Міністерство освіти і науки України
Харківський національний університет імені В. Н. Каразіна

К. Є. Лисицький
І. В Лисицька
Д. Ю. Узлов

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

Методичні вказівки
до практичних занять з дисципліни для здобувачів вищої освіти першого (бакалаврського) рівня за спеціальністю 151 «Автоматизація та комп'ютерно-інтегровані технології» (174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка»)

Електронний ресурс

Харків – 2025

УДК 556.11:504.064
Л 88

Рецензенти:

І. В. Філіпенко – кандидат технічних наук, доцент кафедри автоматизації проектування обчислювальної техніки Харківського національного університету радіоелектроніки;

О. П. Нарєжній – кандидат технічних наук, доцент кафедри кібербезпеки інформаційних систем, мереж і технологій Харківського національного університету імені В. Н. Каразіна.

Затверджено до розміщення в мережі Інтернет рішенням Науково-методичної ради Харківського національного університету імені В. Н. Каразіна (протокол № 9 від 23 квітня 2025 року)

Лисицький К. Є.

Л 88 Технології захисту інформації : методичні вказівки до практичних занять з дисципліни для здобувачів вищої освіти першого (бакалаврського) рівня за спеціальністю 151 «Автоматизація та комп'ютерно-інтегровані технології» (174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка») [Електронний ресурс] / К. Є. Лисицький, І. В. Лисицька, Д. Ю. Узлов. – Харків : ХНУ імені В. Н. Каразіна, 2025. – (PDF 82 с.)

У методичних вказівках наведено загальні положення щодо технологій захисту інформації, подані для розв'язку декілька різновидів практичних робіт задля опанування студентами криптографічних методів захисту інформації, ознайомлення з математичними алгоритмами, які найчастіше використовуються в криптографії, симетричними та несиметричними криптографічними алгоритмами, методиками розрахунку параметрів криптоалгоритмів та специфічними методами криптоаналізу.

УДК 556.11:504.064

ЗМІСТ

Вступ

Питання інформаційної безпеки - важлива частина процесу впровадження нових інформаційних технологій у всі сфери життя суспільства.

Широкомасштабне використовування обчислювальної техніки і телекомунікаційних систем в рамках територіально-розподілених ІС, перехід на цій основі до безпаперової технології, збільшення кількості інформації, яка обробляється, і розширення круга користувачів приводять до якісно нових можливостей несанкціонованого доступу до ресурсів і даних інформаційної системи, до їх високої уразливості. Розповсюдження таких технологій вимагає добре поставленого захисту інформації.

Поняття інформаційної безпеки не обмежується безпекою технічних інформаційних систем чи безпекою інформації у чисельному чи електронному вигляді, а стосується усіх аспектів захисту даних чи інформації незалежно від форми, у якій вони перебувають.

Проводячи аналіз положення інформаційної безпеки різних відомств, організацій і фірм, можна прийти до висновку, що об'єктом захисту, який викликає найбільшу тривогу і акумулює всі проблеми інформаційної безпеки є інформаційно телекомунікаційні системи, які будуються на базі комп'ютерів.

З кожним роком число комп'ютерних атак, які скоюють зловмисники, зростає. Таким чином проблеми безпеки кіберпросторів набувають все більшої значимості та актуальності а витрати на кібербезпеку сягають астрономічних цифр.

Особливу роль у системі захисту інформації займають саме криптографічні методи захисту інформації, які дозволяють ефективно протидіяти викликам сучасності.

Практичне заняття 1

Найпростіші шифри заміни та перестановки. Моноалфавітні та поліалфавітні шифри

Теоретичні відомості

Ключ – деяка послідовність символів, яка керує процедурами шифрування – розшифрування.

Шифрування – процес перетворення відкритих даних у шифртекст по закону ключа.

Розшифрування – процес протилежний шифруванню.

Шифртекст – перетворені дані із закритим семантичним змістом.

Шифри простої заміни перетворюють відкритий текст таким чином, що кожний його символ замінюється на якій-небудь інший. При цьому однаковим символам відкритого тексту відповідають однакові символи шифртексту, а різним – різні. Ключем є таблиця, яка указує в який саме символ шифртекста переходить символ відкритого тексту. Без втрати спільності можна вважати, що повідомлення і шифртекст записують в одному і тому ж алфавіті, оскільки використання екзотичних символів не зробить шифр надійніше. Зробивши це припущення, можна легко підрахувати кількість всіх можливих ключів для шифру підстановки. Для алфавіту з 32 букв це 32! ключів.

Слід зазначити, що комбінація шифрів заміни – перестановки створюють все різноманіття вживаних на практиці симетричних шифрів. Розглянемо основні ідеї шифрів простої заміни на прикладах.

Класичний шифр Цезара

Римський імператор Юлій Цезар (100 - 44 р. до н.е.) шифрував свої повідомлення способом, при якому кожна буква тексту замінювалась деякою другою, яка стоїть у абетці на 3 позиції пізніше. Для української мови це означає а→г; б→д ; в→е. Останні літери абетки зміщувалися циклічно. У даному разі ключ К=3. Говорять, що шифр Цезара – шифр зсуву на 3 позиції (чи заміни .

Якщо узагальнити цю ідею, то можна зміщувати на кількість позицій, що визначаються довільним ключем (не тільки К=3).

Наприклад

Зашифрувати повідомлення ПЕРЕМОГА в українській абетці класичним шифром Цезара з ключем К=5. Зміщуємо кожну букву повідомлення на 5 позицій за українською абеткою.

П → Ф

Е → І

Р → Х

Е → І

М → С

О → У

Г → Ж

А → Д

Отримуємо шифртекст ФІХІСУЖД.

Так як це симетричний шифр то для розшифрування достатньо зсунути всі букви шифртексту на 5 позицій в зворотній бік. Також можна відмітити, що це моноалфавітний шифр. Однаковим символам відкритого тексту відповідають однакові символи шифртексту. Символ Е у повідомленні кожен раз відображається на символ І шифртексту.

Афінна система підстановок Цезара

Визначимо перетворення:

$E_{a,b}: \overline{Z_m} \longrightarrow \overline{Z_m}$

$E_{a,b}: t \longrightarrow E_{a,b}(t)$

$E_{a,b}(t) = at + b(mod\ m).$

a, b - цілі числа $0 \leq a, b < m$ і $НСД(a, m) = 1$.

В даному перетворенні буква, що відповідає числу t замінюється на букву згідно числовому значенню за формулою $at + b(mod\ m)$.

Наприклад

Нехай m=33, a=4, b=5. Виконується умова *НСД* (4,33) = 1. Ми одержуємо наступну відповідність між кодами букв (таблиця 1.1). Використовуватимемо для прикладу український алфавіт (33 букви).

Таблиця 1.1

Афінна система підстановок Цезара

Символ	t	$4t+5(\mathrm{mod}\ 33)$
а	0	5
б	1	9
в	2	13
г	3	17
ґ	4	21
д	5	25
е	6	29
є	7	0
ж	8	4
з	9	8
и	10	12
і	11	16
ї	12	20
й	13	24
к	14	28
л	15	32
м	16	3
н	17	7
о	18	11
п	19	15
р	20	19
с	21	23
т	22	27
у	23	31
ф	24	2
х	25	6
ц	26	10
ч	27	14
ш	28	18
щ	29	22
ь	30	26
ю	31	30
я	32	1

Наприклад слову відкритого тексту КАЛАМБУР відповідає шифртекст ШДЯДЄЗЮП. Афінна система використовувалася на практиці декілька століть назад, зараз її застосування обмежується ілюстрацією основних криптологічних положень.

Система Цезаря з ключовим словом

Система Цезаря з ключовим словом також є моноалфавітною підстановкою.

Наприклад

Нехай обрано слово DIPLOMAT в латинському алфавіті як ключове слово (слово без повторень букв) і числовий ключ $K = 5$.

Ключове слово записується під буквами алфавіту, починаючи з букви, числовий код якої співпадає з обраним числом $K = 5$.

0 1 2 3 4 5 6 …

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

V W Z Y Z D I P L O M A T B C E F G H J K N Q R S U

Решта букв алфавіту підстановки записується після ключового слова в алфавітному порядку, виключаючи букви, які вже використані у ключовому слові.

Відкритий текст *SEND MORE MONEY* перетворюється в шифртекст *HZBY TCGZ TCBZS.*

Шифр "подвійний квадрат" Уїнстона

В 1854 р. англієць Чарльз Уїтстон розробив новий метод шифрування біграмами, який називають "подвійним квадратом". Свою назву цей шифр отримав по аналогії з полібіанським квадратом. Шифр Уїтстона відкрив новий етап в історії розвитку криптографії. На відміну від полібіанського шифр "подвійний квадрат" використовує відразу дві таблиці, розміщені по одній горизонталі, а шифрування йде біграмами, як в шифрі Плейфейра.

Досить прості модифікації привели до появи якісно нової криптографічної системи ручного шифрування. Шифр "подвійний квадрат" виявився дуже

надійним і зручним і застосовувався Німеччиною навіть в роки другої світової війни.

Пояснимо процедуру шифрування цим шифром на прикладі.

Приклад

Нехай є дві таблиці з випадково розташованими в них українськими алфавітами. Перед шифруванням початкове повідомлення розбивають на біграми. Кожна біграма шифрується окремо. Першу букву біграми знаходять в лівій таблиці, а другу букву - в правій таблиці. Потім будують прямокутник так, щоб букви біграми лежали в його протилежних вершинах. Інші дві вершини цього прямокутника дають букви біграми шифртекста.

Таблиця 1.2

Дві таблиці з випадково розташованими символами українського алфавіту для шифру "подвійний квадрат"

	І	Р	Ч	Ю	Я		Ь	Ш	З	А	В	Б
И	Б	Ї	С	Ш	,		Р	Ю	Щ	Ж	Ґ	Г
П	З	В	Й	Т	Щ		С	П	Я	Ч	Є	Д
Ц	Ж	О	Г	К	У		Й	О	Т	_	Е	Ц
_	Х	Є	Н	Ґ	Л		Ї	К	Н	У	Ф	Х
.	Ь	Ф	Д	Е	М		І	И	Л	М	,	.

Припустимо, що шифрується біграма ІЛ початкового тексту. Буква І знаходиться в стовпці 2 і рядку 1 лівої таблиці. Буква Л знаходиться в стовпці 3 і рядку 6 правої таблиці. Це означає, що прямокутник освічений рядками 1 і 6, а також стовпцями 2 лівої таблиці і 3 правої таблиці.

Отже, в біграму шифртекста входять буква З, розташована в стовпці 3 і рядку 1 правої таблиці, і буква Ь, розташована в стовпці 2 і рядку 6 лівої таблиці, тобто одержуємо біграму шифртекста ЗЬ.

Якщо обидва букви біграми повідомлення лежать в одному рядку, то і букви шифртекста беруть з цього ж рядка. Першу букву біграми шифртекста беруть з лівої таблиці в стовпці, відповідному другій букві біграми

повідомлення. Друга ж буква біграми шифртекста береться з правої таблиці в стовпці, відповідному першій букві біграми повідомлення. Тому біграма повідомлення ТЄ перетворюється в біграму шифртекста ЗЄ. Аналогічним чином шифруються всі біграми повідомлення:

Повідомлення ПР ИЛ ІТ АЮ

Шифртекст СИ Щ . ЗЖ ШИ

Шифрування методом "подвійного квадрата" дає вельми стійкий до розкриття і простій в застосуванні шифр. Злам шифртекста "подвійний квадрат" вимагає великих зусиль. При цьому довжина повідомлення повинна бути не менш тридцяти рядків.

Шифр одноразового блокноту Гілберта Вернама

Шифр Вернама (англ. Verrnam Cipher) – система симетричного шифрування, винайдена в 1917 році співробітником AT & T Гилбертом Вернамом.

Шифр є різновидом криптосистеми одноразових блокнотів. У ньому використовується булева функція «виключне АБО».

