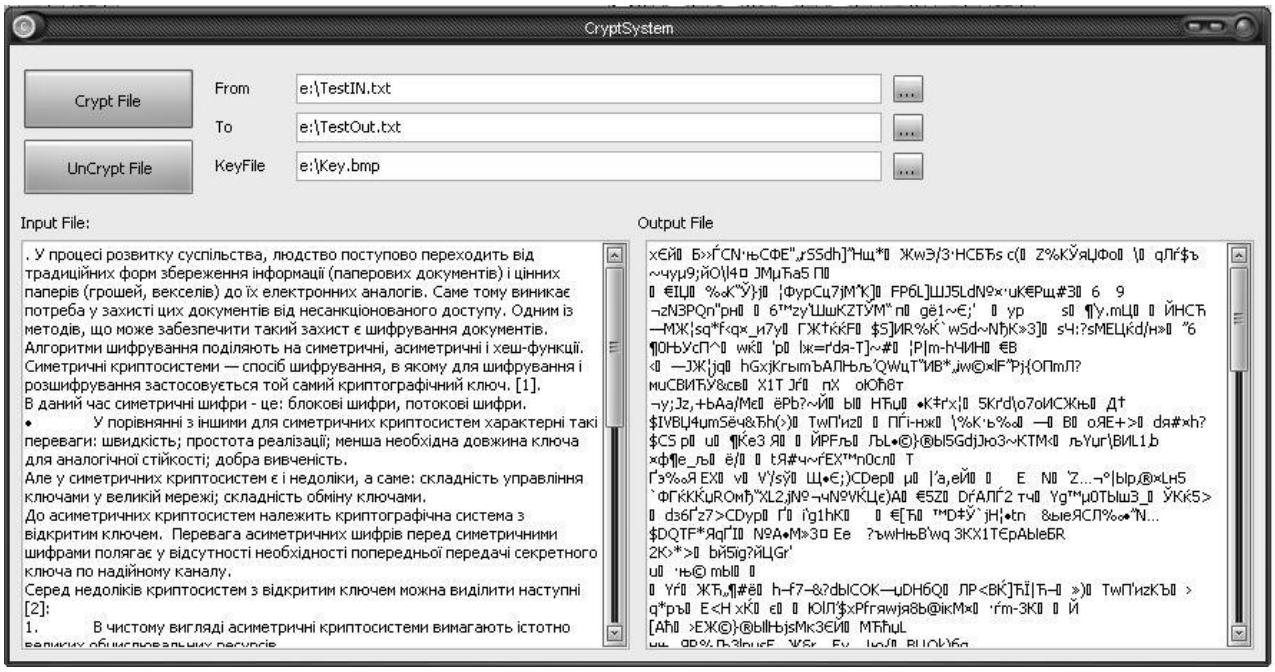

Рис. 3. Інтерфейс програми шифрування

Для того, щоб визначити ефективність алгоритму шифрування, було виконане тестування, результати якого показані у табл. 2. Швидкість шифрування тестували на комп'ютері з операційною системою Windows XP, процесором Pentium 4 з тактовою частотою 3.0 ГГц та оперативною пам'яттю 1 Гб. Як видно з табл. 2, час шифрування (дешифрування) файла виражається сумою часу генерації послідовності *Ateb*-функції та виконання власне самого шифрування (дешифрування). Шифрування проходить дуже швидко, у режимі реального часу, час шифрування збільшується пропорційно до розміру шифрованого файла. Зменшити час роботи програми шифрування для великих файлів можна, зменшивши час генерації послідовності *Ateb*-функції, використовуючи попередньо згенеровані значення.

Таблиця 2

Тестування швидкості шифрування / дешифрування

Розмір файла, байтів	Кількість обчислених значень *Ateb* -функції	Шифрування		Дешифрування	
		Час обчислення *Ateb*-послідовності, мс	Час шифрування файла, мс	Час обчислення *Ateb*-послідовності, мс	Час дешифрування файла, мс
1936461	1306	29594	3766	29610	3781
1936461	541	11860	3500	11860	3515
1936461	2402	52641	3516	52656	3516
15491688	342	7734	30985	7906	30109
15491688	1720	38953	29985	39125	29875
15491688	3296	74563	30578	74625	29609

Оскільки математичний апарат *Ateb*-функцій є досить чутливим до зміни параметрів, то мала зміна ключа приводить до генерації абсолютно іншого шифрованого файла. Ефективність запропонованого методу шифрування визначається невеликим розміром ключа: 12–13 байтів та високою швидкістю роботи.

3. Висновки

Розроблено новий метод шифрування інформації з використанням періодичних *Ateb*-функцій, який належить до симетричних криптосистем. Для розв'язання практично важливої задачі шифрування інформації запропоновано використати періодичні *Ateb*-функції. З цією метою розроблено методи моделювання *Ateb*-функцій залежно від параметрів на основі розкладів у ряди Тейлора та Фур'є. Для моделювання використано методи наближених обчислень. На цій основі розроблено відповідне програмне забезпечення. Представлено інтерфейс ужитку, приклади роботи програми проілюстровано за допомогою графіків. Оцінено похибки обчислень періодичних *Ateb*-функцій та доведено, що обидва методи є ефективними.

Застосування *Ateb*-функцій дає змогу використовувати для шифрування прості операції перетворення інформації (XOR), зберігаючи ефективність вихідного шифру. Щоб збільшити надійність передавання ключа, розроблено алгоритм приховання ключа у файлі з зображенням. Усі алгоритми та методи реалізовано у відповідному програмному забезпеченні. Основними перевагами запропонованого методу шифрування є невеликий розмір ключа та висока швидкість шифрування та дешифрування інформації.

1. Вербицький О.В. Введення в криптологію. – Львів: Наук.-техн. літ.,1998. – 248 с. 2. Саломаа А. Криптография с открытым ключом. – М.: Мир, 1995. – 320 с. 3. Сеник П.М., Возний А.М. Про табулювання періодичної Ateb-функції // Доповіді АН УССР. Сер. А, 1969, № 12. – С. 1089–1092. 4. Фельдман Л. П., Петренко А. І., Дмитрієва О. А. Чисельні методи в інформатиці. – К.: Видавнича група BHV, 2006. – 480 с. 5.Фихтенгольц Г. М. Курс дифференциального и интегрального исчисления. В 3 т. Т. 3. – 8-е изд. – М.: Физматлит, 2003. – 680 с.