УДК 691.3.06

Informatics and Mathematical Methods in Simulation
Vol. 8 (2018), No. 1, pp. 69-77

УДОСКОНАЛЕННЯ РЕАЛІЗАЦІЇ КРИПТОАЛГОРИТМУ ЕЛЬ-ГАМАЛЯ НА ОСНОВІ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ

І.З. Якименко

Тернопільський національний економічний університет,
вул. Львівська, 11, Тернопіль, 46020, Україна; e-mail: iyakimenko@ukr.net

В даній роботі проведено аналіз систем захисту інформаційних потоків з використанням асиметричних криптоалгоритмів, на основі якого встановлені недоліки існуючих підходів реалізації операцій модулярного експоненціювання при шифруванні/дешифруванні, а саме – використання ключів, блоків шифрування та модуля криптоперетворення до 2048 та 4096 біт, що призводить до зменшення часових характеристик. Встановлено, що одним з перспективних підходів щодо вирішення даного класу задач є використання системи залишкових класів (СЗК), яка володіє рядом переваг в порівнянні з двійковою – здійснення операцій паралельно та зменшення розрядності операндів, які не перевищують розрядності набору обраних модулів СЗК. Вказані недоліки, які стосуються переведення з СЗК в десяткову систему числення, а саме необхідність пошуку оберненого елемента за модулем, тобто базисних чисел. В роботі зазначено, що існують набори модулів, які утворюють досконалу форму СЗК (базисні числа рівні 1) та модифіковану досконалу СЗК (базисні числа рівні ±1), що суттєво зменшує часову складність переведення. Наведені теоретичні основи удосконалення реалізації асиметричного криптоалгоритму Ель-Гамаля на основі сумісного використання СЗК та векторно-модульного алгоритму модулярного множення, що дозволило розпаралелити процес, зменшити часову складність та підвищити ефективність виконання процесу шифрування/дешифрування.

Ключові слова: криптосистема Ель-Гамаля, система залишкових класів, модулярне множення, векторно-модульний метод, обчислювальна складність, обернений елемент за модулем, досконала форма системи залишкових класів, модифікована система числення системи залишкових класів, шифрування, дешифрування

Вступ

На сьогоднішній день для забезпечення високого рівня захисту інформаційних потоків використовують асиметричні криптоалгоритми RSA, Ель-Гамаля [1], Рабіна [2] з параметрами – ключі, блок шифрування та модуль криптоперетворення не менше 1024 біт з перспективою їх зростання в найближчі роки до 2048 та 4096 біт, що призводить до зменшення часових характеристик. При шифруванні/дешифруванні основними операціями зазначених асиметричних алгоритмів є модулярне експоненціювання та піднесення до квадрату за модулем багаторозрядних чисел. Багатьма вченими розроблялися методи модулярного множення та експоненціювання, які мають певні функціональні обмеження, а саме використовують двійково-десяткову систему числення, яка характеризується високою обчислювальною складністю.

Найперспективнішим підходом щодо вирішення даного класу задач є використання системи залишкових класів (СЗК), яка володіє рядом переваг в порівнянні з двійковою – здійснення операцій паралельно та зменшення розрядності операндів, які не перевищують розрядності набору обраних модулів СЗК. Поряд з цим існують певні труднощі при переведенні з СЗК в десяткову систему числення, а саме необхідність пошуку оберненого елемента за модулем, тобто базисних чисел. Слід відмітити, що існують набори модулів, які утворюють досконалу форму СЗК (базисні

числа рівні 1) [3] та модифіковану досконалу СЗК (базисні числа рівні ±1) [4], що суттєво зменшує часову складність переведення.

Метою роботи є підвищення швидкодії та зменшення складності базових операцій асиметричних криптоалгоритмів RSA, Ель-Гамаля на основі сумісного застосування СЗК та алгоритму векторно-модульного множення [5].

Удосконалення реалізації алгоритму шифрування Ель-Гамаля з використанням системи залишкових класів

На першому етапі відбувається генерування ключів, а саме:

1. Вибираються два простих числа p і q, та випадкове ціле число x для якого має місце нерівність: $1 < x < p$.