Шифр Вернама є прикладом системи з абсолютною криптографічною стійкістю, при дотриманні певних умов. Але якщо їх не дотримуватися проявляється слабкість одноразового шифроблокнота. Порушення правил веде до того, що абсолютно надійний шифр перетворюється в той, що досить легко зламати.

Для отримання шифртекста відкритий текст об'єднується операцією «виключне АБО» з секретним ключем. Так, наприклад, при застосуванні ключа (1 1 1 0 1) на букву «А» (1 1 0 0 0) отримуємо зашифроване повідомлення (0 0 1 0 1):

$$(11000) \oplus (11101) = (00101)$$

Для прийнятого повідомлення відомий ключ (1 1 1 0 1). Легко отримати вихідне повідомлення за допомогою тієї ж операції:

$$(00101) \oplus (11101) = (11000)$$

Для абсолютної криптографічної стійкості ключ повинен володіти трьома критично важливими властивостями:

– мати випадковий рівномірний розподіл;

– збігатися за розміром із заданим відкритим текстом;

– застосовуватися тільки один раз.

Наприклад

Зашифрувати перші три букви свого імені (наприклад ІРА), використавши шифр одноразового блокноту з ключем 110000 011110 010100. Букви імені для цього спочатку надати в двійковій формі (кожен блок з шести цифр є номером відповідної букви у двійковому запису).

Запишемо українську абетку і пронумеруємо з нуля. Це можна подивитися у табл. 1.1.

Впишемо номери кожної букви імені і переведемо у двійкову форму (молодші розряди праворуч, 6 позицій для відповідності кількості позицій ключа для кожної букви.

І – 11 $=2^3+2^1+1=001011$

Р– 20 $= 2^4+2^2=010100$

А– 0= 000000

Тепер будемо додавати кожну послідовність за модулем 2 до відповідного фрагменту ключа.

І – 001011	Р – 010100	А - 000000
$К_1$ – 110000	$К_2$– 011110	$К_3$– 010100
111011	001010	010100

Результат (шифртекст) переводимо в символи того ж алфавіту. Якщо потрібно зводимо за модулем 33 (кількість символів української абетки).

111011_2= 1+2+8+16+32=59 (mod 33)=26 – Ц

001010_2=2+8=10– И

010100_2=4+16=20– Р

Тобто імені IPA відповідає шифртекст ЦИР.

Багатоалфавітні системи

Багатоалфавітні (поліалфавітні) підстановочні шифри були винайдені Ліном Баттістою (Lean Battista) в 1568 році. Основна ідея багатоалфавітних систем полягає в тому, що впродовж всього тексту одна і та ж літера може бути зашифрована по-різному.

Тобто заміни для літери вибираються із багатьох алфавітів залежно від положення в тексті. Це є хорошим захистом від простого підрахунку частот, тому що не існує єдиного маскування для кожної літери в криптотексті.

Шифр Віженера

Однією із старих і найбільш відомих багатоалфавітних криптосистем є система Віженера, названа на честь французького криптографа Блейза Віженера (Vigenere). Цей метод був вперше опублікований в 1586 році.

У даному шифрі ключ задається набором з d літер. Такі набори підписуються із повторенням під повідомленням, а, потім, отриману послідовність складають із відкритим текстом за модулем n (потужність алфавіту). Тобто виходить наступна формула

$$\mathrm{Vig}_d(m_i) = (m_i + k_{i \bmod d}) \pmod{n}.$$

Літеру шифротексту можна знаходити також із таблиці, як перетин стовпця, визначуваного літерою відкритого тексту, і рядка, визначуваною літерою ключа. В окремому випадку, при d=1, отримуємо шифр Цезара.

Наприклад

Повідомлення *meeting point*, ключ *cipher.*

Пишемо повідомлення і підписуємо ключ. Результат можна подивитися в таблиці 1.3 на перетині стовбця та рядка, який відповідає цім символам.

M E E T I N G P O I N T повідомлення

C I P H E R C I P H E R ключ

O MT A M E I X D P R K шифртекст

Таблиця 1.3

Квадрат Віженера для латинського алфавіту

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Ще один приклад багатоалфавітної криптосистеми - шифр Грончфельда.

Шифр Гронсфельда

Для шифрування тут використовується цифровий ключ. Але кожна буква зміщується не на постійне число позицій, а на число позицій, що відповідає значенню ключа.

Ключ не обов'язково повинен бути таким же довгим як повідомлення, що шифрується. Якщо ключ коротше повідомлення, його просто повторюють по циклу. Так, наприклад, якщо в тексті 10 символів, а довжина ключа 5 символів, то для шифрування ключ використовуватиметься з повтореннями.

Приклад

Вхідний текст: "швидка перемога"

Ключ 14352

Ш В И Д К А П Е Р Е М О Г А

1 4 3 5 2 1 4 3 5 2 1 4 3 5

Зашифрований текст: «ЩЕЙИМБУЗХНТЕД».

Завдання до практичного заняття 1

Завдання 1. Зашифрувати повідомлення КРИПТОГРАФІЯ шифром Цезара з ключем $(m+1)\bmod 17$, де m - номер за списком у журналі.

Завдання 2.

Зашифрувати повідомлення КРИПТОГРАФІЯ афінною системою підстановок Цезара $(at+b)\bmod m$, де $1<a,b<m,\ \text{НОД}(a,m)=1$ в українському алфавіті. Параметри a та b обрати самостійно.

Завдання 3.

Зашифрувати перші три букви свого імені , використавши шифр одноразового блокноту з ключем 110000 011110 010100. Букви імені для цього спочатку надати в двійковій формі (кожен блок з шести цифр є номером відповідної букви у двійковому запису).

Завдання 4 .

Зашифрувати повідомлення (своє прізвище) шифром "подвійний квадрат" Уітстона. (див табл. для шифру подвійний квадрат Уітстона у українському алфавіті).

Завдання 5.

Зашифрувати шифром Гронсфельда повідомлення надане в таблиці завдання 6 згідно з варіантом. Ключ розрахувати за формулою 15148 – 16k, де k – номер за списком у журналі.

Завдання 6.

Дана система Цезара з ключовим словом. Алфавіт український. Зашифрувати повідомлення надане в таблиці 1.4 . Ключ також надано в таблиці. Ключове слово ФОРЕЛЬ.

Таблиця 1.4

Система Цезара з ключовим словом

№ вар	Ключ	Відкрите повідомлення	№ вар	Ключ	Відкрите повідомлення
1	7	КАЛАМБУР	16	7	ЛІЦЕЙ
2	8	МАТЕМАТИКА	17	8	КНИГА
3	9	КРИПТОГРАФІЯ	18	9	ГАЗЕТА
4	10	КРИПТОАНАЛІЗ	19	10	ЖУРНАЛ
5	11	ШИФР	20	11	ФІЗИКА
6	12	АЛГЕБРА	21	12	ПРІНТЕР
7	13	ГЕОМЕТРІЯ	22	13	ТЕЛЕВІЗОР
8	14	ПРАВИЛО	23	14	АУДИТОРІЯ
9	15	ДИПЛОМ	24	15	ДЕКАНАТ
10	1	БІОЛОГІЯ	25	16	ФАКУЛЬТЕТ
11	2	ГЕОГРАФІЯ	26	17	СТУДЕНТ
12	3	ХІМІЯ	27	18	ЕКЗАМЕН
13	4	ІНСТИТУТ	28	19	ПРАКТИКА
14	5	ШКОЛА	29	20	КРЕДИТ
15	6	ГІМНАЗІЯ	30	1	АУДИТОРІЯ

Завдання 6. Зашифрувати шифром Віженера повідомлення надане в таблиці у відповідності з номером по списку в журналі. Ключ також надано в таблиці 1.5.

Таблиця 1.5

Шифр Віженера

№ вар	Повідомлення	Ключ
1	ДОБРИЙ РАНОК	ЯБЛУКО
2	ВАЖКА СПРАВА	ФОРЕЛЬ
3	У НЕДІЛЮ СЬОМОГО	ЯКОР
4	ЗАВТРА ВРАНЦІ	КЛЮЧ
5	ДОПОМОГА ПРИЙДЕ	ДИПЛОМ

№ вар	Повідомлення	Ключ
6	ЧЕКАЙТЕ ПРИЇЗДУ	СЕЗОН
7	СПРАВУ ЗАКІНЧЕНО	ЛЕМОН
8	ЗАЛИШАЙТЕСЬ НА МІСЦІ	БЛИСК
9	ВАЖКИЙ ІСПИТ	БРАТ
10	НЕСПОДІВАНА ЗУСТРІЧ	МОРЕ
11	ТРИВАЛЕ ВІДРЯДЖЕННЯ	КНИГА
12	ЗАГАЛЬНІ ЗБОРИ	ЯБЛУКО
13	ШВИДКИЙ ПОРЯТУНОК	ФОРЕЛЬ
14	ОСТАННЯ НАДІЯ	ЯКОР
15	ЧЕКАТИ ЗВІСТКИ	КЛЮЧ
16	ЗАЛИШИТЬ МІСТО	ДИПЛОМ
17	РЯТУВАТИ МАЙНО	СЕЗОН
18	ВІДШКОДУВАТИ ВТРАТИ	ЛЕМОН
19	КІЛЬКОРАЗОВЕ ШИФРУВАННЯ	БЛИСК
20	КРИПТОГРАФІЯ	БРАТ
21	КРИПТОСИСТЕМА	МОРЕ
22	ШИФР ВІЖЕНЕРА	КНИГА
23	ДОБРИЙ ВЧИНОК	СЕЗОН
24	МІСТО ЗУСТРІЧІ	ЛЕМОН
25	ВАЖКА СПРАВА	БЛИСК
26	У НЕДІЛЮ СЬОМОГО	БРАТ
27	ЗАВТРА ВРАНЦІ	МОРЕ
28	ДОПОМОГА ПРИЙДЕ	КНИГА
29	ЧЕКАЙТЕ ПРИЇЗДУ	ЯБЛУКО
30	СПРАВУ ЗАКІНЧЕНО	ФОРЕЛЬ

Практичне заняття 2

Математичні алгоритми, які найчастіше використовуються в криптографії

Теоретичні відомості

Розглянемо математичні алгоритми, які найчастіше використовуються в криптографічних протоколах.

Алгоритм Евкліда

Нагадаємо, що два числа називають взаємнопростими, якщо вони не мають спільних дільників, крім 1. Іншими словами, якщо найбільший спільний дільник чисел a і n дорівнює 1, то ці числа називають взаємнопростими і записують $НСД\ (a, n) = 1$.

Один з шляхів обчислення найбільшого спільного дільника двох чисел – використання алгоритму Евкліда. Евклід описав цей алгоритм у своїй книзі „Елементи", датованій 300 роком до н. е.

Однак алгоритм був створений не Евклідом. Історики вважають, що алгоритм на 200 років старіше. Це найдавніший нетривіальний алгоритм, що дійшов до наших днів.

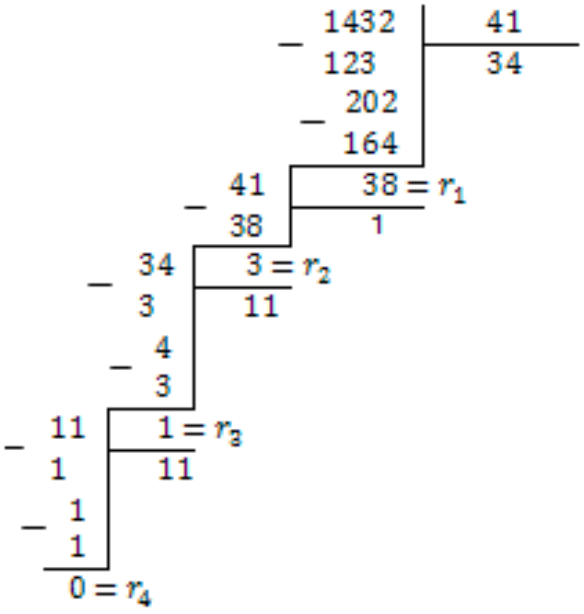
Будемо позначати найбільший спільний дільник чисел A і B через (A,B). Нагадаємо, що алгоритм Евкліда полягає у послідовному виконанні операції ділення із залишком до отримання нульового залишку.

