DOI 10.15276/imms.v15.no2.196
УДК 004.056.55

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 2, pp. 196-204

МЕТОД АФІННОГО ШИФРУВАННЯ НА ОСНОВІ КВАДРАТИЧНОЇ ФУНКЦІЇ

М.М. Касянчук[1], М.П. Голембйовський[2]

Західноукраїнський національний університет
11, Львівська вул., м. Тернопіль, 46009, Україна
Emails: kasyanchuk@ukr.net[1], mykhailo.2097@gmail.com[2]

Афінні шифри виникли ще в античні часи. Однак незважаючи на затвердження сучасних криптографічних стандартів, вони і на даний час зберігають певну актуальність у криптографії. Ці алгоритми можуть бути корисні, наприклад, при вивченні основ захисту інформації, для демонстрації принципів роботи шифрів заміни або при вивченні історії криптографії. Найбільш ефективними такі перетворення є у випадках, коли критичним параметром виступає час шифрування та передачі інформації. Афінні шифри ґрунтуються на лінійних математичних перетвореннях, які є вразливими до теперішніх криптоаналітичних атак. Тому метою даної роботи є розробка афінного шифру, в основі якого лежать квадратичні функції, усунення неоднозначності, яка виникає при розшифровуванні, та підвищення стійкості розробленого шифру до частотного аналізу за рахунок використання біграм. У роботі показано, що використання не лінійної, а квадратичної функції криптографічного перетворення дозволяє збільшити кількість варіантів ключа і, відповідно, криптографічну стійкість запропонованого алгоритму. Визначено умови, яким повинні відповідати коефіцієнти квадратного рівняння та значення модуля. Наведено покрокові шифруючі перетворення усіх символів розширеного українського алфавіту, формулу для розшифрування, а також відповідний приклад. Розроблено метод однозначного розшифровування квадратичних афінних шифрів за рахунок подвійної нумерації символів алфавіту. Це вдвічі збільшує значення модуля, однак дозволяє вибрати діапазон числових кодів, на яких квадратичні лишки будуть визначатися однозначно. Розроблено біграмний афінний шифр, який не піддається частотному аналізу одного символу алфавіту. Це підвищує криптостійкість методу, хоча збільшуються операнди, над якими виконуються арифметичні операції. Наведено приклад біграмного лінійного та квадратичного афінних шифрів.

Ключові слова: афінний шифр, лінійні перетворення, квадратична функція, криптографічні ключі, числові коди букв, біграмний шифр.

Вступ. Афінні шифри є одними з класичних методів симетричного шифрування [1, 2], які виникли ще в античні часи і використовувалися для захисту інформації [3]. Вони базуються на лінійних математичних перетвореннях над символами алфавіту [4, 5]. Їх використання навіть в епоху сучасних криптографічних стандартів має певну актуальність у криптографії [6, 7]. Афінні шифри можуть бути корисними в певних контекстах, попри свою слабкість порівняно з сучасними криптографічними методами [8, 9]. Зокрема, їх доцільно використовувати в навчальних курсах з криптографії для пояснення принципів роботи шифрів заміни і лінійних перетворень або при вивченні історичних аспектів криптографії.

До переваг афінних шифрів можна віднести простоту реалізації, швидкодію та лінійність математичних перетворень. Однак якщо зловмисник має достатньо зашифрованих повідомлень або хоча б одне зашифроване повідомлення і його відкритий текст, то цього може бути достатньо для розкриття ключа. Через лінійність шифру навіть частина зашифрованого тексту дозволяє зловмиснику встановити математичні зв’язки та відновити оригінальний текст. Оскільки афінний шифр є детермінованим і лінійним, то він не приховує статистичних властивостей тексту. Тому зловмисники можуть використати частотний аналіз для виявлення закономірностей та знаходження відповідностей у зашифрованому та відкритому текстах. Крім того, вимога взаємної

простоти елементів ключа та кількості букв в алфавіті значно обмежує кількість можливих варіантів ключів. Наприклад, для англійського алфавіту з 26-ти символів кількість допустимих взаємно простих чисел становить всього 12. Для зловмисника це робить досить реальною можливість перебору ключів навіть при невеликих за обсягом зашифрованих повідомленнях.