Обчислюється значення $y = q^x \bmod p$ на основі сумісного використання СЗК і векторно-модульного алгоритму модулярного експоненціювання, тобто згідно формули, що дозволяє розпаралелити процес на l потоків, які відповідають кількості модулів:

$$y = q^x \bmod p = \left(\sum_{i=1}^{l} b_i B_i q_i \right) \bmod p,$$

де $q_i = (q \bmod p_i)^x \bmod p_i$, $p = \prod_{i=1}^{l} p_i$, $B_i = \frac{p}{p_i}$, $b_i = B_i^{-1} \bmod p_i$, l – кількість модулів та потоків.

Пошук значення $q_i = (q \bmod p_i)^x \bmod p_i$ здійснюється на основі використання векторно-модульного методу модулярного множення з використанням представлення $x = \sum_{j=0}^{n-1} x_j \cdot 2^j$, де $x_j = 0,1$ згідно формули обчислити q_i:

$$q_i = (q \bmod p_i)^{\sum_{j=0}^{n-1} x_j \cdot 2^j} \bmod p_i = \prod_{j=1}^{n-1} (q \bmod p_i)^{x_j \cdot 2^j} = \prod_{j=0}^{n-1} s_j \bmod p_i,$$

де $s_i = M^{2^i} \bmod p_i$, при чому $s_i = (s_{i-1})^2 \bmod p_i$. Тоді будь–який степінь x можна записати за степенями 2 і шуканий результат можна отримати, перемноживши відповідну кількість стовбців за допомогою таблиці 1.

Таблиця 1.

Вектор піднесення до степеня в базисі Радемахера–Крестенсона

x_{n-1}		x_i	…	x_1	x_0
s_{n-1}		s_i	…	s_1	s_0
$q^{2^{n-1}} \bmod p_i$	…	$q^{2^i} \bmod p_i$	…	$q^{2^1} \bmod p_i$	$q^{2^0} \bmod p_i$

Для пошуку значення q_i перемножаються ті значення s_i, для яких $x_j = 1$. Основними перевагами такого методу є здійснення операцій над числами значно менших розмірів в порівнянні з класичним підходом, що дозволяє пришвидшити алгоритм модулярного експоненціювання.

При знаходженні значення $s_i s_{i-1} \bmod p_i$ представимо $s_{i-1} = \sum_{k=0}^{n-1} w_k \cdot 2^k$, де $w_k = 0,1$, n – розрядність модуля p_i. На основі використання векторно-модульного методу будуються два вектор-рядки, в першому з яких записуються елементи:

$$h_0 = 2^0 s_i \bmod p_i,\ h_i = 2 \cdot s_{i-1} \bmod p_i,$$

в другому w_i, як показано в таблиці 2.

Таблиця 2.

Представлення вектор-рядків модульного множення

h_{n-1}	…	h_i	…	h_1	h_0
w_{n-1}		w_i	…	w_1	w_0

Результат модулярного множення двох *n*-розрядних чисел знаходиться згідно формули:

$$s_i s_{i-1} \bmod p_i = \left(\sum_{i=0}^{n-1} w_i \cdot h_i \right) \bmod p_i .$$

Розроблений метод характеризується меншою часовою складністю порівняно з класичними. Отже, відкритим ключем виступає (p, q, y), а закритим – x.

2. Шифрування. Вибирається випадкове ціле число k таке, що $1 < k < p-1$. Обчислюється значення $a = q^k \bmod p$. Для цього використовується СЗК та векторно-модульний алгоритм модулярного експоненціювання на основі формули:

$$y = q^k \bmod p = \left(\sum_{i=1}^{l} b_i B_i q_i \right) \bmod p,$$

де $q_i = (q \bmod p_i)^k \bmod p_i$, $p = \prod_{i=1}^{l} p_i$, $B_i = \frac{p}{p_i}$, $b_i = B_i^{-1} \bmod p_i$, l – кількість модулів та потоків.

Пошук значення $q_i = (q \bmod p_i)^k \bmod p_i$ здійснюється на основі використання векторно-модульного методу модулярного множення з використанням представлення $k = \sum_{j=0}^{n-1} k_j \cdot 2^j$, де $k_j = 0,1$ згідно формули обчислити q_i:

$$q_i = (q \bmod p_i)^{\sum_{j=0}^{n-1} k_j \cdot 2^j} \bmod p_i = \prod_{j=1}^{n-1} (q \bmod p_i)^{k_j \cdot 2^j} = \prod_{j=0}^{n-1} y_j \bmod p_i,$$

де $y_i = q^{2^i} \bmod p_i$, при чому $y_i = (y_{i-1})^2 \bmod p_i$. Тоді будь–який степінь k можна записати за степенями 2 і шуканий результат можна отримати, перемноживши відповідну кількість стовбців за допомогою таблиці 3:

Таблиця 3.

