ISSN 2078–5097. Вісн. Львів. ун-ту. Сер. прикл. матем. та інф. 2014. Вип. 21. С. 110–117
Visnyk of the Lviv University. Series Appl. Math. and Informatics. Issue 21. P. 110–117

УДК 512.742.72

КРИПТУВАННЯ З ВИКОРИСТАННЯМ ЕЛІПТИЧНОЇ КРИВОЇ

О. Коссак, Я. Холявка

Львівський національний університет імені Івана Франка,
вул. Університетська, 1, Львів, 79000,
e-mail: evagata23@yahoo.com, ya_khol@franko.lviv.ua

Розглянуто криптосхему, засновану на протоколі Діффі-Геллмана для кільця $\mathbf{Z}_p$ та групи точок еліптичної кривої Вейєрштрасса. Запропонований алгоритм має достатній рівень безпеки при невеликих обчислювальних затратах.

Ключові слова: еліптичні криві Вейєрштрасса, протокол Діффі-Геллмана.

1. ВСТУП

Розглянемо схему криптування, засновану на криптографічному протоколі Діффі-Геллмана для кільця $\mathbf{Z}_p$ та його аналогові для групи точок еліптичної кривої над скінченним полем [3].

Протокол Діффі-Геллмана є асиметричною схемою шифрування. Він дає змогу створити секретний ключ без передачі його каналами зв'язку. Потрібно, щоб учасники отримали той самий секретний ключ без обміну секретною інформацією. Цей ключ створюють так: Аліса і Боб (імена учасників відповідають визначеній у криптографії традиції) відкритими повідомленнями вибирають достатньо велике просте число p, за модулем якого проводитимуть усі обчислення, і основу g, $2<g<p$. Потім Аліса вибирає секретне число a і передає Бобу обчислене нею число $g^a \pmod p$, а Боб вибирає відоме тільки йому число b і передає Алісі число $g^b \pmod p$. Тепер Алісі потрібно підняти отримане від Боба число до степеня a, а Бобу отримане від Аліси число у степінь b, і у них обох буде секретний ключ $g^{ab} \pmod p$. Стійкість такої криптосистеми пов'язана з обчислювальною трудністю операції дискретного логарифмування – знаючи числа g, p і $g^a \pmod p$, потрібно обчислити a. Такий спосіб створення відомого тільки Алісі та Бобу (секретного) ключа дає підстави уникнути прямого обміну ключами, що є важливою проблемою для користування будь-якою симетричною системою шифрування. Цей ключ також можна використати для подальшого шифрування шифрами з симетричним ключем.

Замість $\mathbf{Z}_p$ у цій схемі можна використовувати групу раціональних точок на еліптичній кривій. В. Міллер і Н. Кобліц [4,5] запропонували застосовувати в криптографії еліптичні криві Вейєрштрасса. Алгоритми, побудовані на властивостях групи раціональних точок еліптичної кривої Вейєрштрасса з відповідно підібраними параметрами, мають високу стійкість. За роки використання таких алгоритмів не відбулось помітного падіння їхньої стійкості, хоча стійкість алгоритмів, побудованих на інших групах, помітно зменшилась.

Домовимось обміном повідомленнями вважати таку передачу інформації відкритими каналами зв'язку, коли від імені абонента передають і отримують саме його повідомлення.

2. ГРУПА ТОЧОК ЕЛІПТИЧНОЇ КРИВОЇ

Над кільцем $\mathbf{Z}_p$, p – достатньо велике просте число, розглянемо невироджену еліптичну криву E, задану у формі Вейєрштрасса рівнянням

$$y^2 = x^3 + ax + b, \tag{1}$$

де a, b – елементи $\mathbf{Z}_p$. Раціональною точкою еліптичної кривої E називають точку $P=(x,y)$, де x, y – елементи $\mathbf{Z}_p$ і задовольняють (1). Надалі розглядатимемо лише раціональні точки кривої E, тому ці точки та нескінченно віддалену точку O будемо називати точками кривої E. Усі міркування та арифметичні дії проводитимемо над кільцем $\mathbf{Z}_p$, елементи $\mathbf{Z}_p$ будемо називати числами.