Отже, афінний шифр є вразливим до сучасних криптографічних атак, таких як атака методом грубої сили, атака за допомогою відомого відкритого тексту, атаки на основі математичних властивостей тощо. Афінний шифр є малоефективним при великих обсягах даних, тому його можна вважати безпечним тільки для досить обмежених ситуацій, в яких критичним параметром є час шифрування та передачі інформації.

Огляд літератури. Незважаючи на вказані недоліки, певна модифікація афінних шифрів (приховування кількості букв в алфавіті), їх поєднання з іншими криптографічними алгоритмами або деякими математичними перетвореннями (зокрема, використання системи залишкових класів [10, 11]) дозволяє підвищити стійкість зашифрованого повідомлення до криптоаналізу [12, 13].

Наприклад, для покращення захищеності баз даних в [14] після шифру Цезаря було запропоновано використовувати афінний шифр. Зашифрований текст зберігався у розділеному на поля текстовому файлі, що збільшувало його рівень безпеки.

У [15] розглядається алгоритм шифрування зображень, що базується на афінному шифрі. Спочатку шифруються позиції пікселів, потім афінний шифр використовується для розсіювання та заплутування зашифрованих значень. Такий підхід забезпечує кращу безпеку шифрування, а також високий рівень дифузії та заплутаності.

У [16] застосовано концепцію теорії афінних груп для захисту цифрових зображень на основі алгоритму DES і вейвлет-перетворень з використанням операцій множення матриць та векторного додавання.

Дослідження [17] описує метод, де спочатку використовується афінний шифр, а потім - шифр транспозиції. Це робить криптоаналіз більш складним завдяки використанню різних типів ключів та різній кількості символів у відкритому та зашифрованому текстах.

У [18] пропонується гібридна схема, що поєднує асиметричний криптоалгоритм Рабіна та симетричний афінний шифр. Афінне перетворення використовується для шифрування повідомлень, а система Рабіна — для шифрування та розшифрування ключів.

У [19] представлено варіант афінного шифру з використанням асиметричних ключів, які формуються з прямокутних матриць. Це рішення покращує криптостійкість запропонованого алгоритму шифрування.

В [20] описано можливість поєднання афінного шифру з генератором псевдовипадкових чисел Blum Blum Shub. Це дозволяє генерувати випадкові потоки ключів, що підвищує непередбачуваність зашифрованого тексту та збільшує криптостійкість системи.

Мета роботи. Метою даної роботи є розробка квадратичного афінного шифру, усунення неоднозначності при розшифровуванні та підвищення стійкості розробленого шифру до частотного аналізу за рахунок використання біграм. Для досягнення поставленої мети потрібно вирішити такі завдання:

- аналіз класичного афінного шифру, виявлення його переваг та недоліків, визначення необхідних арифметичних операцій, встановлення правил числового кодування тексту;

- розробка квадратичного афінного шифру, встановлення вимог до ключів шифрування/розшифрування, побудова таблиці з квадратичними криптографічними перетвореннями для розширеного українського алфавіту;

- розробка методу однозначного розшифровування для квадратичних афінних шифрів;

- розробка методу біграмного лінійного та квадратичного афінного шифрування.

Класичний афінний шифр. Класичне афінне шифрування полягає у лінійному перетворенні числового коду кожної букви у тексті. Це є частковий випадок для більш загального моноалфавітного шифру заміни і тому афінному шифру властиві усі вразливості даного класу шифрів. Зокрема, він може легко піддаватися частотному криптоаналізу, тобто володіє порівняно невеликою криптографічною стійкістю.

Найпростішим способом числового кодування тексту є заміна кожної букви її номером в алфавіті. В результаті отримається ряд 0, 1, 2, …, n-1, де n – кількість букв в алфавіті. Не враховуючи великих та малих символів та пробілів, відповідність між буквами українського алфавіту та їх числовими значеннями можна представити таблицею 1.