Нехай $A > B > 0$. Позначимо $A = r_{-1}$, $B = r_0$ і $r_{i-2} = d_i r_{i-1} + r_i$ при $i = 1, \ldots, k$ і $r_{k-1} = d_{k+1} r_k$. Тоді $(A, B) = r_k$ і до отримання залишку $r_{k+1} = 0$ необхідно виконати $k + 1$ ділення.

Можна також відмітити, що алгоритм Евкліда широко використовується не тільки при визначенні найбільших спільних дільників чисел, але й поліномів. А саме, у теорії подільності його використовують при тестуванні взаємної простоти двох поліномів з коефіцієнтами, наприклад, з кінцевого поля.

Приклад

Знайти найбільший спільний дільник чисел 1432 та 41.



Останній ненульовий залишок дорівнює 1, тому НСД (1432,41)=1. Тобто ці числа взаємнопрості.

Розширений алгоритм Евкліда

Розглянемо алгоритм, що дозволяє не тільки знаходити *НСД* чисел A і B, а ще й знаходити цілі числа x і y , що задовольняють рівності $Ax + By = (A, B)$.

Від звичайного алгоритму Евкліда він відрізняється тим, що разом з послідовністю залишків r_i обчислюються ще дві допоміжні послідовності x_i і y_i.

Сам алгоритм можна подати таким чином:

$r_{-1} = A;\ r_0 = B$

$x_{-1} = 1;\ y_{-1} = 0;\ x_0 = 0;\ y_0 = 1$

for $i = 1$ *until* $r_i > 0$ *do*

begin

$d_i = \lfloor r_{i-2} / r_{i-1} \rfloor;$

$r_i = r_{i-2} - d_i r_{i-1};$

$x_i = x_{i-2} - d_i x_{i-1};$

$y_i = y_{i-2} - d_i y_{i-1};$

$i = i + 1;$

end

Приклад

Потрібно вирішити за допомогою розширеного алгоритму Евкліда діофантове рівняння вигляду *18x +27y = НСД (18,27)*

1. $r_{-1} = 18; r_0 = 27$

$x_{-1} = 1; y_{-1} = 0; x_0 = 0; y_0 = 1$

$d_1 = \lfloor r_{-1} / r_0 \rfloor = \lfloor 18 / 27 \rfloor = 0$

$r_1 = r_{-1} - d_1 r_0 = 18 - 0 \times 27 = 18$

$x_1 = x_{-1} - d_1 x_0 = 1 - 0 \times 0 = 1$

$y_1 = y_{-1} - d_1 y_0 = 0 - 0 \times 1 = 0$

2. $d_2 = \lfloor r_0 / r_1 \rfloor = \lfloor 27 / 18 \rfloor = 1$

$r_2 = r_0 - d_2 r_1 = 27 - 1 \times 18 = 9$

$x_2 = x_0 - d_2 x_1 = 0 - 1 \times 1 = -1$

$y_2 = y_0 - d_2 y_1 = 1 - 1 \times 0 = 1$

3. $d_3 = \lfloor r_1 / r_2 \rfloor = \lfloor 18 / 9 \rfloor = 2$

$r_3 = r_1 - d_3 r_2 = 18 - 2 \times 9 = 0$

Дійсно, знайдені числа *x* та *y*, що задовольняють рівності

НСД(18,27)=9

18 ×(-1) +27× 1 = НСД (18,27)

Також можна вирішувати такі рівняння методом ланцюгових дробів. Напом'ятовуємо.

Ланцюговим або неперервним дробом називається вираз

$$a + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ldots + \cfrac{1}{a_n}}}} \qquad (2.1)$$

де a – ціле число, a $a_1, a_2, \ldots, a_n$ – натуральні числа.

Для зручності запису ланцюговий дріб (2.1) можна позначати і так:

$(a; a_1, a_2, a_3, \ldots, a_n)$.

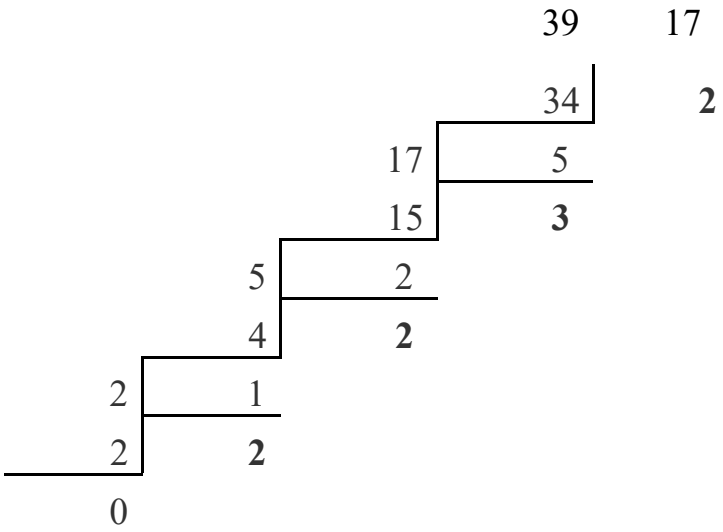
Отже, можемо записати

$$\frac{39}{17} = 2 + \cfrac{1}{3 + \cfrac{1}{2 + \cfrac{1}{2}}}.$$

Це – зображення нескоротного звичайного дробу ланцюговим дробом.

Таке зображення для довільного нескоротного дробу будується наступним чином.

Будемо шукати *НСД* (39,17) .



Бачимо, що числа 2, 3, 2 та 2, за допомогою яких побудовано ланцюговий дріб, є послідовними частками в алгоритмі Евкліда.

У цьому записі ціле число відділяється крапкою з комою, а інші числа – комами.

Ланцюгові дроби використовуються для розв’язування діофантових рівнянь.

Приклад

Розв’язати у цілих числах рівняння

$$15x + 28y = 185.$$

Розв’язання

Розкладемо $\frac{28}{15}$ у ланцюговий дріб:

$$\frac{28}{15}=1+\frac{1}{\frac{15}{13}}=1+\frac{1}{1+\frac{1}{\frac{13}{2}}}=1+\frac{1}{1+\frac{1}{6+\frac{1}{2}}}.$$

Передостаннє наближення – це

$$1+\frac{1}{1+\frac{1}{6}}=\frac{13}{7}.$$

Знайдемо різницю:

$$\frac{28}{15}-\frac{13}{7}=\frac{28\cdot 7-15\cdot 13}{7\cdot 15}=\frac{1}{7\cdot 15}.$$

Звідси

$$28\cdot 7-13\cdot 15=1$$
$$15\cdot(-13)+28\cdot 7=1$$
$$15\cdot(-13)\cdot 185+28\cdot 7\cdot 185=185.$$

Отже

$$x=-13\cdot 185+28t,\quad y=7\cdot 185-15t;$$
$$x=-2405+28t,\quad y=1295-15t.$$

Замість t підставимо t+86. Тоді

$$x=-2405+28t+2408,\quad y=1295-15t-1290;$$
$$x=3+28t,\quad y=5-15t,\quad t\in Z.$$

Відповідь:

$$x=3+28t,\quad y=5-15t\quad де\quad t\in Z.$$

Алгоритм Монтгомері

Ефективний шлях багаторазового приведення за модулем – використання методу Монтгомері, який було запропоновано в 1985 році. Цей метод особливо ефективний при апаратній реалізації алгоритмів. Дуже зручно відмовитися від

операцій множення і ділення та замінити їх операціями додавання. Метод полягає в наступному.

Нехай N - непарне число, потрібно помножити лишки

$$A = \sum_{i=0}^{n-1} 2^i a_i \text{ і } B.$$

Розглянемо алгоритм:

R = 0;

for i = 0 until i < n do

begin

if a_i = 1 then R = R + B;

if R – непарне then R = R + N;

R = R / 2;

end

if R ≥ N then R = R – N.

Суть даного алгоритму полягає в тім, що в силу рівності

$$\text{A} = \sum_{i=0}^{n-1} 2^i a_i = (\ldots(2a_{n-1} + a_{n-2})2 + \ldots + a_1)2 + a_0$$

Тобто множення числа B на число A зводиться до обчислення

$$AB = a_0 B + 2(a_1 B + \ldots 2(a_{n-2} B + 2a_{n-1} B)\ldots).$$

Воно виконується за n кроків, на кожнім з яких здійснюється додавання до поточного значення R значення $a_i B$, $i = 0, \ldots, n-1$, з наступним діленням на 2. Завдяки цьому діленню отримані значення завжди знаходяться в інтервалі $0 < R < N$.

У результаті роботи даного алгоритму виходить число $2^{-n} AB \ (mod\, N)$. Тепер для одержання числа $AB \ (mod\, N)$ необхідно застосувати ще один раз даний алгоритм до чисел $2^{2n} (mod\, N)$ і $2^{-n} AB (mod\, N)$.

Оскільки число $2^{2n} (mod\, N)$ обчислюється за допомогою зрушень і вирахувань, його можна обчислити заздалегідь і зберігати отримане значення).

Наприклад

Нехай $\boldsymbol{A} = 27 = 1\times2^0 + 1\times2^1 + 0\times2^2 + 1\times2^3 + 1\times2^4 = 1 + 2 + 8 + + 16 = (11011)$

$\boldsymbol{B} = \mathbf{16}$

$\boldsymbol{N} = \mathbf{41}$

Зрозуміло, що $AB(\text{mod N}) = 27\times16\ (\text{mod } 41) = 432(\text{mod } 41) = 22$

Обчислимо добуток цих чисел за допомогою вищевказаного алгоритму.

1. $R = 0$

   $a_0 = 1$

   $R = R + B = 0 + 16 = 16;$

   R – парне;

   $R = R / 2 = 8.$

2. $a_1 = 1;$

   $R = R + B = 8 + 16 = 24;$

   R - парне;

   $R = R / 2 = 12;$

3. $a_2 = 0$

   R - парне;

   $R = R / 2 = 6;$

4. $a_3 = 1;$

   $R = R + B = 6 + 16 = 22;$

   R - парне;

   $R = R / 2 = 11;$

5. $a_4 = 1$

   $R = R + B = 11 + 16 = 27;$

   R – непарне;

   $R = R + N = 27 + 41 = 68;$

   R – парне;

   $R = R / 2 = 34;$

   $R < N \rightarrow R = 34.$

Це ми одержали $2^{-n}\,AB(\text{mod } N)$.

Тепер ми повинні ще раз скористатися цим алгоритмом для обчислення AB (mod N).

$\boldsymbol{A'} = 2^{2n} (\text{mod N}) = 2^{2\times5} (\text{mod N}) = 1024 (\text{mod } 41) = 40 = 0\times2^0 + 0\times2^1 + 0\times2^2 + 1\times2^3 + 0\times2^4 + 1\times2^5$

$\boldsymbol{B'} = 34;$

$\boldsymbol{N} = 41.$

1. $R = 0$

   $a_0 = 0$

   R – парне;

   $R = R / 2 = 0.$

2. $a_1 = 0;$

   R – парне;

   $R = R / 2 = 0;$

3. $a_2 = 0$

   R – парне;

   $R = R / 2 = 0;$

4. $a_3 = 1;$

   $R = R + B = 0 + 34 = 34;$

   R – парне;

   $R = R / 2 = 17;$

5. $a_4 = 0;$

   R – непарне;

   $R = R + N = 17 + 41 = 58;$

   $R = R / 2 = 27;$

6. $a_5 = 1;$

   $R = R + B = 27 + 34 = 63;$

   $R = R - N = 63 - 41 = 22.$

Перевірка показує, що рішення вірне.