На множині точок кривої (1) визначають операцію $\oplus$ [6]. Спочатку для довільної відмінної від O точки $P=(x,y)$ кривої E приймемо $-P=(x,-y)$. Координати $-P$ задовольняють (1), тому $-P \in E$.

Якщо $P_1=(x_1,y_1)$, $P_2=(x_2,y_2)$ – відмінні від O різні точки еліптичної кривої E, заданої рівнянням (1), і $P_1 \neq -P_2$, тоді $P_1 \oplus P_2$ визначимо як точку $P_3=(x_3,y_3)$, де (x_3,y_3) обчислюють так:

$$\begin{cases} x_3 = \left(\dfrac{y_2-y_1}{x_2-x_1}\right)^2 - x_1 - x_2, \\ y_3 = \dfrac{y_2-y_1}{x_2-x_1}(x_1-x_3) - y_1. \end{cases} \tag{2}$$

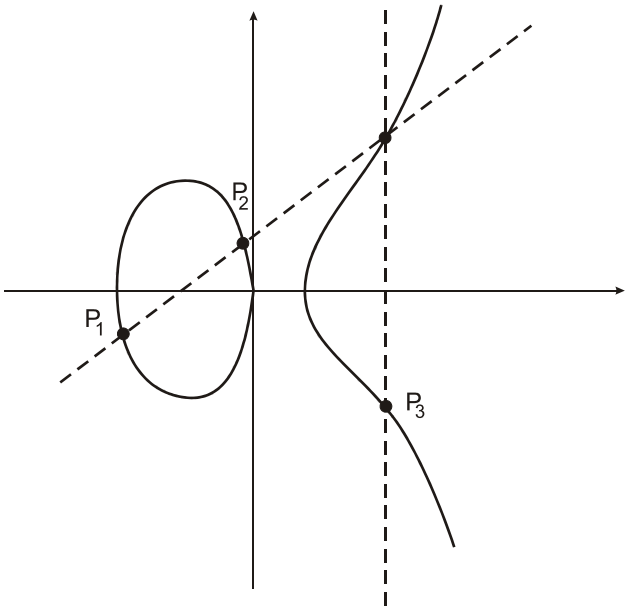
Якщо $P_1=P_2$, $P_1 \neq O$, то $2P_1 = P_1 \oplus P_1 = P_3$ і

$$\begin{cases} x_3 = \left(\dfrac{3x_1^2+a}{2y_1}\right)^2 - 2x_1, \\ y_3 = -\dfrac{3x_1^2-a}{2y_1}x_3 + \dfrac{x_1^3-ax_1-2b}{2y_1}. \end{cases} \tag{3}$$

Відомо [6], що точки кривої (1) разом з O утворюють абелеву групу стосовно так визначеної операції $\oplus$, нейтральним елементом якої є O, а протилежним елементу P є елемент $-P$. Надалі групову операцію $\oplus$ будемо позначати через +, а також позначимо $2P = P+P$, $3P = 2P+P$, …, $(k-1)P = (k-2)P+P$, де k – порядок точки P.

Крива (1) задана над $\mathbf{Z}_p$, тому група точок такої кривої скінченна. Порядок N цієї групи (його називають порядком кривої E) задовольняє нерівність $|N-p-1| \le 2\sqrt{p}$ [2,6]. У криптографії зазвичай використовують еліптичні криві Вейєрштрасса, задані над $\mathbf{Z}_p$ і порядок яких ділиться на достатньо велике просте число.

Якщо крива $y^2 = x^3 + ax + b$ задана над полем дійсних чисел, то визначеній співвідношеннями (2) груповій операції можна надати геометричну інтерпретацію. На рис. схематично зображено операцію $P_3 = P_1 + P_2$ для різних точок еліптичної кривої Вейєрштрасса.