Таблиця 1.

Відповідність між буквами українського алфавіту та числами

Буква	а	б	в	г	ґ	д	е	є	ж	з	и
Номер	00	01	02	03	04	05	06	07	08	09	10
Буква	і	ї	й	к	л	м	н	о	п	р	с
Номер	11	12	13	14	15	16	17	18	19	20	21
Буква	т	у	ф	х	ц	ч	ш	щ	ь	ю	я
Номер	22	23	24	25	26	27	28	29	30	31	32

Далі, згідно властивостей модульної арифметики, відбувається шифруюче лінійне перетворення кожного числа, яке відповідає символу відкритого тексту, за такою формулою:

$$X=(a\cdot x+s) \bmod n, \quad (1)$$

де x і X – номери букв відкритого та зашифрованого тексту відповідно; пара a ключі шифру, для яких повинні виконуватися умови: $1\le a\le n$-1, НСД (a, n)=1, $0\le s\le n$-1.

Для розшифровування використовується аналогічне перетворення:

$$x=(A\cdot X+S) \bmod n, \quad (2)$$

де $A=a^{-1} \bmod n$ – обернений елемент до числа a за взаємнопростим модулем n; $S=(-As) \bmod n$.

В таблиці 2, згідно виразів (1)-(2), наведено приклад криптографічних перетворень повідомлення «бот» (01 18 22 згідно таблиці 1) з ключем шифрування a=13, s=9. Відповідно, ключ для розшифровування $A=13^{-1} \bmod 33=28$, $S=(-28\cdot 9) \bmod 33=(5\cdot 9) \bmod 33=12$.

Таблиця 2.

Приклад криптографічних перетворень за допомогою афінних шифрів

Зашифрування				Розшифрування			
Повідомлення	б	о	т	Шифртекст	т	ї	ю
x	01	18	22	X	22	12	31
$13\cdot x+9$	22	243	295	$28\cdot x+12$	628	348	880
$X=(13\cdot x+9) \bmod 33$	22	12	31	$x=(28\cdot x+12) \bmod 33$	01	18	22
Шифртекст	т	ї	ю	Повідомлення	б	о	т

Якщо a=1, то афінний шифр трансформується у шифр зсуву (або шифр Цезаря) і процеси шифрування та розшифровування зводяться до простого лінійного зсуву:

$$X=(x+s) \bmod n,\ x=(X+S) \bmod n, \quad (3)$$

де $S=(-s) \bmod n=n-s$.

Якщо $a\neq 1$ і s=0, то шифрування та розшифровування здійснюються тільки за допомогою операції множення:

$$X=(ax) \bmod n,\ x=(AX) \bmod n, \tag{4}$$

Якщо зловмиснику відома потужність алфавіту n, то швидкий криптоаналіз можливий навіть прямим перебором всіх можливих варіантів. Наприклад, для українського алфавіту n=33, параметр a можна вибрати 20-ма способами (функція Ейлера $\phi(33)=20$), параметр – 33-ма способами. Тобто для успішного криптоаналізу лінійного афінного шифру потрібно розглянути всього 660 варіантів ключа, причому обчислення будуть виконуватися над порівняно невеликими операндами. Крім того, оскільки однаковим буквам відкритого повідомлення відповідають однакові букви шифртексту, то афінні шифри вразливі і до частотного аналізу.

Квадратичні криптографічні перетворення. Збільшити кількість варіантів ключа дозволяє використання не лінійної, а квадратичної функції криптографічного перетворення:

$$X=\left(b\cdot x^2+c\cdot x+d\right)\bmod n=\left(b\cdot\left(\left(x+\frac{c}{2\cdot b}\right)^2+\frac{d}{b}-\frac{c^2}{4\cdot b^2}\right)\right)\bmod n, \tag{5}$$

де b, c, d – коефіцієнти квадратичної функції, які повинні бути менші за n.