Треба ще відмітити, що для коректної роботи алгоритму потрібно, щоб число ділень при першому і другому проході алгоритму було однаковим. Як видно другий раз це теж було 5 ділень!

Завдання до практичного заняття 2

Завдання 1.

За допомогою розширеного алгоритму Евкліда знайти цілі числа x та y, які задовольняють рівнянню $Ax + By = (A, B)$. Рівняння надані у таблиці 2.1.

Таблиця 2.1

Вариант (номер у журналі)	**Рівняння**
1	$3x + 4y = \text{НОД}(3,4)$
2	$3x + 7y = \text{НОД}(3,7)$
3	$5x + 3y = \text{НОД}(3,5)$
4	$2x + 3y = \text{НОД}(2,3)$
5	$2x + 5y = \text{НОД}(2,5)$
6	$2x + 7y = \text{НОД}(2,7)$
7	$2x + 9y = \text{НОД}(2,9)$
8	$5x + 13y = \text{НОД}(5,13)$
9	$10x + 11y = \text{НОД}(10,11)$
10	$13x + 12y = \text{НОД}(12,13)$
11	$2x + 4y = \text{НОД}(2,4)$
12	$4x + 8y = \text{НОД}(4,8)$
13	$5x + 10y = \text{НОД}(5,10)$
14	$2x + 11y = \text{НОД}(2,11)$
15	$3x + 12y = \text{НОД}(3,12)$
16	$7x + 12y = \text{НОД}(7,12)$
17	$5x + 12y = \text{НОД}(5,12)$
18	$11x + 12y = \text{НОД}(11,12)$
19	$3x + 16y = \text{НОД}(3,16)$
20	$8x + 17y = \text{НОД}(8,17)$
21	$7x + 15y = \text{НОД}(7,15)$
22	$9x + 19y = \text{НОД}(9,19)$
23	$11x + 17y = \text{НОД}(11,17)$
24	$10x + 15y = \text{НОД}(10,15)$
25	$16x + 8y = \text{НОД}(16,8)$

Завдання 2.

За допомогою алгоритму Монтгомері знайти добуток чисел $A \times B (\mathrm{mod}\, N)$. Дані надані у таблиці 2.2 у залежності від номеру у журналі.

Таблиця 2.2

Вариант (номер у журналі)	A	B	N
1	21	18	37
2	19	16	37
3	23	18	37
4	25	16	37
5	25	18	37
6	21	16	41
7	27	20	41
8	25	20	41
9	27	18	41
10	29	16	41
11	21	14	29
12	21	16	29
13	21	12	29
14	19	16	29
15	19	14	29
16	27	18	31
17	27	20	31
18	27	16	31
19	27	14	31
20	25	16	31
21	33	18	47
22	33	16	47
23	35	18	47
24	35	16	47

Практичне заняття 3

Основні типи перетворень, що використовуються в перспективних симетричних криптосистемах

Теоретичні відомості

Розглянем перетворення Bitesub алгоритму AES.

Bitesub (заміна байтів) – це два табличних перетворення, здійснюються над байтами послідовно по стовпцях.

1. Перше перетворення здійснюється засобом заміни a_{ij} байта на a_{ij}^{-1} обернений, що досягається розв'язком порівняння:

$$a_{ij} \cdot a_{ij}^{-1} \equiv 1(mod(x^8 + x^4 + x^3 + x + 1)). \quad (3.1)$$

2. Друге табличне перетворення кожного байта здійснюється як афінне:

$$Y = (C \cdot x + C_1)\, mod \quad (x^8 + 1), \quad (3.2)$$

де C, C_1 - константи, що мають вигляд:

$$C = \begin{vmatrix} 10001111 \\ 11000111 \\ 11100011 \\ 11110001 \\ 11111000 \\ 01111100 \\ 00111110 \\ 00011111 \end{vmatrix}, \quad C_1 = \begin{vmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{vmatrix},$$

$x = (x_0 x_1 x_2 x_3 x_4 x_5 x_6 x_7)$ - біти a_{ij}^{-1} байта.

В сукупності (3.1) та (3.2) задають деяку нелінійну підстановку типу байт в байт. Тому реально в алгоритмі перетворення (3.1) та (3.2) не виконуються, а задаються фіксованою таблицею підстановки.

Приклад

Знайти афінне перетворення виду $a_{ij}^{'} = C \cdot a_{ij}^{-1} + C_1$, де C та C_1 - константи, що мають вигляд:

$$C = \begin{vmatrix} 11111000 \\ 01111100 \\ 00111110 \\ 00011111 \\ 10001111 \\ 11000111 \\ 11100011 \\ 11110001 \end{vmatrix} \qquad C_1 = \begin{vmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{vmatrix}$$

При цьому $a_{ij} \cdot a_{ij}^{-1} \equiv 1(mod(x^8 + x^4 + x^3 + x + 1))$, якщо $a_{ij} = 71$.

Знайти відстань Хемінга між вхідними та вихідними елементами.

Розв′язок

Знайдемо a_{ij}^{-1}. Для цього зведемо розв'язок порівняння

$a_{ij} \cdot a_{ij}^{-1} \equiv 1(mod(x^8 + x^4 + x^3 + x + 1))$ до розв'язку порівняння виду

$ax + by = 1$. Це не що інше як Діофантове рівняння.

Перепишемо порівняння алгоритму у вигляді:

$(-k) \cdot \phi(N) + a_{ij} \cdot a_{ij}^{-1} = 1,$

де $b = a_{ij} = 71, \quad a = \phi(N) = x^8 + x^4 + x^3 + x + 1.$ В умовах Діофантового рівняння треба знайти $y = a_{ij}^{-1}$ та $x = (-k)$. Але в умовах задачі нас цікавить тільки $y = a_{ij}^{-1}$.

Діофантове рівняння має розв'язок, якщо $\varphi(N) \geq E_k$ та $((\varphi(N), E_k) = 1$.

Розглянемо два методи вирішення Діофантового рівняння.

1. За допомогою розширеного алгоритму Евкліда

Надаємо цей розв'язок у вигляді ланцюгового дробу. Для цього запишемо $a_{ij} = 71$ у вигляді поліному: $a_{ij} = 01000111 = x^6 + x^2 + x + 1$.

Тоді наш ланцюговий дріб матиме вигляд:

$$\frac{x^8 + x^4 + x^3 + x + 1}{x^6 + x^2 + x + 1} = x^2 + \frac{x^2 + x + 1}{x^6 + x^2 + x + 1};$$

$$\frac{x^6 + x^2 + x + 1}{x^2 + x + 1} = (x^4 + x^3 + x) + \frac{1}{x^2 + x + 1}.$$

$$a_0 = r_0 = x^2; \quad b_0 = 1;$$

$$a_1 = r_0 r_1 + 1 = x^2(x^4 + x^3 + x) + 1 = x^6 + x^5 + x^3 + 1;$$

$$b_1 = r_1 = x^4 + x^3 + x.$$

Тоді, якщо μ – порядок ланцюгового дробу, а a, b – його параметри, то

$$\left.\begin{matrix} y = (-1)^{\mu} a_{\mu-1} = (-1)^2 \cdot a_1 = x^6 + x^5 + x^3 + 1 \\ x = (-1)^{\mu} b_{\mu-1} = (-1)^2 \cdot b_1 = x^4 + x^3 + x. \end{matrix}\right\}$$

Отже , $a_{ij}^{-1} = y = x^6 + x^5 + x^3 + 1 = 01101001_2 = 105_{10}$.

Перевірку правильності розв'язку рівняння виконуємо, підставивши значення a_{ij} та a_{ij}^{-1} в $a_{ij} \cdot a_{ij}^{-1} \equiv 1(mod(x^8 + x^4 + x^3 + x + 1))$. Маємо

$$(x^6 + x^2 + x + 1)(x^6 + x^5 + x^3 + 1) = 1(mod(x^8 + x^4 + x^3 + x + 1)).$$

Дійсно

$(x^6 + x^2 + x + 1)(x^6 + x^5 + x^3 + 1)(mod(x^8 + x^4 + x^3 + x + 1) = x^{12} + x^{11} + +x^9 + x^6 + x^8 + x^7 + x^5 + x^2 + x^7 + x^6 + x^4 + x + x^6 + x^5 + x^3 + 1(mod(x^8 + +x^4 + x^3 + x + 1))$.

Знайдемо залишок:

$$\begin{array}{l|l} x^{12} + x^{11} + x^9 + x^8 + x^2 + x^4 + x + x^6 + x^3 + 1 & x^8 + x^4 + x^3 + x + 1 \\ \underline{x^{12} + x^8 + x^7 + x^5 + x^4} & \\ x^{11} + x^9 + x^7 + x^6 + x^5 + x^3 + x^2 + x + 1 & \\ \underline{x^{11} + x^7 + x^6 + x^4 + x^3} & \\ x^9 + x^5 + x^4 + x^2 + x + 1 & \\ \underline{x^9 + x^5 + x^4 + x^2 + x} & \\ 1 & \end{array}$$

Таким чином, лишок =1. Елементи $x^6 + x^2 + x + 1$ та $x^6 + x^5 + x^3 + 1$ є зворотними.

Знайдемо афінне перетворення $a_{ij}^{'} = C \cdot a_{ij}^{-1} + C_1$. Для цього запишемо $a_{ij}^{'} = 01101001$ у вигляді матриці-стовпця:

$$a_{ij}^{-1} = \begin{vmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{vmatrix}.$$

Позначимо $C *= C \cdot a_{ij}^{-1}$:

$$C *= \begin{vmatrix} 11111000 \\ 01111100 \\ 00111110 \\ 00011111 \\ 10001111 \\ 11000111 \\ 11100011 \\ 11110001 \end{vmatrix} \cdot \begin{vmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{vmatrix} = \begin{vmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{vmatrix};$$

Тепер знайдемо $a_{ij}^{'} = C * + C_1$:

$$a_{ij}^{'} = \begin{vmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{vmatrix} \oplus \begin{vmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{vmatrix} = \begin{vmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{vmatrix}$$

Отже, $a_{ij}^{-1} = 11111010_2 = 250_{10}$.

2. Методом підхідних дробив

Знайдемо a_{ij}^{-1}. Для цього зведемо розв'язок порівняння

$a_{ij} \cdot a_{ij}^{-1} \equiv 1(mod(x^8 + x^4 + x^3 + x + 1))$ до розв'язку порівняння виду $ax + by = 1$. Це Діофантове рівняння.

Перепишемо, як і в першому способі рішення, порівняння алгоритму у вигляді:$(-k) \cdot \phi(N) + a_{ij} \cdot a_{ij}^{-1} = 1$, де $b = a_{ij} = 71$,

$a = \phi(N) = x^8 + x^4 + x^3 + x + 1$. В умовах Діофантового рівняння треба знайти $y = a_{ij}^{-1}$ та $x = (-k)$. Але в умовах задачі нас цікавить тільки $y = a_{ij}^{-1}$.

Діофантове рівняння має розв'язок, якщо $\varphi(N) \geq E_k$ та $((\varphi(N), E_k) = 1$.

Напам'ятовуємо теорему з теорії чисел.

Загальне рішення у цілих числах порівняння вигляду $ax + by = c$. Де a, b, c – цілі числа, а *НСД* (a, b)=1 можна надати у вигляді:

$$\begin{cases} x = (-1)^{n-1} \cdot c \cdot B_{n-1} + bt \\ y = (-1)^n \cdot c \cdot A_{n-1} - at \end{cases},$$

де t – довільне ціле число;

A_{n-1}, B_{n-1} – чисельник і знаменник передостаннього підхідного дробу при розкладанні числа $\frac{a}{b}$ у ланцюговий дріб.

Зауважимо наступне:

- ми працюємо у двійковому полі;
- c у нашому випадку дорівнює 1;
- нас цікавить найменше позитивне рішення;
- в умовах задачі нас цікавить тільки $y = a_{ij}^{-1}$.

Шукаємо $y = a_{ij}^{-1} = A_{n-1}$.