Операція додавання точок на еліптичній кривій Вейєрштрасса

3. АЛГОРИТМ КРИПТУВАННЯ ЗА ДОПОМОГОЮ ГРУПИ ТОЧОК ЕЛІПТИЧНОЇ КРИВОЇ

Опишемо алгоритм криптування, який використовує одночасно кільце $\boldsymbol{Z}_p$ і групу точок кривої $\boldsymbol{E}$. Обмін закритим повідомленням Аліса та Боб виконують у декілька кроків.

3.1. СТВОРЕННЯ КЛЮЧІВ

Відкрита інформація.

Перед початком обміну закритими повідомленнями Аліса та Боб відкритими повідомлення визначають таке:

1) достатньо велике просте число p. Наприклад, згідно зі стандартами FIPS (*Federal Information Processing Standards*) число p має довжину 192, 224, 256, 384 або 521 біт;

2) еліптичну криву E: $y^2 = x^3 + ax + b$ над $\boldsymbol{Z}_p$ [1, 2] (для вибраного згідно зі стандартами числа p FIPS рекомендують і сертифіковану еліптичну криву) та точку C_0 достатньо великого порядку;

3) випадкове число g з кільця $\boldsymbol{Z}_p$, $2<g<p$;

4) алфавіт – тобто створюють таблицю, в якій кожному елементу потрібного для користування алфавіту ставлять у відповідність точку еліптичної кривої E. Різним елементам алфавіту відповідають різні точки кривої;

5) довжину n випадкових послідовностей.

Створення закритих ключів.

Після узгодження початкових даних Аліса генерує випадкові послідовності $\{\alpha_{i,j}\}$, $i=1,2,3$, $j=1,\ldots,n$, $\alpha_{i,j}\in \mathsf{Z}_p$ наперед домовленої довжини n, та обчислює послідовності $\{g^{\alpha_{i,j}}\}$, $\{\alpha_{3,j}C_0\}$, $i=1,2$, $j=1,\ldots,n$.

Боб генерує випадкові послідовності $\{\beta_{i,j}\}$, $i=1,2,3$, $j=1,\ldots,n$, $\beta_{i,j}\in \mathsf{Z}_p$, та обчислює послідовності $\{g^{\beta_{i,j}}\}$, $\{\beta_{3,j}C_0\}$, $i=1,2$, $j=1,\ldots,n$.

Позначимо згенеровані та обчислені Алісою і Бобом послідовності через (α_1), (α_2), (α_3), (g^{α_1}), (g^{α_2}), (α_3C_0), (β_1), (β_2), (β_3), (g^{β_1}), (g^{β_2}) та (β_3C_0), відповідно. Відкритим повідомленням вони обмінюються послідовностями (g^{α_1}), (g^{α_2}), (α_3C_0), (g^{β_1}), (g^{β_2}) та (β_3C_0).

Отримавши повідомлення від Боба, Аліса обчислює послідовності $((g^{\beta_1})^{\alpha_1}) = \{(g^{\beta_{1,1}})^{\alpha_{1,1}}, \ (g^{\beta_{1,2}})^{\alpha_{1,2}},\ldots, \ (g^{\beta_{1,n}})^{\alpha_{1,n}}\}$, $((g^{\beta_2})^{\alpha_2}) = \{(g^{\beta_{2,1}})^{\alpha_{2,1}}, \ (g^{\beta_{2,2}})^{\alpha_{2,2}},\ldots, (g^{\beta_{2,n}})^{\alpha_{2,n}}\}$ та $(\alpha_3\beta_3C_0)=\{\alpha_{3,1}\beta_{3,1}C_0, \ \alpha_{3,2}\beta_{3,2}C_0,\ldots, \ \alpha_{3,n}\beta_{3,n}C_0\}$. Боб, отримавши повідомлення від Аліси, обчислює послідовності $((g^{\alpha_1})^{\beta_1})$, $((g^{\alpha_2})^{\beta_2})$, та $(\beta_3\alpha_3C_0)$.