Вектор піднесення до степеня в базисі Радемахера–Крестенсона

k_{n-1}		k_i	…	k_1	k_0
y_{n-1}		y_i	…	y_1	y_0
$q^{2^{n-1}} \bmod p_i$	…	$q^{2^i} \bmod p_i$	…	$q^{2^1} \bmod p_i$	$q^{2^0} \bmod p_i$

Для пошуку значення q_i перемножаються ті значення y_i, для яких $k_j = 1$. При знаходженні значення $y_i y_{i-1} \bmod p_i$ представимо $y_{i-1} = \sum_{z=0}^{n-1} a_z \cdot 2^z$, де $a_z = 0,1$, n – розрядність модуля p_i. На основі використання векторно-модульного методу будуються два вектор-рядки, в першому з яких записуються елементи:

$$r_0 = 2^0 y_i \bmod p,\ r_i = 2 \cdot y_{i-1} \bmod p,$$

в другому a_z, як показано в таблиці 4.

Таблиця 4.

Представлення вектор-рядків модульного множення

r_{n-1}	…	r_i	…	r_1	r_0
a_{n-1}		a_i	…	a_1	a_0

Результат модулярного множення двох *n*-розрядних чисел знаходиться згідно формули:

$$y_i y_{i-1} \bmod p_i = \left(\sum_{i=0}^{n-1} a_i \cdot r_i \right) \bmod p_i .$$

Розроблений метод характеризується меншою часовою складністю порівняно з класичними за рахунок заміни операції множення операцією додавання.

Для отримання шифр-тексту для повідомлення M знаходиться значення $b = y^k \cdot M \bmod p$.

Спочатку обчислюється значення $\alpha = y^k \bmod p$ на основі використання векторно-модульного алгоритму модулярного експоненціювання згідно формули:

$$\alpha = y^k \bmod p = \left(\sum_{i=1}^{l} b_i B_i y_i \right) \bmod p,$$

де $y_i = \left(y \bmod p_i\right)^k \bmod p_i$, $p = \prod_{i=1}^{l} p_i$, $B_i = \frac{p}{p_i}$, $b_i = B_i^{-1} \bmod p_i$, l – кількість модулів та потоків.

Пошук значення $y_i = \left(y \bmod p_i\right)^k \bmod p_i$ здійснюється на основі використання векторно-модульного методу модулярного множення з використанням представлення $k = \sum_{j=0}^{n-1} k_j \cdot 2^j$, де $k_j = 0,1$ згідно формули обчислити y_i:

$$y_i = \left(y \bmod p_i\right)^{\sum_{j=0}^{n-1} k_j \cdot 2^j} \bmod p_i = \prod_{j=1}^{n-1} \left(y \bmod p_i\right)^{k_j \cdot 2^j} = \prod_{j=0}^{n-1} \beta_j \bmod p_i,$$

де $\beta_i = y^{2^i} \bmod p_i$, при чому $\beta_i = \left(\beta_{i-1}\right)^2 \bmod p_i$. Тоді будь-який степінь k можна записати за степенями 2 і шуканий результат можна отримати, перемноживши відповідну кількість стовбців за допомогою таблиці 5.

Таблиця 5.

Вектор піднесення до степеня в базисі Радемахера–Крестенсона

k_{n-1}		k_i	…	k_1	k_0
β_{n-1}		β_i	…	β_1	β_0
$y^{2^{n-1}} \bmod p_i$	…	$y^{2^i} \bmod p_i$	…	$y^{2^1} \bmod p_i$	$y^{2^0} \bmod p_i$

Для пошуку значення y_i перемножаються ті значення β_i, для яких $k_j = 1$. Для знаходження значення $\beta_i \beta_{i-1} \bmod p_i$ представимо $\beta_{i-1} = \sum_{z=0}^{n-1} f_z \cdot 2^z$, де $f_z = 0,1$, n – розрядність модуля p_i. На основі використання векторно-модульного методу будуються два вектор-рядки, в першому з яких записуються елементи:

$$c_0 = 2^0 \beta_i \bmod p_i,\ c_i = 2 \cdot \beta_{i-1} \bmod p_i,$$

в другому f_z, як показано в таблиці 6.