Знайдемо чисельник передостаннього підхідного дробу при розкладанні числа $\frac{a}{b}$ у ланцюговий дріб.

Відокремлюємо цілі частини. Для $a_{ij} = 71$.

$$71 = 64 + 4 + 2 + 1 = 2^6 + 2^2 + 2^1 + 2^0.$$

Замінюємо двійку у цьому запису на x.

Отримуємо $2^6 + 2^2 + 2^1 + 2^0 = x^6 + x^2 + x + 1$. Це багаточлен, який у двійковому полі відповідає числу 71 за варіантом.

Розкладаємо $\frac{a}{b}$ у ланцюговий дріб.

$$\frac{a}{b} = \frac{x^8+x^4+x^3+x+1}{x^6+x^2+x+1}$$

$$\begin{array}{l|l} x^8+x^4+x^3+x+1 & x^6+x^2+x+1 \\ \hline x^8+x^4+x^3+x^2 & x^2 \quad = q_0 \\ \hline x^2+x+1 & \end{array}$$

Тобто можна записати:

$$\frac{x^8+x^4+x^3+x+1}{x^6+x^2+x+1} = x^2 + \frac{x^2+x+1}{x^6+x^2+x+1}.$$

Далі перегортаємо дріб і продовжуємо ділення:

$$\begin{array}{l|ll} x^6+x^2+x+1 & x^2+x+1 & = q_2 \\ \hline x^6+x^5+x^4 & x^4+\ x^3+x & = q_1 \\ \hline x^5+x^4+x^2+x+1 & & \\ \hline x^5+x^4+x^3 & & \\ \hline x^3+\ x^2+x+1 & & \\ \hline x^3+\ x^2+x & & \\ \hline 1 & & \end{array}$$

Отримали 1 у остачі. Ділення закінчене.

Можна записати:

$$\frac{x^6+x^2+x+1}{x^2+x+1} = (x^4+x^3+x) + \frac{1}{x^2+x+1}.$$

Знаходимо чисельники і знаменники підхідних дробив.

Для спрощення рішення заповнимо таблицю 3.1.

Таблиця 3.1

q_i	q_{-1}	q_0=x^2	$q_1 = x^4+\ x^3+x$	$q_2 = x^2+x+1$
A_i		$\boldsymbol{A_0 = q_0 = x^2}$	$A_1 = x^6+\ x^5+x^3+1$	A_2=$x^8+x^4+x^3+x+1$
B_i		$\boldsymbol{B_0 = 1}$	…	…

У цій таблиці жирним відмічені результати записані за властивостями підхідних дробів. Тобто A_{-1} завжди 1, B_{-1} завжди – 0. $A_0 = q_0$. B_0 - завжди – 1.

А далі розрахунки проводять згідно з формулами:

$$A_s = q_s \cdot A_{s-1} + A_{s-2}$$
$$B_s = q_s \cdot B_{s-1} + B_{s-2}$$

Тобто:

$A_1 = q_1 \cdot A_0 + A_{-1}$=$(x^4 + x^3 + x)\cdot x^2+1= x^6 + x^5 + x^3 + 1$;

$A_2 = q_2 \cdot A_1 + A_0$=$(x^2 + x + 1)\cdot (x^6 + x^5 + x^3 + 1) + x^2 = x^8 + x^4 + +x^3 + x + 1$.

Причому у таблиці заповнено тільки перший рядок, так як в умовах задачі нас цікавить тільки $y = a_{ij}^{-1} = A_{n-1}$. Останнє $A = A_2 = x^8 + x^4 + x^3 + +x + 1$ підраховане для перевірки. Воно повинно дорівнювати модуля перетворення. У нас все співпало. Перетворення виконане правильно.

Знайдено мультиплікативно зворотній елемент до числа 71 за модулем $x^8 + x^4 + x^3 + x + 1$. Це $y = a_{ij}^{-1} = A_{n-1} = A_1 = x^6 + x^5 + x^3 + 1 = 2^6 + 2^5 + 2^3 + 1 = 105$.

Далі знайдемо афінне перетворення $a_{ij}^{'} = C \cdot a_{ij}^{-1} + C_1$ таким чином, як робили раніше. Тобто ми отримуємо $a_{ij}^{'} = C \cdot a_{ij}^{-1} + C_1 = 11111010_2 = 250_{10}$.

Завдання до практичного заняття 3

Завдання 1.

Знайти афінне перетворення $a_{ij}^{'} = C \cdot a_{ij}^{-1} + C_1$, де C та C_1 - константи, що мають вигляд:

$$C = \begin{vmatrix} 11111000 \\ 01111100 \\ 00111110 \\ 00011111 \\ 10001111 \\ 11000111 \\ 11100011 \\ 11110001 \end{vmatrix}, \qquad C_1 = \begin{vmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{vmatrix}$$

При цьому $a_{ij} = a_{ij}^{-1} \equiv 1(\mathrm{mod}(x^8 + x^4 + x^3 + x + 1))$, якщо $a_{ij} = 99 + 3k$, де k - номер у журналі.

Практичне заняття 4

Класичні криптосистеми з відкритим ключем

Теоретичні відомості

Кардинальна відмінність криптосистеми з відкритим ключем полягає в тому, що в криптосистемах з відкритим ключем процедура шифрування стає загальнодоступною.

Це, однак, не означає як у традиційних системах шифрування, що загальнодоступною є й процедура розшифрування. Поняття ключа розбивається на дві частини (включає тепер два поняття): ключ відкритий, і ключ таємний.

Загальнодоступний відкритий ключ використовується для шифрування, але розшифрування може здійснити тільки той, хто володіє таємним ключем.

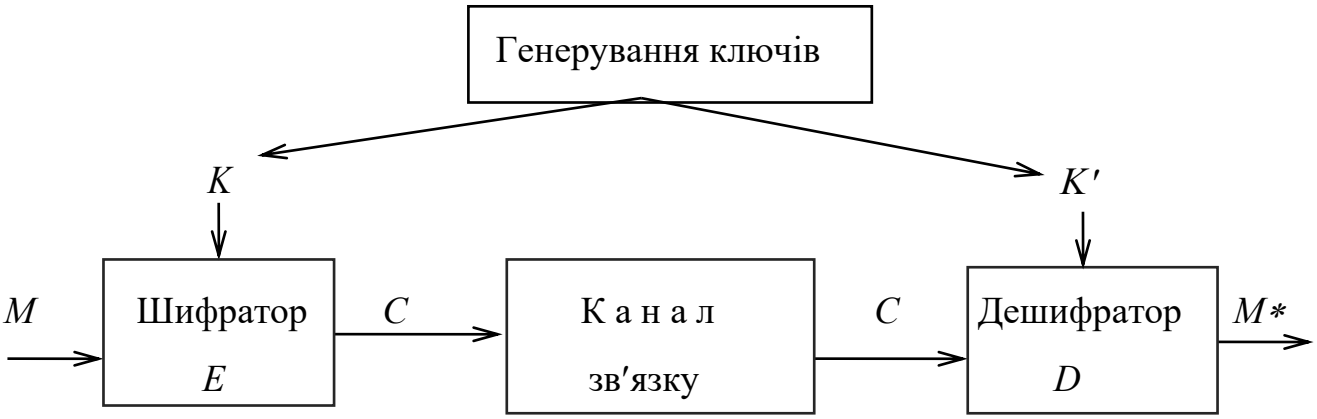


Рис.4.1 – Нова криптографічна схема захищеної передачі інформації

- Алфавіт A, у якому записуються повідомлення (відкриті тексти), і алфавіт B, у якому записуються криптотексти.

- Простір ключів K (безліч слів у деякому алфавіті).

- Алгоритм генерування ключів. Це поліноміальний (ефективний) імовірнісний алгоритм, що видає (дозволяє сформувати) випадкову пару $K, K' \in \boldsymbol{K}$.

Компонента K називається відкритим ключем і використовується для шифрування, а компонента K' називається таємним ключем і використовується для розшифрування.

- Поліноміальний (ефективний) детермінований алгоритм шифрування E, що одержує на вхід повідомлення M й відкритий ключ K, а видає криптотекст C, що записується як $C = E_k(M)$.

- Поліноміальний (ефективний) детермінований алгоритм розшифрування D, що одержує на вхід криптотекст C і секретний ключ

K', а видає відкритий текст M, що записуємо як $M = D_{K'}(C)$.

Перераховані алгоритми задовольняють таким умовам:

- Якщо пара (K, K') породжена алгоритмом генерування ключів, то з криптотексту $C = E_k(M)$ можна отримати відкрите повідомлення $M = D_{K'}(C)$ для будь - якого відкритого тексту M.

- Немає (або, принаймні, невідомо) хоча б одного ефективного алгоритму, який би по відомим $C = E_k(M)$ і K знаходив би M.

Остання умова забезпечує надійність криптосистеми навіть тоді, коли з відкритого ключа K не робиться секрету. Із цієї умови витікає, зокрема, що пари (K, K') могли б були породжені алгоритмом генерування ключів.

Криптосистеми з відкритим ключем ще називають й асиметричними.

Криптосистема шифрування RSA

Ця система запропонована в 1977 році, і є однією з найвідоміших криптосистем з відкритим ключем. Назва системи утворена з перших букв імен її творців (Рональда Райвеста, Ади Шаміра й Леонарда Адлемана).

Генерування ключів

Вибирають два досить великих простих числа p і q. Для їхнього добутку $n = pq$ функція Ойлера дорівнює $\varphi(n) = (p-1)(q-1) = n - p - q + 1$ (у теорії чисел використовується поняття функції Ойлера $\varphi(m)$, під якою розуміється число чисел менш ніж m і взаємно простих з m).

Потім випадковим чином обирають число *e*, що не перевищує значення $\varphi(n)$ й взаємнопросто з ним. Для цього з числа *e* за допомогою розширеного алгоритму Евкліда знаходять елемент *d*, зворотний до *e*, тобто такий, що $d < \varphi(n)$ й

$$ed \equiv 1(\mathrm{mod}\,\varphi(n)). \qquad (4.1)$$

Цей запис у теорії чисел позначає що добуток ed при діленні на число $\varphi(n)$ дає залишок рівний 1 (читається добуток ed порівняно з одиницею за модулем $\varphi(n)$.

У результаті полагають:

Як відкритий ключ пара чисел e й n.

В якості таємного ключа – число d.

Також числа p і q неможна відкривати.

Шифрування

Здійснюється блоками. Для цього повідомлення записують у цифровому вигляді й розбивають на блоки так, що кожен блок представляє число, що не перевищує n.

Скажемо, якщо блок *M* записаний у двійковій формі довжини m, то повинне виконуватися умова $2^m < n$.

Алгоритм шифрування *E* в системі RSA складається у зведенні двійкового числа *M* у степінь e. Запишемо це так

$$E(M) = M^e (\mathrm{mod}\, n)$$

У результаті виходить блок криптотексту $C = E(M)$.

Розшифрування

Алгоритм розшифрування D блоку криптотексту C складається у зведенні числа C в степінь d, тобто

$$D(C) = C^d (\mathrm{mod}\, n).$$

Приклад

Показати роботу алгоритму шифрування RSA, якщо обрані прості числа

$p = 23$ й $q = 17$. Повідомлення ПОЧАТИ. Треба це повідомлення зашифрувати і розшифрувати. Всі додаткові параметри обрати за умовами алгоритму самостійно.

Нехай $p = 23$ й $q = 17$. Тоді $n = 391$ й $\varphi(n) = 352$. Візьмемо $e = 13$. Можна перевірити, що *НСД*(13,352)=1. Одночасно обчислюємо $d = 13^{-1}(mod\ 352) = 325$. Ключі знайдені.

Відкритий ключ $e = 13$ й $n = 391$ опубліковуємо. Припустимо, що один з ділових партнерів вирішив послати нам вказівку ПОЧАТИ .