Отже, після проведених обчислень Аліса і Боб мають ті ж самі послідовності (секретні ключі). Позначимо ці послідовності так: $(k_1) = (g^{\alpha_1\beta_1})$, $(k_2) = (g^{\alpha_2\beta_2})$, $(k_3) = (C) = \{C_j\}_{j=1,\ldots,n} = (\alpha_3\beta_3C_0)$, тобто

$$(k_1) = \{k_{1,j}\}_{j=1,\ldots,n} = \{g^{\alpha_{1,j}\beta_{1,j}}\}_{j=1,\ldots,n},$$

$$(k_2) = \{k_{2,j}\}_{j=1,\ldots,n} = \{g^{\alpha_{2,j}\beta_{2,j}}\}_{j=1,\ldots,n},$$

$$(k_3) = \{\alpha_{3,j}\beta_{3,j}C_0\}_{j=1,\ldots,n} = \{C_j\}_{j=1,\ldots,n} = \{(c_{1,j},c_{2,j})\}_{j=1,\ldots,n}.$$

Зауважимо, що ключ (k_3) можна побудувати без відкритого обміну точкою C_0. Наприклад, Аліса вибирає точку A достатньо великого порядку на кривій E, обчислює $(k_1)A$ та $(k_2)(k_1)A$ і надсилає Бобу $(k_1)A$. Боб, отримавши $(k_1)A$, обчислює $(k_2)(k_1)A$. Тепер Аліса і Боб мають спільний ключ $(k_3) = (k_1)(k_2)A$. Якщо алгоритм будувати з використанням несертифікованої еліптичної кривої (наприклад, кривої Едвардса), то подібно можна вибрати і параметри цієї кривої.

3.2. ШИФРУВАННЯ ПОВІДОМЛЕННЯ

Для відправлення повідомлення Аліса шифрує його так:

1) за допомогою алфавітної таблиці записує повідомлення M у цифровому форматі й отримує послідовність точок еліптичної кривої (1), яку позначимо (M_1);

2) до отриманої послідовності $(M_1)=(x_1,y_1)=\{(x_{1,j},y_{1,j})\}_{j=1,\ldots,n}$ точок кривої E додає послідовність (k_3): $(M_2)=\{(x_{1,j}+c_{1,j},y_{1,j}+c_{2,j})\}_{j=1,\ldots,n}=(x_2,y_2)$;

3) до перших координат точок (M_2) додає (k_1), а до других координат – (k_2):
$(M_3) = (x_2,y_2)+(k_1,k_2) = \{(x_{2,j}+k_{1,j},y_{2,j}+k_{2,j})\}_{j=1,\ldots,n} = \{(x_{3,j},y_{3,j})\}_{j=1,\ldots,n}$;

4) передає Бобу отриману послідовність $E(M)=(M_3)$.

Розміри повідомлення і ключа узгоджують. Якщо повідомлення великої довжини, то його розбивають на блоки, довжина яких залежить від довжини ключа. Блоки у разі потреби шифрують окремо та використовують різні ключі, різні алгоритми для різних блоків тощо.

3.3. ДЕШИФРУВАННЯ ПОВІДОМЛЕННЯ

Усі перетворення Аліса виконувала над елементами групи точок еліптичної кривої і елементами $\boldsymbol{Z}_p$, тому вони оборотні. Щоб прочитати повідомлення, Боб над отриманою послідовністю виконує у зворотному порядку виконані Алісою перетворення тексту:

1) (M_2): $(M_2) = E(M) - (k_1, k_2)$;

2) (M_1): $(M_1) = (M_2) + (-C)$;

3) (M_1) перетворює у текст (M) відповідного алфавіту згідно з визначеною таблицею.