Таблиця 6.

Представлення вектор-рядків модульного множення

c_{n-1}	…	c_i	…	c_1	c_0
f_{n-1}		f_i	…	f_1	f_0

Результат модулярного множення знаходиться згідно формули:

$$\beta_i \beta_{i-1} \bmod p_i = \left(\sum_{i=0}^{n-1} c_i \cdot f_i \right) \bmod p_i .$$

На наступному кроці обчислюються значення $b = y^k \cdot M \bmod p = \alpha \cdot M \bmod p$ на основі векторно-модульного методу модулярного множення. Для знаходження значення $\alpha \cdot M \bmod p$ представимо $M = \sum_{k=0}^{n-1} M_k \cdot 2^k$, де $\alpha_j, M_k = 0,1$, n – розрядність модуля p. Будуються два вектор-рядки, в першому з яких записуються елементи:

$$\delta_0 = 2^0 \alpha \bmod p_i,\ \delta_i = 2 \cdot \delta_{i-1} \bmod p_i,$$

в другому M_i, як показано в таблиці 7.

Таблиця 7.

Представлення вектор-рядків модульного множення

δ_{n-1}	…	δ_i	…	δ_1	δ_0
M_{n-1}		M_i	…	M_1	M_0

Результат модулярного множення знаходиться зі співвідношення:

$$b = \alpha \cdot M \bmod p = \left(\sum_{i=0}^{n-1} \delta_i \cdot M_i \right) \bmod p .$$

В результаті проведених обчислень, отримується пара (a,b), яка є шифротекстом.

3. Дешифрування відбувається згідно формули $M = b \cdot (a^x)^{-1} \bmod p$. Спочатку знаходиться значення $\varepsilon = a^x \bmod p$, для цього використовується векторно-модульний метод модулярного експоненціювання:

$$\varepsilon = a^x \bmod p = \left(\sum_{i=1}^{l} b_i B_i a_i \right) \bmod p ,$$

де $a_i = (a \bmod p_i)^k \bmod p_i$, $p = \prod_{i=1}^{l} p_i$, $B_i = \frac{p}{p_i}$, $b_i = B_i^{-1} \bmod p_i$, l – кількість модулів та потоків.

Пошук значення $a_i = (a \bmod p_i)^x \bmod p_i$ здійснюється на основі використання векторно-модульного методу модулярного множення, представивши $x = \sum_{j=0}^{n-1} x_j \cdot 2^j$, *де* $x_j = 0,1$ і згідно формули обчислити a_i:

$$a_i = (a \bmod p_i)^{\sum_{j=0}^{n-1} x_j \cdot 2^j} \bmod p_i = \prod_{j=1}^{n-1} (a \bmod p_i)^{x_j \cdot 2^j} = \prod_{j=0}^{n-1} \phi_j \bmod p_i .$$

де $\phi_i = a^{2^i} \bmod p_i$, при чому $\phi_i = (\phi_{i-1})^2 \bmod p_i$.

Тоді будь–який степінь x можна записати за степенями 2 і шуканий результат можна отримати, перемноживши відповідну кількість стовбців за допомогою таблиці 8. Для пошуку значення a_i перемножаються ці значення ϕ_i для яких $x_j = 1$. При обчисленні $\phi_i \phi_{i-1} \bmod p_i$ представимо $\phi_{i-1} = \sum_{j=0}^{n-1} \varphi_j \cdot 2^j$, де $\varphi_j = 0,1$, n – розрядність модуля p_i.

Таблиця 8.

Вектор піднесення до степеня в базисі Радемахера–Крестенсона

x_{n-1}		x_i	…	x_1	x_0
ϕ_{n-1}		ϕ_i	…	ϕ_1	ϕ_0
$a^{2^{n-1}} \bmod p_i$	···	$a^{2^i} \bmod p_i$	···	$a^{2^1} \bmod p_i$	$a^{2^0} \bmod p_i$

На основі використання векторно-модульного методу будуються два вектор-рядки, в першому з яких записуються елементи:

$$g_0 = 2^0 \phi_i \bmod p_i,\ g_i = 2 \cdot g_{i-1} \bmod p_i,$$

в другому φ_j, як показано в таблиці 9.

Таблиця 9.