Спочатку він перетворить своє повідомлення до цифрового виду, замінивши кожну букву її цифровим десятковим номером в алфавіті 19 18 27 0 22 10 (тут нумерація букв алфавіту починається з нуля). Видно, що для нашого модуля $n = 391$ цифрове повідомлення доцільно розбивати на блоки по 2 цифри, тобто 19 18 27 0 22 10.

При шифруванні перший блок перетвориться в число$19^{13}(mod\ 391) = 168$. У такий же спосіб шифруються й інші блоки, і в результаті виходить шифртекст 168 ... .

Розшифрування цієї шифрограми виконується зведенням кожного блоку в степінь $d = 325$ за модулем $n = 391$ Легко перевірити, що $168^{325}(\ mod\ 391) = 19$ й т.д.

Алгоритм цифрового підпису RSA

Першою і найбільш відомою у всьому світі конкретною системою ЕЦП стала система RSA , математичну схему якої було розроблено у 1977 році в Массачуссетському технологічному інституті.

Генерація ключів

Для того, щоб згенерувати пари ключів виконуються наступні дії:

- вибираються два великих простих числа *p* та *q*;
- обчислюється їх добуток (модуль) *n=p q*;
- обчислюється функція Ойлера *φ(n)=(p-1)(q-1)* ;

- вибирається ціле e таке, що $1 < e < \varphi(n)$ та e взаємно просте з $\varphi(n)$;

- за допомогою розширеного алгоритма Евкліда знаходиться число d таке, що $e\,d \equiv 1 \pmod{\varphi(n)}$.

Число n називається модулем, а числа e і d — відкритою й секретною експонентами, відповідно. Пари чисел (n, e) є відкритою частиною ключа, а (p, q, d) — секретною. Числа p і q після генерації пари ключів можуть бути знищені, але в жодному разі не повинні бути розкриті.

Підпис S повідомлення з хеш – функцією m обчислюється з використанням секретного ключа за формулою:

$$s = m^d (mod\ n).$$

Для перевірки правильності підпису потрібно переконатися, що виконується рівність

$$m = s^e (mod\ n).$$

Приклад

Показати роботу алгоритму електронного цифрового підпису RSA, якщо обрані прості числа $p = 19$ й $q = 13$. Хеш значення повідомлення характеризується числом $h(M) = m = 3$. Додаткові параметри обрати самостійно за умовами алгоритму.

Розрахуємо модуль $n = p \cdot q = 19 \cdot 13 = 247$ та значення функції Ойлера $\varphi(n) = (p-1)(q-1) = 216$.

Візьмемо $e = 7$. Можна перевірити, що *НСД*(7,247)=1. Одночасно обчислюємо $d = 7^{-1} (mod\ 216) = 31$. Ключі знайдені.

Відкриті параметри: відкритий ключ $e = 7$ та модуль $n = 247$.

Секретні параметри: таємний ключ $d = 31$, та числа $p = 19$ та $q = 13$.

Накладаємо цифровий підпис на хеш функцію за допомогою таємного ключа: $s = m^d (mod\ n) = 3^{31} (mod\ 247) = 185$.

Перевіряємо підпис за допомогою відкритого ключа:

$m = s^e (mod\ n) = 185^7 (mod\ 247) = 3$.

Все вірно.

Криптосистема Ель- Гамала

Генерування ключів

Вибирають велике просте число p, а також число g, $1 < g < p-1$, що має в мультиплікативній групі $Z_p^{\bullet}$ великий порядок. В ідеальному випадку g є первісним коренем за модулем p. Числа p і g не є секретними й перебувають у загальному користуванні. Кожен абонент вибирає собі випадкове число a в проміжку від 1 до $p-1$, і обчислює $h = g^a \bmod p$.

Відкритий ключ: p, g, h.

Секретний ключ: a.

Шифрування

Здійснюється блоками. Кожен блок M вважається елементом з $Z_p^{\bullet}$ (мультиплікативна група елементів, для яких у Z_n є зворотні щодо множення елементи (є мультиплікативні інверсії)). Повідомлення $M \in Z_p^{\bullet}$ перетвориться в криптотекст $C \in \left(Z_p^{\bullet}\right)^2$ у такий спосіб.

– Вибирається випадкове число r таке, що $1 \le r \le p-1$.

– Обчислюють $C = (c_1, c_2)$, де

$$c_1 = g^r \bmod p,\ c_2 = Mh^r \bmod p.$$

Розшифрування

Маючи секретний ключ a і криптотекст $C = (c_1, c_2)$, обчислюють

$$D(C) = c_2 \cdot \left(c_1^a\right)^{-1} \bmod p$$

Приклад

Показати роботу алгоритму шифрування Ель – Гамала, якщо обрані $p = 23, g = 5, a = 6$. Відкрите повідомлення характеризується числом $M = 7$.

Як і у всіх попередніх випадках, ми жертвуємо реалізмом для простоти обчислень. Тобто числа у прикладах достатньо малі. Нехай $p = 23, g = 5, a = 6$. Обчислюємо $h = 5^6 \bmod 23 = 8$. Відкритий і секретний ключі сформовані.

Припустимо, що шифрується числова інформація й необхідно зашифрувати повідомлення $M = 7$. Нехай обрано $r = 10$. Тоді $c_1 = 5^{10} \bmod 23 = 9$ й $c_2 = \left(7 \cdot 8^{10}\right) \bmod 23 = 21$. Одержуємо криптотекст $C = (9, 21)$.

Легко перевірити, що при розшифруванні цього криптотекста дійсно $D(9,21) = 21 \cdot \left(9^6\right)^{-1} \bmod 23 = 7$.

Електронний цифровий підпис по Ель-Гамалу

Формування і перевірка підпису відбувається за етапами.

1. Генерується випадкове просте число *p* довжини *n* бітів.

2. Вибирається випадковий примітивний елемент *g* поля Z_p.

3. Вибирається випадкове ціле число *x* таке, що $1 < x < p-1$

4. Обчислюється y, за формулою

$$Y = g^x mod\ p$$

g – випадковий примітив поля;

x – випадкове ціле число;

p – випадкове просте число довжини *n* бітів;

5. Відкритим ключем є трійка (*p, g , y*), закритим (таємним) ключем – число *x*.

При роботі в режимі підпису передбачається наявність фіксованої хеш-функції *h*, значення якої лежать в інтервалі (*1, p-1*).

3. Генерування підпису:

Обчислюється хеш значення повідомлення *h(M) =m*. При цьому хеш значення лежить в інтервалі $1 < m < (p - 1)$.

Обирається випадкове число *k* (це рандомізатор, таємний параметр)

з інтервалу (1; p - 1) , та взаємно просте з (p −1), потім обчислюються $a = g^k \pmod p$ та b з рівняння $m = ax + kb$ (mod (p-1))

Пара чисел (a, b) є цифровим підписом.

Отримувачу відправляється (M, a, b).

4. Перевірка підпису:

Перевіряють умови $1 < a < p$, $0 < b < (p - 1)$. Якщо хоча б одно невиконане – підпис недійсна.

Обчислюється хеш значення $m=h(M)$.

Підпис приймається при умові: $Y^a a^b \pmod p = g^m \pmod p$.

Приклад

Поставити підпис та перевірити його згідно зі схемою Ель Гамала, якщо надані параметри P = 11, G = 2. Еквівалентом хеш - значення є контрольна сума за модулем 5.

Символи повідомлення кодуються згідно з їх номерами в українській абетці.

Нехай є повідомлення РАНОК

Нумеруємо українську абетку з «0» і виписуємо номери символів повідомлення.

Обчислюємо еквівалент хеш – значення:

РАНОК- (20+0+16+18+14)(mod 5)=68(mod 5)=3 . Тобто $m=h(M)$=3

Для початку згенеруємо ключі шифрування. Якщо P = 11, G = 2.

Виберемо x = 8 – випадкове ціле число x таке, що $1 < x < p - 1$.

Обчислимо $y = g^x \pmod p = 2^8 \pmod{11} = 3$.

Отже, відкритим даними є трійка є 11, 2 та 3, закритим ключем є число x = 8.

Для отримання підпису вибираємо випадкове ціле число k = 9 таке, що $1 < k < p - 1$ та НСД (k, (p-1))=1. Дійсно НСД (9, (11-1))=1.

Обчислюємо $a = g^k \pmod p = 2^9 \pmod{11} = 512 \pmod{11} = 6$.

Обчислюємо b з рівняння $m = ax + kb$ (mod (p-1))

$3 = 6 \cdot 8 + 9 \cdot b \pmod{(11-1)}$

$9 \cdot b = -45 \pmod{10}$

$b = -\frac{45}{9} \pmod{10}$

$b = \frac{-45+\alpha \cdot 10}{9}$

$b = 5$ при $\alpha = 9$.

Тобто підпис (6, 5) , секретний ключ $x = 8$.

Перевіряємо підпис:

$Y^a a^b \pmod{p} = g^m \pmod{p}$

$3^6 \cdot 6^5 \pmod{11} = 2^3 \pmod{11}$

$9 = 9$

Все вірно!

Протолкол Діффі - Геллмана

Протокол Діффі-Геллмана (англ. Diffie–Hellman key exchange (D–H)) — це метод обміну криптографічними ключами. Один з перших практичних прикладів узгодження ключа, що дозволяє двом учасникам, що не мають жодних попередніх даних один про одного, отримати спільний секретний ключ з використанням незахищеного каналу зв'язку.

Припустимо обом абонентам відомі деякі два числа g та p, які не є секретними та можуть бути розповсюджені. Для того, щоб побудувати невідомий більш нікому секретний ключ, обидва абоненти генерують великі випадкові числа: перший абонент – число a, другий абонент – число b.

Далі перший абонент обчислює значення $A = g^a \bmod p$ та надсилає його другому абоненту, а другий абонент обчислює $B = g^b \bmod p$ та передає першому.

Передбачується, що зловмисник може отримати обидва ці значення, та не модифікувати їх (у нього немає можливості втручання в процес передачі).

На другому етапі перший абонент на основі a (яке у нього є) та отриманого з мережі B обчислює значення $B^a \bmod p = g^{ab} \bmod p$, а другий абонент на основі b (яке у нього є) та отриманого з мережі A обчислює значення A^b

mod $p = g^{a\ b} \bmod p$. Як можна бачити, у обох абонентів побудовано одне и те ж число: $K = g^{ab} \bmod p$. Його вони можуть використовувати у якості секретного ключ.

Тут зловмисник зустрічається з проблемою обчислення $g^{ab} \bmod p$ з перехоплених $g^a \bmod p$ и $g^b \bmod p$ (за реальний час). Числа p, a, b обирають достатньо великими.

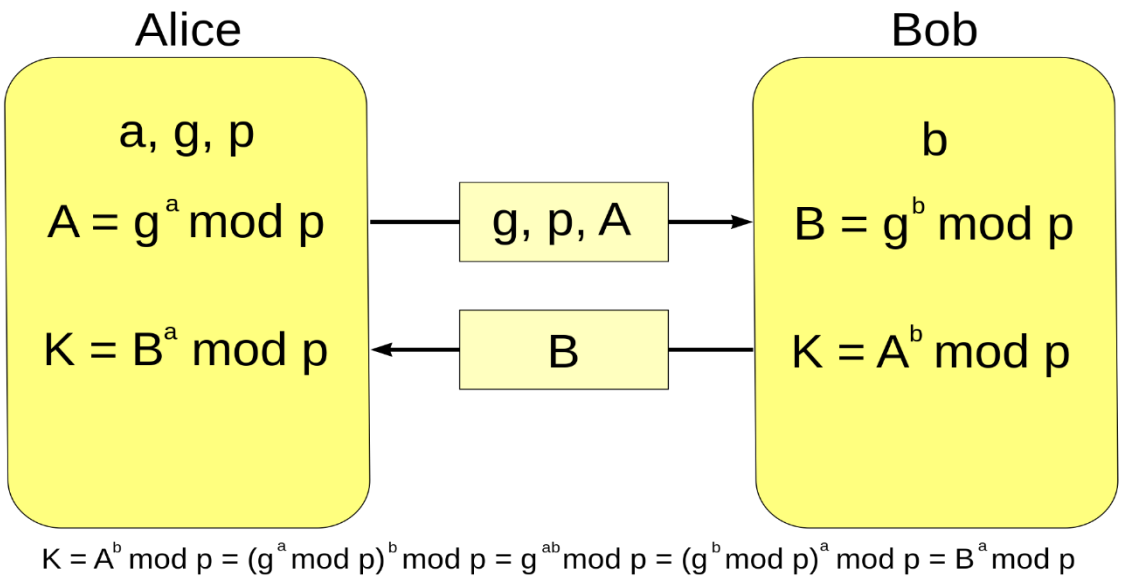


Рис 4.1 – Алгоритм Діффі – Геллмана

При роботі алгоритму, кожна сторона:

1. Генерує випадкове натуральне число a — закритий ключ;
2. Сумісно з віддаленою стороною установлює відкриті параметри p та g (звичайно значення p та g генеруються на одній стороні та передаються другій), де

p є випадковим простим числом

g є первісним коренем за модулем p;

Обчислюють відкритий ключ A, використовує перетворення закритого ключа

$A = g^a \ mod\ p$

Обмінюються відкритими ключами з віддаленою стороною;

3. Обчислюють загальний секретний ключ *K*, використовуя відкритий ключ віддаленої сторони *B* та свій закритий ключ *a*.