4. ПРИКЛАД

Припустимо, що Аліса хоче передати Бобу повідомлення **bead**. Спочатку Аліса та Боб відкритими каналами зв'язку домовляються про вибір простого числа p та еліптичної кривої E. У прикладі достатньо взяти малі числа, тому приймемо $p = 47$, $E: y^2 = x^3 + 3x + 5 \pmod{47}$. Крива E складається з таких точок:

(1, 3), (1, 44), (4, 9), (4, 38), (5, 2), (5, 45), (6, 2), (6, 45), (8, 20), (8, 27), (9, 3), (9, 44), (10, 1), (10, 46), (11, 10), (11, 37), (13, 19), (13, 28), (14, 21), (14, 26), (17, 9), (17, 38), (18, 4), (18, 43), (19, 23), (19, 24), (20, 13), (20, 34), (22, 12), (22, 35), (23, 16), (23, 31), (24, 6), (24, 41), (25, 17), (25, 30), (26, 9), (26, 38), (32, 4), (32, 43), (34, 5), (34, 42), (35, 11), (35, 36), (36, 2), (36, 45), (37, 3), (37, 44), (38, 1), (38, 46), (40, 8), (40, 39), (41, 10), (41, 37), (42, 10), (42, 37), (44, 4), (44, 43), (46, 1), (46, 46).

Ці точки разом з точкою O утворюють групу стосовно операції додавання, визначеної співвідношеннями (2) та (3).

У нашому прикладі приймемо n = 5, виберемо алфавіт з п'яти елементів і визначимо алфавітну табличку:

a	b	c	d	e
(1, 3)	(1, 44)	(4, 9)	(4, 38)	(5, 2)

Аліса та Боб вибирають число g та точку C_0 кривої E. Приймемо $g = 5$, $C_0 = (5,45)$. Аліса генерує випадкові числові послідовності $\{\alpha_{i,j}\}_{i=1,2,3,\, j=1,\ldots,5}$:

$\alpha_{1,1}$	$\alpha_{1,2}$	$\alpha_{1,3}$	$\alpha_{1,4}$	$\alpha_{1,5}$
1	2	3	4	5

$\alpha_{2,1}$	$\alpha_{2,2}$	$\alpha_{2,3}$	$\alpha_{2,4}$	$\alpha_{2,5}$
6	7	8	9	10

$\alpha_{3,1}$	$\alpha_{3,2}$	$\alpha_{3,3}$	$\alpha_{3,4}$	$\alpha_{3,5}$
11	12	13	14	15

Боб так само генерує випадкові числові послідовності $\{\beta_{i,j}\}_{i=1,2,3,\, j=1,\ldots,5}$:

$\beta_{1,1}$	$\beta_{1,2}$	$\beta_{1,3}$	$\beta_{1,4}$	$\beta_{1,5}$
16	17	18	19	20

$\beta_{2,1}$	$\beta_{2,2}$	$\beta_{2,3}$	$\beta_{2,4}$	$\beta_{2,5}$
21	22	23	24	25

$\beta_{3,1}$	$\beta_{3,2}$	$\beta_{3,3}$	$\beta_{3,4}$	$\beta_{3,5}$
26	27	28	29	30

Незалежно один від одного, Аліса та Боб обчислюють відповідні степені числа $g = 5$ та точки, кратні точці $C_0 = (5,45)$. Після проведення обчислень, вони обмінюються послідовностями $(g^{\alpha_1}), (g^{\alpha_2}), (\alpha_3 C_0), (g^{\beta_1}), (g^{\beta_2})$ та $(\beta_3 C_0)$:

$g^{\alpha_{1,1}}$	$g^{\alpha_{1,2}}$	$g^{\alpha_{1,3}}$	$g^{\alpha_{1,4}}$	$g^{\alpha_{1,5}}$
5	25	31	14	23

$g^{\alpha_{2,1}}$	$g^{\alpha_{2,2}}$	$g^{\alpha_{2,3}}$	$g^{\alpha_{2,4}}$	$g^{\alpha_{2,5}}$
21	11	8	40	12

$g^{\beta_{1,1}}$	$g^{\beta_{1,2}}$	$g^{\beta_{1,3}}$	$g^{\beta_{1,4}}$	$g^{\beta_{1,5}}$
17	38	2	10	3