Після перетворення $X=\left(b\cdot\left(\left(x+\left(c\cdot\left((2\cdot b)^{-1}\bmod n\right)\right)\bmod n\right)^2+\right.\right.$ $\left.\left.+\left(d\cdot\left(b^{-1}\right)\bmod n-c^2\cdot\left((2\cdot b)^{-2}\right)\bmod n\right)\bmod n\right)\right)\bmod n$ вираз (5) доцільно переписати у такому вигляді:

$$X=\left(b\cdot\left((x+f)^2+g\right)\right)\bmod n, \tag{6}$$

де $f=\left(c\cdot\left((2\cdot b)^{-1}\bmod n\right)\right)\bmod n;\ g=\left(d\cdot\left(b^{-1}\right)\bmod n-c^2\cdot\left((2\cdot b)^{-2}\right)\bmod n\right)\bmod n$.

Звідси випливає, що параметри b і $2b$, для яких потрібно шукати обернені елементи за модулем n, повинні бути взаємно прості з кількістю букв в алфавіті. Для автоматичного виконання таких умов доцільно потужність алфавіту розширити до деякого простого числа. В цьому випадку половина елементів зведеної системи лишків будуть квадратичними лишками.

Розшифрування повинно відбуватися в зворотному порядку і передбачає обчислення кореня квадратного за модулем, методи пошуку якого описані, наприклад, в [21, 22]. Отже, з формули (6) можна отримати:

$$x=\left(\sqrt{b^{-1}X-g}-f\right)\bmod n, \tag{7}$$

Запропоноване квадратичне перетворення ускладнює криптоаналіз в порівнянні з лінійним афінним шифром, особливо, якщо зловмиснику невідома потужність алфавіту, однак не усуває вразливості до частотного аналізу. Крім того, розв'язок квадратного рівняння або пошук квадратного кореня приводить до неоднозначності при розшифруванні

Для прикладу розглянемо функцію шифрування:

$$X=(3x^2+7x+11) \bmod 37. \tag{8}$$

Тут український алфавіт розширений з 33 до 37 символів додаванням, наприклад, крапки (.) - номер 33, коми (,) – номер 34, пробілу ( ) – номер 35 та знаку оклику (!) – номер 36.

Згідно формули (6) b=3, інші параметри шукаються таким чином:

$$f=\left(\frac{c}{2b}\right)\bmod 37=\frac{7}{6}\bmod 37=(7\cdot 31)\bmod 37=32\bmod 37=-5\bmod 37;$$

$$g=\left(\frac{d}{b}-\left(\frac{c}{2b}\right)^2\right)\bmod 37=\left(\frac{11}{3}-\left(\frac{7}{6}\right)^2\right)\bmod 37=\left(11\cdot 25-(7\cdot 31)^2\right)\bmod 37=$$

$$=28\bmod 37=-9\bmod 37.$$

Тоді з виразу (8) отримується:

$$X=\left(3\cdot\left((x-5)^2-9\right)\right)\bmod 37. \tag{9}$$

В таблиці 3 наведено приклади покрокових шифруючих перетворень усіх символів алфавіту потужністю 37.

Таблиця 3

Квадратичні афінні перетворення над символами розширеного українського алфавіту

x	00	01	02	03	04	05	06	07	08	09	10	11	12
$x^2 \bmod 37$	0	1	4	9	16	25	36	12	27	7	26	10	33
$(x\text{-}5)^2 \bmod 37$	25	16	9	4	1	0	1	4	9	16	25	36	12
$((x\text{-}5)^2\text{-}9) \bmod 37$	16	7	0	32	29	28	29	32	0	7	16	27	3
$3\cdot((x\text{-}5)^2\text{-}9) \bmod 37$	11	21	0	22	13	10	13	22	0	21	11	7	9
x	13	14	15	16	17	18	19	20	21	22	23	24	25
$x^2 \bmod 37$	21	11	3	34	30	28	28	30	34	3	11	21	33
$(x\text{-}5)^2 \bmod 37$	27	7	26	10	33	21	11	3	34	30	28	28	30
$((x\text{-}5)^2\text{-}9) \bmod 37$	18	35	17	1	24	12	2	31	25	21	19	19	21
$3\cdot((x\text{-}5)^2\text{-}9) \bmod 37$	17	31	14	3	35	36	6	19	1	26	20	20	26
x	26	27	28	29	30	31	32	33	34	35	36		
$x^2 \bmod 37$	10	26	7	27	12	36	25	16	9	4	1		
$(x\text{-}5)^2 \bmod 37$	34	3	11	21	33	10	26	7	27	12	36		
$((x\text{-}5)^2\text{-}9) \bmod 37$	25	31	2	12	24	1	17	35	18	3	27		
$3\cdot((x\text{-}5)^2\text{-}9) \bmod 37$	1	19	6	36	35	3	14	31	17	9	7		