$K = B^a \ mod\ p$

K получаємо рівним з обох сторін, тому що:

$B^a\ mod\ p = (g^b\ mod\ p)^a\ mod\ p = g^{ab}\ mod\ p = (g^a\ mod\ p)^b\ mod\ p = A^b\ mod\ p$

Приклад

Показати роботу алгоритму Діффі- Геллмана, якщо модуль p=47, а примітивний елемент g=23.

Припустимо користувачі *A* та *B* обрали свої секретні ключі

a=12 (mod 47) та b=33 (mod 47).

Для того, щоб мати загальний ключ, обидва користувачі обчислюють значення відкритих ключів:

$A = g^a\ (\ mod\ p) = 23^{12}\ (\text{mod } 47) = 27$

$B = g^b\ (\ mod\ p) = 23^{33}\ (\text{mod } 47) = 33$

Після цього користувачі обмінюються *A* та *B* та обчислюють незалежно загальний ключ.

Користувач *A* обчислює:

$$K = B^a\ (\ mod\ p) = 33^{12}\ (\text{mod } 47) = 25.$$

Користувач *B* обчислює:

$$K = A^b\ (\ mod\ p) = 27^{33}\ (\text{mod } 47) = 25.$$

Як бачимо ключі рівні К = $g^{ab}\ mod\ p = g^{ba}\ mod\ p$.

Тепер можна використовувати цей загальний ключ, наприклад, в RSA.

Тобто $К_1$=25 – перший ключ для RSA. Другий ключ можна знайти як

$$К_1\ К_2 \equiv 1\ (\text{mod } \varphi(p))$$

$$25\ К_2 \equiv 1\ (\text{mod } (47 - 1))$$

$$К_2 = 35.$$

Припустимо, треба зашифрувати системою RSA повідомлення M=16.

Шифруємо ключем $К_1$:

$$C = M^{к1}(\text{mod p}) = 16^{25}\ (\text{mod } 47) = 21$$

Розшифровуємо ключем $К_2$:

$$M=C^{к2}(\text{mod } p) = 21^{35} (\text{mod } 47)=16$$

Завдання до практичного заняття 4

Завдання 1.

Зашифрувати та розшифрувати повідомлення M=2 з використанням RSA криптоалггоритму:

P=11,Q=13(0);

P=11,Q=23(1);

P=7,Q=23 (2);

P=7,Q=19 (3).

Вибрати та розрахувати ключові параметри $(\varphi(n), E, D)$. P та Q обирати у залежності від номеру журналу k. № вар.$=(k+1)\bmod 4$.

Завдання 2.

Зашифрувати повідомлення $M=2$ з використанням алгоритму Ель – Гамала та розшифрувати його. Таємний ключ та випадкове число k обрати самостійно. P та G обирати у залежності від номеру у журналі.

1. $P=11, G=3$;
2. $P=13, G=5$;
3. $P=11, G=5$;
4. $P=11, G=4$;
5. $P=17, G=5$;
6. $P=17, G=4$;
7. $P=19, G=5$;
8. $P=17, G=3$;
9. $P=19, G=3$;
10. $P=19, G=4$;
11. $P=13, G=4$;
12. $P=23, G=2$;
13. $P=11, G=3$;
14. $P=13, G=5$;
15. $P=11, G=5$;

16.$P = 11, G = 4$;
17. $P = 17, G = 5$;
18. $P = 17, G = 4$;
19. $P = 19, G = 5$;
20. $P = 17, G = 3$;
21. $P = 19, G = 3$;
22. $P = 19, G = 4$;
23. $P = 13, G = 4$;
24.$P = 23, G = 2$;
25. $P = 13, G = 3$.
26. $P = 13, G = 3$.

Завдання 3.

Продемонструвати роботу алгоритму відкритого розповсюдження ключів Діффі- Геллмана, якщо *K1*, *K2* та *G* надані в таблиці 4.1. *N*=41.

Таблиця 4.1

№	*K1*	*K2*	*G*
1	2	13	2
2	3	19	3
3	5	13	2
4	7	11	3
5	11	5	2
6	13	3	3
7	19	2	2
8	2	11	3
9	2	17	2
10	3	11	3
11	3	13	2
12	5	11	3
13	5	17	2
14	5	19	3
15	7	13	2
16	7	17	3
17	11	13	2
18	11	17	3
19	11	19	2
20	13	17	3
21	2	19	2
22	3	17	3

Завдання 4.

Поставити підпис та перевірити його згідно зі схемою Ель Гамала, якщо надані параметри P та G. Додаткові параметри обрати самостійно згідно з умовами алгоритму.

Еквівалентом хеш – значення є контрольна сума за модулем 5. Символи повідомлення кодуються згідно з їх номерами в українській абетці. Якщо сума за модулем 5 дорівнює «0» – еквівалент хеш - значення взяти 3.

1. $P = 13, G = 5$ *АЛГЕБРА*;
2. $P = 11, G = 5$ *ГЕОМЕТРІЯ*;
3. $P = 11, G = 4$ *КРИПТОГРАФІЯ*;
4. $P = 17, G = 5$ *КРИПТОАНАЛІЗ*;
5. $P = 17, G = 4$ *ФІЗИКА*;
6. $P = 19, G = 5$ *ПРИКЛАД*;
7. $P = 17, G = 3$ *ПРИВІТАННЯ*;
8. $P = 19, G = 3$ *ГАЗЕТА*;
9. $P = 19, G = 4$ *ЖУРНАЛ*;
10. $P = 13, G = 4$ *ПЕРЕВІРКА*;
11. $P = 23, G = 2$ *ПИТАННЯ*;
12. $P = 11, G = 3$ *ДЕКАНАТ* ;
13. $P = 13, G = 5$ *ФАКУЛЬТЕТ*;
14. $P = 11, G = 5$ *ІНСТИТУТ*;
15. $P = 11, G = 4$ *ПРАКТИКА*;
16. $P = 17, G = 5$ *СТУДЕНТ*;
17. $P = 17, G = 4$ *ЕКЗАМЕН*;
18. $P = 19, G = 5$ *ПРАВИЛО*;
19. $P = 17, G = 3$ *ШКОЛА*;
20. $P = 19, G = 3$ *ГІМНАЗІЯ*;
21. $P = 19, G = 4$ *ХІМІЯ* ;
22. $P = 13, G = 4$ *ПРОТОКОЛ*;
23. $P = 23, G = 2$ *ШИФР*;
24. $P = 13, G = 3$ *КНИГА*;
25. $P = 13, G = 3$ *МУЗЕЙ*;
26. $P = 11, G = 3$ *ГЕОГРАФІЯ*.

Практичне заняття 5

Алгоритми факторизаці

Теоретичні відомості

Метод Полларда

Найбільш популярним імовірнісним алгоритмом факторизації є метод запропонований Дж. Поллардом в 1975 р.

Алгоритм Полларда

Крок 1. Обираємо багаточлен $f(x) \in Z[x]$.

Крок 2. Випадково обираємо $x_0 \in Z_n$ й, обчислюючи значення $x_i = f(x_{i-1}) \bmod n,\ i = 1,\ldots,m,$ перевіряємо тест кроку 3.

Крок 3. Полагаємо $j = 2^h - 1$ й для кожного $2^h \le k < 2^{h+1}$ обчислюємо $d = (x_j - x_k, n)$. Якщо $1 < d < n$, то нетривіальний дільник числа n знайдений. Якщо $d = 1$ або $d = n$, то переходимо до наступного значення h.

Щоб зрозуміти сутність алгоритму розглянемо його на простому прикладі з невеликими значеннями чисел.

Приклад.

Нехай потрібно факторизувати число $n = 221$. Обрано багаточлен з цілими коефіцієнтами $f(x) = x^2 + 1,\ x_0 = 1$.

Обчислюємо $x_i = f(x_{i-1}) \bmod n,\ i = 1 \ldots, n.$

$x_1 = 1^2 + 1\ (mod\ 221) = 2$:

$x_2 = 2^2 + 1\ (mod\ 221) = 5$:

$x_3 = 5^2 + 1\ (mod\ 221) = 26$:

$x_4 = 26^2 + 1\ (mod\ 221) = 14$:

$x_5 = 14^2 + 1\ (mod\ 221) = 197$:

$x_6 = 197^2 + 1\ (mod\ 221) = 135.$

Знаходимо $d = (x_j - x_k, n)$.

$(x_2 - x_1, n) = (5 - 2, 221) = 1;$

$(x_3 - x_1, n) = (26 - 2, 221) = 1;$

$(x_4 - x_1, n) = (14 - 2, 221) = 1;$

$(x_5 - x_1, n) = (197 - 2, 221) = 1;$

.

.

.

$(x_6 - x_2, n) = (135 - 2, 221) = 13.$

$1 < 13 < 221$– нетривіальний дільник знайдено.

221=13 ·17 – другий дільник знайдено.

Варто помітити, що ми відразу вдало підібрали багаточлен, при якому метод швидко дав результат. Це буває не завжди.

p-1 метод факторизаії Полларда

Припустимо, що n- непарне складене число, що не має невеликих простих дільників. Позначимо через p найменший простий дільник числа n. Наша задача полягає в його знаходженні.

Припустимо, що число $(p-1)$ розкладається в добуток невеликих простих дільників. Виберемо число k, що є параметром методу. Для успішної роботи алгоритму потрібно, щоб виконувалася умова

$$(p-1) | M(k),$$

де $M(k) = \text{НСК}(1,2,...,k)$ (замість $M(k)$ можна використати $k!$ або добуток $p_1^{\alpha_1} \dots p_2^{\alpha_2}$ перших k простих чисел у деяких степенях $\alpha_1 \geq \dots \geq \alpha_k$, які обираються з евристичних міркувань).

У силу малої теореми Ферма виконується порівняння

$$2^{M(k)} \equiv 1 (\text{mod } p).$$

Якщо при цьому

$$2^{M(k)} \neq 1 (\text{mod } n),$$

то

$$p|(2^{M(k)}-1,n),$$

де $1<p,(2^{M(k)}-1,n)<n.$

Таким чином, $d=(2^{M(k)}-1,n)$ – є власним дільником числа n кратним p.

На цій ідеї заснований наступний метод знаходження власного дільника числа n. Число k невідомо, тому використовується послідовний перебір малих значень до деякого фіксованого значення.

Нехай k – ціле число, наприклад $k<10^6$, і c – невелике ціле з умовою $(c,n)=1,$ наприклад $c=2.$

Крок 1. Для кожного i від 1 до k обчислюється $m_i=c^{M(i)} \bmod n$ й перевіряємо тест кроку 2.