$g^{\beta_{2,1}}$	$g^{\beta_{2,2}}$	$g^{\beta_{2,3}}$	$g^{\beta_{2,4}}$	$g^{\beta_{2,5}}$
15	28	46	42	22

$\alpha_{3,1}C_0$	$\alpha_{3,2}C_0$	$\alpha_{3,3}C_0$	$\alpha_{3,4}C_0$	$\alpha_{3,5}C_0$
(11,37)	(38,46)	(10,46)	(17,9)	(34,42)

$\beta_{3,1}C_0$	$\beta_{3,2}C_0$	$\beta_{3,3}C_0$	$\beta_{3,4}C_0$	$\beta_{3,5}C_0$
(8,27)	(23,16)	(20,34)	(24,41)	(42,37)

Отримавши послідовності (g^{α_1}), (g^{α_2}), $(\alpha_3 C_0)$, (g^{β_1}), (g^{β_2}) та $(\beta_3 C_0)$, Аліса і Боб обчислюють закриті (секретні) ключі (k_1), (k_2) та $(k_3) = (C)$:

$k_{1,1} = g^{\alpha_{1,1}\beta_{1,1}}$	$k_{1,2} = g^{\alpha_{1,2}\beta_{1,2}}$	$k_{1,3} = g^{\alpha_{1,3}\beta_{1,3}}$	$k_{1,4} = g^{\alpha_{1,4}\beta_{1,4}}$	$k_{1,5} = g^{\alpha_{1,5}\beta_{1,5}}$
17	34	8	36	8

$k_{2,1} = g^{\alpha_{2,1}\beta_{2,1}}$	$k_{2,1} = g^{\alpha_{2,2}\beta_{2,2}}$	$k_{2,3} = g^{\alpha_{2,3}\beta_{2,3}}$	$k_{2,1} = g^{\alpha_{2,4}\beta_{2,4}}$	$k_{2,1} = g^{\alpha_{2,5}\beta_{2,5}}$
34	17	1	7	3

$C_1 = \alpha_{3,1}\beta_{3,1}C_0$	$C_2 = \alpha_{3,2}\beta_{3,2}C_0$	$C_3 = \alpha_{3,3}\beta_{3,3}C_0$	$C_4 = \alpha_{3,4}\beta_{3,4}C_0$	$C_5 = \alpha_{3,5}\beta_{3,5}C_0$
(9,3)	(22,12)	(8,20)	(42,37)	(23,16)

Аліса записує повідомлення $(M) =$ **bead** у цифровому форматі:

$$(M_1) = (1,44)(5,2)(1,3)(4,38).$$

Створює послідовність $(M_2) = (M_1) + (C)$:

$(1,44) + (9,3) = (17,38)$,

$(5,2) + (22,12) = (41,10)$,

$(1,3) + (8,20) = (18,43)$,

$(4,38) + (42,37) = (19,23)$,

$(1,44)(5,2)(1,3)(4,38) + (9,3)(22,12)(8,20)(42,37) = (17,38)(41,10)(18,43)(19,23)$.

$(M_2) = (17,38)(41,10)(18,43)(19,23)$.

Отриману послідовність (M_2) Аліса змінює покоординатно, тобто до координат точок послідовності (M_2) додає відповідно послідовності (k_1) і (k_2), одержуємо послідовність ($(x) + (k_1)$, $(y) + (k_2)$):

17 + 17 = 34, 38 + 34=25,
41 + 34 = 28, 10 +17 =27,
18 + 8 = 26, 43 +31 =27,
19 + 36 = 8, 23 + 7=30.

Після перетворення повідомлення (M) Аліса отримала послідовність $E(M) = (34,25)(28,27)(26,27)(8,30)$, яку й надсилає Бобу.