Представлення вектор-рядків модульного множення

g_{n-1}	…	g_i	…	g_1	g_0
φ_{n-1}		φ_i	…	φ_1	φ_0

Результат модулярного множення обчислюється згідно формули:

$$\phi_i \phi_{i-1} \bmod p_i = \left(\sum_{i=0}^{n-1} g_i \cdot \varphi_i \right) \bmod p_i .$$

В подальшому необхідно знайти $\eta = \varepsilon^{-1} \bmod p$ на основі методу з додаванням залишку, що дозволить зменшити часову складність в порівнянні з класичними методами, які грунтуються на розширеному алгоритмі Евкліда, методі повного перебору та з використанням функції Ейлера.

Спочатку обчислюється $\eta_0 = p \bmod \varepsilon \neq 0$, після чого послідовно виконується операція додавання: $\eta_1 = (\eta_0 + 1) \bmod \varepsilon$, $\eta_2 = (\eta_1 + \eta_0) \bmod \varepsilon = (2\eta_0 + 1) \bmod \varepsilon$, … , $\eta_i = (\eta_{i-1} + \eta_0) \bmod \varepsilon = (i\eta_0 + 1) \bmod \varepsilon$.

Описана процедура продовжується до тих пір, поки деяке число η_i не стане рівним нулю. Тоді обернений елемент визначається за формулою:

$$\eta = \varepsilon^{-1} \bmod p = \frac{i \cdot p + 1}{\varepsilon}.$$

Векторно-модульний метод модулярного множення дозволить знайти значення $M = b \cdot \eta \bmod p$, що і є результатом дешифрування. Запишемо $\eta = \sum_{k=0}^{n-1} \eta_k \cdot 2^k$, де $b_j, \eta_k = 0,1$, n – розрядність модуля p. На основі використання векторно-модульного методу будуються два вектор-рядки, в першому з яких записуються елементи:

$$\lambda_0 = 2^0 b \bmod p,\ \lambda_i = 2 \cdot \lambda_{i-1} \bmod p,$$

в другому η_i, як показано в таблиці 10.

Таблиця 10.

Представлення вектор-рядків модульного множення

λ_{n-1}	…	λ_i	…	λ_1	λ_0
η_{n-1}		η_i	…	η_1	η_0

Результат модулярного множення $M = b \cdot \phi \bmod p$ знаходиться згідно співвідношення:

$$M = b \cdot \eta \bmod p = \left(\sum_{i=0}^{n-1} \lambda_i \cdot \eta_i \right) \bmod p .$$

Отже, запропонований підхід шифрування/дешифрування асиметричної криптосистеми Ель-Гамаля дозволяє розпаралелити процес та проводити обчислення над числами меншої розрядності в порівнянні з класичним підходом, що, в свою чергу, призводить до зменшення часової складності базових операцій: модулярного множення та експоненціювання, пошуку оберненого елемента за модулем.

Висновки

В роботі представлено удосконалення реалізації асиметричного алгоритму шифрування Ель-Гамаля, а саме базові операції модулярного експоненціювання багаторозрядних чисел, на основі СЗК та векторно-модульного алгоритму модулярного множення, що дозволило суттєво зменшити часову складність та підвищити ефективність виконання процесу шифрування/дешифрування.

Список літератури

1. Касянчук, М.М. Модифікований метод шифрування Рабіна з використанням різних форм системи залишкових класів / М.М. Касянчук, І.З. Якименко, Л.О. Дубчак, Н.А. Рендзеняк, Н.М. Мандебура // Вісник Хмельницького національного університету. Технічні науки, 2017. — № 1 (245). — С. 127-131.
2. Якименко, І.З. Теорія алгоритмів RSA та Ель–Гамаля в розмежованій системі числення Радемахера–Крестенсона / І.З. Якименко, М.М. Касянчук, О.І. Волинський, І.Р. Пітух // Вісник Хмельницького національного університету. Технічні науки, 2011. — № 3. — С. 265-273.
3. Kasianchuk, M.M. Algorithms of findings of perfect shape modules of remaining classes system / M. Kasianchuk, I. Yakymenko I. Pazdriy, O. Zastavnyy // XIII International Conference “The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM-2015)”, 23-25 February, 2015, Polyana-Svalyava (Zakarpattya), Ukraine. — Pp. 168-171.
4. Касянчук, М.М. Аналітичний пошук модулів досконалої форми системи залишкових класів та їх застосування в китайській теоремі про залишки / М.М. Касянчук, І.З. Якименко, І.Р. Паздрій, Я.М. Николайчук // Вісник Хмельницького національного університету. Технічні науки, 2015. — № 1 (221). — С. 170-176.
5. Kozaczko, D. Vector Module Exponential in the Remaining Classes System / D. Kozaczko, M. Kasianchuk, I. Yakymenko, S. Ivasiev // Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS–2015) – Warsaw, Poland, September, 2015. — V.1. — Pp. 161-163.