Для прикладу, слово «вежа», яке має числовий код (02 06 08 00), перетвориться у шифртекст (00 13 00 11) або «айаі» згідно таблиці 1. Букви «в» і «ж» шифруються однаковим символом «а». Це якраз і пов'язується з тим, що квадратне рівняння має два розв'язки і результат розшифрування згідно формули (7) буде неоднозначний. Зокрема, враховуючи, що $3^{-1} \bmod 37=25$, хід розшифрування буде такий:

1) $\left(\sqrt{3^{-1}\cdot 0+9}+5\right)\bmod 37=(\pm 3+5)\bmod 37=2$ і 8, що відповідає буквам «в» і «ж»;

2) $\left(\sqrt{3^{-1}\cdot 13+9}+5\right)\bmod 37=\left(\sqrt{25\cdot 13+9}+5\right)\bmod 37=(\pm 1+5)\bmod 37=4$ і 6, що відповідає буквам «ґ» і «е»;

3) $\left(\sqrt{3^{-1}\cdot 11+9}+5\right)\bmod 37=\left(\sqrt{25\cdot 11+9}+5\right)\bmod 37=(\pm 5+5)\bmod 37=0$ і 10, що відповідає буквам «а» і «и».

Метод однозначного розшифровування квадратичних афінних шифрів. Зрозуміло, що неоднозначність при розшифровуванні є суттєвим недоліком квадратичних афінних шифрів, оскільки потрібно розглядати 2^k варіантів, де k – кількість букв у повідомленні. Усунути його дозволяють властивості таблиці 3. Видно, що при використанні функції $X=x^2 \bmod n$ результати шифрування симетричні відносно параметра $\frac{n}{2}$. Для функції $X=(x+f)^2 \bmod n$ усі значення X циклічно зсуваються на величину f. Зсув відбувається ліворуч при $f>0$ і праворуч при $f<0$. При використанні двох інших функцій відбувається зміна результату шифрування в залежності від параметрів g і b. Це означає, що при $f<0$ на ділянці від $x=f$ до $x=\frac{n-1}{2}+f$, а при $f>0$ – від $x=\frac{n-1}{2}-f$ до $x=n-f$ квадратичні лишки повторюватися не будуть. Тому якщо букви відкритого тексту вибирати на цій ділянці, то результат розшифрування буде однозначний. Щоб охопити весь алфавіт його символи потрібно пронумерувати двічі, кількість символів доцільно вибрати так, щоб число $2n$-1, яке визначає потужність алфавіту, було простим.

В таблиці 4 наведено фрагмент алфавіту потужністю 19 з перших 10-ти букв з функцією шифрування $X=(x^2+6x+7) \bmod 19=((x+3)^2\text{-}2) \bmod 19$. Для шифрування і

розшифровування вибирається діапазон від x=07 (буква «є») до x=16 (буква «е»). Шифртекст слова «вежа» - (12 16 08 10) буде «ґєдд» - (14 17 05 15).

Враховуючи, що b=1, процедура розшифрування матиме такий вигляд:

1) $\left(\sqrt{14+2}-3\right)\text{mod}19=(\pm4-3)\,\text{mod}19=1$ і 12;

2) $\left(\sqrt{17+2}-3\right)\text{mod}19=(0-3)\,\text{mod}19=16$;

3) $\left(\sqrt{5+2}-3\right)\text{mod}19=(\pm8-3)\,\text{mod}19=5$ і 8;

4) $\left(\sqrt{15+2}-3\right)\text{mod}19=(\pm6-3)\,\text{mod}19=3$ і 10.