Щоб перетворити отриману послідовність $E(M)$ у повідомлення (M), Бобу потрібно виконати дії Аліси у зворотному порядку. Спочатку Боб записує $E(M)$ як послідовності перших і других координат. Додаючи послідовності $(p - k_1)$ і $(p - k_2)$ до відповідних послідовностей координат, він отримує координати точок послідовності (M_2). За обчисленим ключем (k_3) Боб будує послідовність $(-k_3)$, замінивши $\{(c_{1,j}, c_{2,j})\}_{j=1,\ldots,5}$ в (k_3) на $\{(c_{1,j}, p - c_{2,j})\}_{j=1,\ldots,5}$. Після знаходження $(-k_3)$ він обчислює $(M_1) = (M_2) + (-k_3)$ та замінює (M_1) на повідомлення (M) згідно з домовленою алфавітною табличкою.

5. ВИСНОВКИ

Коректність, ефективність і надійність запропонованого протоколу визначаться відповідними властивостями протоколу Діффі-Геллмана та властивостями групи точок еліптичної кривої. Для уникнення ефективного дискретного логарифмування просте число p треба вибирати так, щоб $p - 1$ мало великий простий дільник.

При використанні описаного протоколу можливе втручання супротивника, який створює секретні ключі окремо з Алісою і Бобом, використовуючи їхню відкриту інформацію (атака “Людина посередині”). Після цього він має змогу приймати достовірні повідомлення, змінювати їх, передавати як достовірні від імені Аліси або Боба. Щоб запобігти такій ситуації, треба запропонований протокол доповнити протоколом ідентифікації.

Як і будь-яка асиметрична криптосхема, запропонований протокол також має переваги над симетричними криптосхемами при великій кількості абонентів – це надійність і мала кількість ключів невеликої довжини.

Для зручного користування афінними координатами можна замість еліптичної кривої Вейєрштрасса використати еліптичну криву Едвардса.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. *Болотов А. А.* Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых / А. А. Болотов, С. Б. Гашков, А. Б. Фролов. – М.: КомКнига, 2006. – 280 с.
2. *Василенко О. В.* Теоретико-числовые алгоритмы в криптографии / О. В. Василенко. – М.: МЦНМО, 2006. – 334 с.
3. *Черепнев М. А.* Криптографические протоколы / М. А. Черепнев. – М.: Издательство мех.-мат. ф-та МГУ, 2006. – 69 с.
4. *Koblitz N.* Elliptic Curve Cryptosystems / N. Koblitz // Math. Comp. – 1987. – Vol. 48. – P. 203-209.
5. *Miller V. S.* Use of Elliptic Curves in Cryptography / V. S. Miller // CRYPTO'85, LNCS. – 1986. – Vol 218 – P. 417-426.
6. *Silverman J. H.* The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, 106, / J. H. Silverman. – Springer-Verlag, New York, 1986. – 413 p.

Стаття: надійшла до редколегії 12.09.2013
доопрацьована 27.11.2013
прийнята до друку 18.12.2013

ШИФРОВАНИЕ С ИСПОЛЬЗОВАНИЕМ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

О. Коссак, Я. Холявка

Львовский национальный университет имени Ивана Франко,
ул. Университетская, 1, Львов, 79000,
e-mail: evagata23@yahoo.com, ya_khol@franko.lviv.ua

Рассмотрено шифросхему, основанную на протоколе Диффи-Хеллмана для кольца $\mathbf{Z}_p$ и группы точек эллиптической кривой Вейерштрасса. Предложенный алгоритм имеет достаточный уровень безопасности при небольших вычислительных затратах.

Ключевые слова: эллиптические кривые Вейерштрасса, протокол Диффи-Хеллмана.

ENCRYPTION USING ELLIPTIC CURVE

O. Kossak, Ya. Kholyavka

Ivan Franko National University of Lviv,
Universytetska Str., 1, Lviv, 79000,
e-mail: evagata23@yahoo.com, ya_khol@franko.lviv.ua

We consider an encryption system based on Diffie–Hellman protocol applied both to the ring $\mathbf{Z}_p$ and to the group of points on the Weierstrass elliptic curve. The algorithm proposed here provides sufficient security at sufficiently small computational expenses.

Key words: Weierstrass elliptic curves, Diffie-Hellman algorithm.