УСОВЕРШЕНСТВОВАНИЕ РЕАЛИЗАЦИИ КРИПТОАЛГОРИТМА ЭЛЬ-ГАМАЛЯ НА ОСНОВЕ СИСТЕМЫ ОСТАТКОВ

И.З. Якименко

Тернопольский национальный экономический университет,
ул. Львовская, 11, Тернополь, 46020, Украина; e-mail: iyakymenko@ukr.net

В данной работе проведен анализ систем защиты информационных потоков с использованием асимметричных криптоалгоритмов, на основе которого установлены недостатки существующих подходов реализации операций модулярного експоненцирования при шифровании/дешифровании, а именно – использование ключей, блоков шифрования и модуля криптопреобразования до 2048 и 4096 бит, что приводит к уменьшению временных характеристик. Установлено, что одним из перспективных подходов к решению данного класса задач является использование системы остаточных классов (СОК), которая обладает рядом преимуществ по сравнению с двоичной – осуществление операций параллельно и уменьшение разрядности операндов, которые не превышают разрядности набора выбранных модулей СОК. Указанные недостатки, касающиеся перевода с СОК в десятичную систему счисления, а именно необходимость поиска обратного элемента по модулю, то есть базисных чисел. В работе отмечено, что существуют наборы модулей, которые образуют совершенную форму СОК (базисные числа равны 1) и модифицированную совершенную СОК (базисные числа равны ±1), что существенно уменьшает временную сложность перевода. Приведенные теоретические основы совершенствования реализации асимметричного криптоалгоритма Эль-Гамаля на основе совместного использования СОК и векторно-модульного алгоритма модулярного умножения, что позволило распараллелить процесс, уменьшить временную сложность и повысить эффективность выполнения процесса шифрования/дешифрования.

Ключевые слова: криптосистема Эль-Гамаля, система остаточных классов, модульное умножение, векторно-модульный метод, вычислительная сложность, обратный элемент по модулю, совершенная форма системы остаточных классов, модифицированная система счисления системы остаточных классов, шифрование, дешифрование

IMPROVING THE IMPLEMENTATION OF EL-GAMAL CRYPTOALGORITHM ON THE BASIS OF THE SYSTEM OF RESIDUE CLASSES

I.Z. Yakymenko

Ternopil National Economic University,
11, Lvivska Str., Ternopil, 46020, Ukraine; e-mail: iyakymenko@ukr.net

The analysis of information flow protection systems, using asymmetric cryptalgorithms, on the basis of which the shortcomings of existing approaches of realization of the operations of modular exponentiation at encrypting/decrypting, namely - use of keys, encryption units and crypto-conversion module up to 2048 and 4096 bt, which reduces the time characteristics, was made in this work (thesis). It was established, that one of the perspective approaches concerning the solution of this class of tasks is use of the system of residue classes (SRC), which has several advantages in comparison with the binary one – conducting operations in parallel and digit capacity decrease of the operands, which do not exceed digit capacity of the selected SRC modules set. These drawbacks concern transfer from SRC to the decimal number system, namely the need to search for the reverse element by module, that is, the basis numbers. The thesis states that there are modules sets, which form the perfect SRC form (basic numbers are equal to 1) and modified perfect SRC (basic numbers are equal to ±1), which significantly reduces the time complexity of the transfer. Theoretical foundations of improvement of implementation of asymmetric El-Gamal cryptoalgorithm on the basis of joint use of SRC and vector-modular algorithm of modular multiplication, which made it possible to parallelize the process, to reduce time complexity and to improve performance of encrypting/decrypting process were given.

Keywords: El-Gamal cryptosystem, the system of residue classes, modular multiplication, vector-modular method, computational complexity, reverse element by module, perfect form of the system of residue classes, modified system of computation of the system of residue classes, encrypting, decrypting