Вибравши числа з діапазону від 7 до 16, можна однозначно отримати розшифрований числовий код (12 16 08 10), що відповідає слову «вежа».

Таблиця 4

Однозначне розшифрування для фрагменту алфавіту

Буква	а	б	в	г	ґ	д	е	є	ж	з
x	00	01	02	03	04	05	06	07	08	09
x^2mod 19	0	1	4	9	16	6	17	11	7	5
$((x+3)^2-2)$mod 19	7	14	4	15	9	5	3	3	5	9
Буква	а	б	в	г	ґ	д	е	є	ж	з
x	10	11	12	13	14	15	16	17	18	19
x^2mod 19	5	7	11	17	6	16	9	4	1	0
$((x+3)^2-2)$mod 19	15	4	14	7	2	18	17	18	2	7

Біграмний афінний шифр. Усі розглянуті вище афінні шифри вразливі до частотного аналізу, оскільки тим самим буквам відкритого тексту відповідають однакові букви зашифрованого. Усунути цей недолік дозволяє використання шифрів складної заміни, зокрема біграмних, в яких блоком шифрування виступають пари букв – біграми. У відкритому повідомленні кількість символів має бути парною (непарну кількість можна доповнити крапкою). Модуль криптографічного перетворення, згідно розширеної таблиці 1, повинен перевищувати 3236 (повідомлення «я!») і бажано, щоб був простим числом. Передача зашифрованого повідомлення буде здійснюватися в числовому коді.

Нехай потрібно зашифрувати розбите на біграми повідомлення «шифри.» з числовим кодом (2810 2420 1033). Для прикладу у лінійному випадку вибираємо такі ключі шифрування: a=31, s=1590, n=3701. Відповідно формула шифрування: $X=(31\cdot x+1590)$ mod 3701. Обчисливши ключі для розшифрування $A=31^{-1}$ mod 3701=2149, $S=(-2149\cdot1590)$ mod 3701=2814, можна отримати формулу для розшифрування: $x=(2149\cdot X+2814)$ mod 3701. Для квадратичного шифрування можна вибрати розглянуте вище рівняння з модулем n=3701: $X=(x^2+6x+7)\text{mod }3701=((x+3)^2-2)\text{mod }3701$. Розшифрування відбувається за допомогою формули $x_{1,2}=\left(\pm\sqrt{X+2}-3\right)\text{mod }3701$.

У таблиці 5 наведено результати шифрування і розшифровування біграмним лінійним та квадратичним афінними шифрами.

Таблиця 5.

Результати шифрування і розшифровування біграмним лінійним та квадратичним афінними шифрами

Зашифрування				Розшифрування			
Повідомлення	ши	фр	и.	Лінійний афінний шифр			
x	2810	2420	1033	X	3577	2590	304
Лінійний афінний шифр				$2149\cdot X+2814$	7689787	5568724	656110
$31\cdot x+1590$	88700	76610	33613	x	2810	2420	1033
X	3577	2590	304	Повідомлення	ши	фр	и.
Квадратичний афінний шифр				Квадратичний афінний шифр			

Зашифрування				Розшифрування			
x^2+6x+7	7912967	5870927	1073294	X	229	1141	4
X	229	1141	4	$x_{1,2}$	885, 2810	1275, 2420	1033, 2662
				Повідомлення	2810, ши	2420, фр	1033, и.

З таблиці 5 видно, що букві «и», яка два рази міститься у відкритому повідомленні, у шифртексті відповідають зовсім різні числові коди. Тому частотний аналіз по одній букві в даному випадку непридатний, що підвищує криптостійкість методу. Однак збільшуються операнди, над якими виконуються арифметичні операції.

Крім того, для квадратичного шифру знову виникає проблема неоднозначності. Вибір букв у певному діапазоні, як було показано на прикладі таблиці 4, в цьому випадку непридатний. Однак, згідно таблиці 1, для розв'язків (8 85), (12 75), (26 62) не існує відповідної букви, що значно спрощує пошук правильного розв'язку.

Висновки. Дана робота присвячена розробці афінного шифру, в основі якого лежить використання не лінійної, а квадратичної функції криптографічного перетворення. Це дозволяє збільшити кількість варіантів ключа і, відповідно, криптографічну стійкість запропонованого методу. Визначено умови, яким повинні відповідати коефіцієнти квадратного рівняння та значення модуля. Наведено покрокові шифруючі перетворення усіх символів розширеного українського алфавіту, формулу для розшифрування, а також відповідний приклад. Розроблено метод однозначного розшифровування квадратичних афінних шифрів за рахунок подвійної нумерації символів алфавіту. Це вдвічі збільшує значення модуля, однак дозволяє вибрати діапазон числових кодів, на яких квадратичні лишки будуть визначатися однозначно. Розроблено біграмний афінний шифр, який не піддається частотному аналізу одного символу алфавіту. Це підвищує криптостійкість методу, хоча збільшуються операнди, над якими виконуються арифметичні операції. Наведено приклад біграмного лінійного та квадратичного афінних шифрів.

Список літератури

1. Корченко О.Г., Сіденко В.П., Дрейс Ю.О. Прикладна криптологія: системи шифрування: підручник. К.: ДУТ, 2014. 448 с.
2. Глинчук Л.Я. Криптологія: навч.-метод. посіб. Луцьк: Вежа-Друк, 2014. 164 с.
3. Гребенніков В.В. Історія криптології та секретного зв'язку. К.: КНТ, 2023. 800 с.
4. Кожухівський А.Д., Горбенко І.Д., Гайдур Г.І., Кожухівська О.А., Марченко В.В. Математичні методи криптології. К.: ДУТ, 2021. 244 с.
5. Гапак О.М., Балога С.І. Захист інформації в комп'ютерних системах: підручник. Ужгород: УжНУ, 2021. 184 с.
6. Красиленко В.Г., Грабовляк С.К. Матричні афінні шифри для створення цифрових сліпих підписів на текстографічні документи. *Системи обробки інформації*. Х.: ХУПС, 2011. Вип. 7(97). С. 60 – 63.
7. Красиленко В.Г., Нікітович Д.В. Удосконалення та моделювання матричних афінних шифрів для криптографічних перетворень зображень. *Електроніка та інформаційні технології*: збірник наукових праць. Львів: Львівський національний університет імені Івана Франка, 2017. Вип. 7. С. 20-42.
8. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. Житомир: Державний університет «Житомирська політехніка», 2021. 120 с.
9. Гапак О.М. Криптоаналіз. Криптографічні протоколи: навчальний посібник. Ужгород: УжНУ, 2021. 93 с.
10. Касянчук М.М. Теорія та математичні закономірності досконалої форми системи залишкових класів. *Питання оптимізації обчислень* (*ПОО–XXXV*): Праці Міжнародного симпозіуму. Київ–Кацивелі. 2009. Т.1. С. 306–310.
11. Kasianchuk M. Conception of theoretical bases of the accomplished form of Krestenson's transformation and its practical application. *Advanced Computer Systems and Network: Design*

and Application (*ACSN–2009*): Proceedings of the 4–th International Conference. L'viv. 2009. P.299–301.
12. Kasianchuk M., Yakymenko I., Nykolaychuk Y.M. Symmetric cryptoalgorithms in the residue number system. *Cybernetics and Systems Analysis*. Vol.57(2), 2021. P.329–336.
13. Nykolaychuk Y., Yakymenko I., Vozna Y., Kasianchuk M. Residue number system asymmetric cryptoalgorithms. *Cybernetics and Systems Analysis*. Vol.58(4), 2022. P.611–618.
14. Hammood D.A., Maitham A. Implementation and Enhancement Affine Cipher of Database. *Journal of Engineering and Sustainable Development.* Vol.20, 2016. P.264–276.
15. Ke Q., Liao Q.-N., Li A.-Q., Gao R. Digital Image Encryption Algorithm Based on Affine Cipher. In *Advances in Intelligent Systems and Computing*; Springer International Publishing: Cham, 2019. P. 578–585.
16. Soekarta R., Sigit M. Implementation of Affine Group Algebra on Digital Image Security. *Mob. Forensics*. Vol.4, 2023. P. 137–146.
17. Alhassan M.J., Hassan A., Sani S., Alhassan Y. A Combine Technique of an Affine Cipher and Transposition Cipher. *Journal of Research in Applied Mathematics*, Vol. 7, 2021. P. 8–12.
18. Budiman M.A., Handrizal H., Azzahra S. An Implementation of Rabin-p Cryptosystem and Affine Cipher in a Hybrid Scheme to Secure Text. *J. Phys. Conf. Ser.* Vol. 1898, 2021. P. 012042.
19. Maxrizal M., Aniska Prayanti B.D. Application of Rectangular Matrices: Affine Cipher Using Asymmetric Keys. *CAUCHY – Jurnal Matematika Murni dan Aplikasi*. Vol. 5(4), 2019. P. 181–185.
20. Shoup V. A Computational Introduction to Number Theory and Algebra. Cambridge University Press: Cambridge, England. 2009. 578 p.
21. Yakymenko I., Kasianchuk M., Shylinska I., Shevchuk R., Yatskiv V., Karpinski M. Polynomial Rabin Cryptosystem Based on the Operation of Addition. Proceedings of the 12th International Conference "Advanced Computer Information Technology (ACIT 2022)" (Ruzomberok, Slovakia), 2022. P. 345–350.
22. Ivasiev S., Kasyanchuk M., Yakymenko I., Gomotiuk O., Shylinska I., Bilovus L. Algorithmic Support for Rabin Cryptosystem Implementation Based on Addition. Proceedings of the 10th International Conference "Advanced Computer Information Technology (ACIT 2020)" (Deggendorf, Germany). 2020. P. 779-782

AFFINE ENCRYPTION TECHNIQUE BASED ON QUADRATIC FUNCTION

M.M. Kasianchuk[1], M.P. Holembiovskyi[2]

West Ukrainian National University
11, Lvivska Str., Ternopil, 46009, Ukraine
Emails: kasyanchuk@ukr.net[1], mykhailo.2097@gmail.com[2]

Affine ciphers originated in ancient times. However, despite the advent of modern cryptographic standards, they are still relevant in cryptography. These algorithms can be useful, for example, when teaching the fundamentals of data protection, demonstrating the principles of substitution ciphers, or studying the history of cryptography. Such transformations are particularly effective in cases where encryption and data transmission speed is a critical parameter. Affine ciphers are based on linear mathematical transformations that are vulnerable to current cryptanalytic attacks. Therefore, the purpose of this work is to develop an affine cipher based on quadratic functions, eliminate the ambiguity that arises during decryption, and increase the resistance of the developed cipher to frequency analysis using bigrams. The study demonstrates that using a quadratic rather than a linear cryptographic transformation function allows increasing the number of possible keys, thereby improving the cryptographic strength of the proposed algorithm. Conditions are defined for the coefficients of the quadratic equation and the modulus values. Step-by-step encryption transformations for all characters of the extended Ukrainian alphabet are given as well as the decryption formula, and an illustrative example. A technique for unambiguous decryption of quadratic affine ciphers is developed based on double numbering of the alphabet symbols. This leads to doubling the modulus value, but allows you to select a range of number codes for which quadratic residues can be uniquely determined. A bigram affine cipher is developed, which is resistant to single-character frequency analysis. This increases the cryptographic strength of the technique, although the operands on which arithmetic operations are performed increase. Examples of linear and quadratic affine cipher bigram are given.

Keywords: affine cipher, linear transformations, quadratic function, cryptographic keys, letter number codes, bigram cipher.