Крок 2. Обчислити $d=(m_i-1,n).$ Якщо $1<d<n,$ те знайдений нетривіальний дільник числа n. У противному випадку полагаємо $i=i+1.$

Наприклад

Методом Полларда факторизувати число 221.

Нехай $M(i)=k!, c=2.$

Обчислюємо для кожного i від 1 до k $m_i=c^{M(i)} \bmod n$.

$m_1=2^1(mod\ 221)=2;$

$m_2=2^{1\cdot 2}(mod\ 221)=4 \qquad d=(4-1,221)=1;$

$m_3=2^{1\cdot 2\cdot 3}(mod\ 221)=64 \qquad d=(64-1,221)=1;$

$m_4=2^{1\cdot 2\cdot 3\cdot 4}(mod\ 221)=1 \qquad d=(64-1,221)=1.$

Далі рахувати немає сенсу.

Оберемо друге с. Нехай с=3.

$m_1=3^1(mod\ 221)=3;$

$m_2=3^{1\cdot 2}(mod\ 221)=9 \qquad d=(9-1,221)=1;$

$m_3=2^{1\cdot 2\cdot 3}(mod\ 221)=729 \qquad d=(729-1,221)=13;$

Нетривіальний дільник знайдений.

Другий дільник можна знайти безпосередньо діленням. $221=13 \cdot 17$ – другий дільник знайдено.

Факторизація Ферма

Досить плідною ідеєю при побудові алгоритмів факторизації є пошук чисел x й y, для яких виконується співвідношення $x^2 \equiv y^2 (\mathrm{mod}\, n), x \neq \pm y (\mathrm{mod}\, n)$.

Якщо при цьому $x \neq \pm y (\mathrm{mod}\, n)$, то числа $НСД(x+y,n)$ й $НСД(x-y,n)$ суть нетривіальні дільники числа n.

Безумовно, першим у цьому напрямку є метод факторизації, застосований П. Ферма. Він заснований на теоремі Ойлера про подання числа у вигляді різниці двох квадратів.

Метод Ферма полягає в тім, що при малих значеннях параметра y в поданні $n = x^2 - y^2$ можна знайти пару (x,y), перебираючи як кандидатів на значення числа x $\lfloor \sqrt{n} \rfloor + 1, \lfloor \sqrt{n} \rfloor + 2, \ldots$ й перевіряючи для кожного з них рівності $(\lfloor \sqrt{n} \rfloor + i)^2 - n = y^2$.

Для відбраковування помилкових значень x можна скористатися тим, що якщо число не є квадратом, то воно з великою ймовірністю не буде й квадратичним відрахуванням для одного з невеликих простих чисел p. Остання властивість легко перевіряється шляхом обчислення відповідного символу Лежандра.

Алгоритм Ферма

Вхід: $n -$ непарне число, $p_1, \ldots, p_k -$ невеликі прості числа.

Крок 0. Перевірити $p_i | n, i = 1, \ldots, k$. Якщо так, то дільник знайдений.

Крок 1. Для кожного x від $\lfloor \sqrt{n} \rfloor + 1$ до $\lfloor \sqrt{n} \rfloor + n_0$ обчислити величини

$$t = x^2 - n, t_i = t \bmod p_i, i = 1, \ldots, k.$$

Крок 2. Якщо хоча б для одного $i = 1, \ldots, k$ виконано одне з умов:

$- t_i = 0$ і p_i^2 не ділить t;

або

$-t_i \neq 0$ і $\left(\frac{t_i}{p_i}\right) = -1,$

то перейти до наступного x на кроці 1.

У противному випадку перейти до кроку 3.

Крок 3. Перевірити, чи є $t = x^2 - n$ повним квадратом. Якщо $x^2 - n = y^2$, то видати відповідь: «$n-$ складене, ».

Відповідь буде $n = a \cdot b$, де a = НСД$(x + y, n)$, b = НСД $(x - y, n)$.

Якщо $t = x^2 - n$ - не повний квадрат, то перейти до наступного x на кроці 1.

Наприклад

Нехай потрібно факторизувати число $n = 221$ Вхід $n = 221, p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11.$

Крок 0. 221 не ділиться на жодне з p_i.

Крок 1. $\lfloor\sqrt{221}\rfloor = 14$

$x = \lfloor\sqrt{221}\rfloor + 1 = 15$

x_1=15

x_2=16

x_3=17

.

.

.

$t = x_1^2 (mod\ n) = 15^2 (\text{mod } 221) = 4;$

$t_{i1} = 4(mod\ p_1) = 4(mod\ 2) = 0;$

($t_i = 0$,але p_i^2 ділить t);

$t_{i2} = 4(mod\ p_2) = 4(mod\ 3) = 1;$;

$$\left(\frac{t_{i2}}{p_i}\right) = \left(\frac{1}{2}\right) = \left(\frac{1}{3}\right) = \left(\frac{1}{5}\right) = \left(\frac{1}{7}\right) = \left(\frac{1}{11}\right) = 1 (\text{т. к. } \left(\frac{1}{p}\right) = 1);$$

$t_{i3} = 4(mod\ p_3) = 4(mod\ 5) = 4;$

$$\left(\frac{t_{i3}}{p_i}\right)=\left(\frac{4}{3}\right)=\left(\frac{4}{5}\right)=\left(\frac{4}{7}\right)=\left(\frac{4}{11}\right)=1\text{ (т. к. }\left(\frac{a^2}{p}\right)=1);$$

$t_{i4}=4$

$$\left(\frac{t_{i4}}{p_i}\right)=\left(\frac{4}{3}\right)=\left(\frac{4}{5}\right)=\left(\frac{4}{7}\right)=\left(\frac{4}{11}\right)=1;$$

$$t_{i5}=4(mod\ p_5)=4(mod\ 11)=4;$$

$$\left(\frac{t_{i5}}{p_i}\right)=\left(\frac{4}{3}\right)=\left(\frac{4}{5}\right)=\left(\frac{4}{7}\right)=\left(\frac{4}{11}\right)=1.$$

Умови $-t_i=0$ й p_i^2 не ділить t; або

$$-t_i\neq 0 \text{ і } \left(\frac{t_i}{p_i}\right)=-1, \text{ не виконуються ні для одного } i=1,\ldots,k.$$

Переходимо до кроку 3.

Перевіряємо, чи є $t=x^2-n$ повним квадратом. $t=15^2(mod\ 221)=4=2^2=y^2$

n- складене, $n=a\cdot b$, де $a=$ НСД$(x-\text{у}, n)=$ НСД$(15-2, 221)=13$

$$b=\text{НСД}(x+\text{у}, n)=\text{НСД}(15+2, 221)=17$$

Алгоритм Діксона

У багатьох сучасних алгоритмах факторизації для знаходження дільників використовується ідея Лежандра (1798 р.), що полягає в пошуку чисел x й y, що задовольняють умовам

$$x^2\equiv y^2\,(\text{mod}\,n), x\neq\pm y(\text{mod}\,n).$$

Цей підхід є узагальненням методу Ферма, у якому потрібне виконання строгої рівності.

Для пошуку таких чисел використається поняття факторної бази

Назвемо факторною базою деяка множина $B=\{p_1,p_2,\ldots,p_h\}$ невеликих простих чисел. Звичайно в якості $\{p_1,p_2,\ldots,p_h\}$ беруть прості числа, що не перевершують деякої границі $M, h=\pi(M)$.

Будемо говорити . що ціле число $b \in N \in B$ - числом, якщо число $b^2 \bmod n$ розкладається в добуток простих чисел з факторної бази.

$$b^2 \bmod n = \prod_{p \in B} p^{\alpha_p(b)} .$$

Зіставимо кожному B - числу вектор показників із цього розкладання

$$\vec{\alpha}(b) = (\alpha_{p_1}(b), \ldots, \alpha_{p_h}(b)),$$

а також двійковий вектор, отриманий з вектора $\vec{\alpha}(b)$ приведенням всіх його координат за модулем 2,

$$\vec{\varepsilon}(b) = (\alpha_{p_1}(b) \bmod 2, \ldots, \alpha_{p_h}(b) \bmod 2).$$

Якщо тепер яким-небудь способом підібрати таку множину різних B - чисел $b_1, \ldots, b_m$, при якому виконується лінійне співвідношення

$$\vec{\varepsilon}(b_1) \oplus \ldots \oplus \vec{\varepsilon}(b_m) = \vec{0},$$

те для добутку $x = b_1 \ldots b_m$ виконується співвідношення

$$x^2 \equiv y^2 (\bmod n),$$

де число y визначається по векторах показників рівністю

$$y = \prod_{p \in B} p^{\frac{1}{2}(\vec{\alpha}_p(b_1) + \ldots + \vec{\alpha}_p(b_m))} .$$

Алгоритм Діксону полягає в наступному.

Крок 1. Вибрати випадкове $b, 1 < b < n$, і обчислити $b^2 \bmod m$.

Крок 2. Пробними діленнями спробувати розкласти $b^2 \bmod m$ на прості множники з факторної бази.

Крок 3. Якщо B є B - числом, тобто $b^2 \bmod n = \prod_{p \in B} p^{\alpha_p}(b)$,

те запам'ятати $\vec{\alpha}(b)$ й $\vec{\varepsilon}(b)$. Повторити процедуру генерації чисел b доти не буде знайдено $m = h + 1$ B - чисел $b_1, \ldots, b_m$.

Крок 4. Знайти, наприклад вирішуючи за допомогою алгоритму послідовного виключення невідомих Гауса, однорідну систему лінійних рівнянь $x_1 \vec{\varepsilon}(b_1)\oplus\ldots\oplus x_m \vec{\varepsilon}(b_m) = \vec{0}$ щодо невідомих $(x_1,\ldots,x_m))$ співвідношення лінійної залежності

$$\vec{\varepsilon}(b_{i_1})\oplus\ldots\oplus\vec{\varepsilon}(b_{i_t}) = \vec{0}, 1 < t \le m.$$

Покласти

$$x = b_{i_1}\ldots b_{i_{t_y}}, \qquad y = \prod_{p\in B} p^{\frac{1}{2}(\vec{\alpha}_p(b_1)+\ldots+\vec{\alpha}_p(b_m))}.$$

Крок 5. Перевірити $x \equiv \pm y(\mathrm{mod}\, n)$. Якщо це так, то повторити процедуру генерації. Якщо ні, то знайдено нетривіальне розкладання

$$n = u\cdot v, u = (x+y,n), v = (x-y,n).$$

Наприклад. Нехай потрібно факторизувати число $n = 221$.

Розрахуємо . $\lfloor\sqrt{221}\rfloor = 14$

$x_1 = \lfloor\sqrt{221}\rfloor + 1 = 15$

x_2=16

x_3=17

.

.

.

Візьмемо фактор - базу 2,3,5,7.

1. $x_1^2(mod\ n) = 15^2(mod\ 221) = 4 = 2^2$;
2. $x_2^2(mod\ n) = 16^2(mod\ 221) = 35 = \mathbf{5\cdot 7}$;
3. $x_3^2(mod\ n) = 17^2(mod\ 221) = 68 = 17\cdot 2^2$;
4. $x_4^2(mod\ n) = 18^2(mod\ 221) = 103$;
5. $x_5^2(mod\ n) = 19^2(mod\ 221) = 140 = \mathbf{7\cdot 5\cdot 2^2}$;

Вже є претенденти на відповідь.

Розглянемо цей варіант.

$x = 19 \cdot 16$

$y = \sqrt{5 \cdot 7 \cdot 7 \cdot 5 \cdot 2^2} = \sqrt{5^2 \cdot 7^2 \cdot 2^2} = 5 \cdot 7 \cdot 2$

НСД $(19 \cdot 16 - 5 \cdot 7 \cdot 2, 221) = 13;$

НСД $(19 \cdot 16 + 5 \cdot 7 \cdot 2, 221)$=17.

Отже ми знайшли відповідь 221=13 ·17.

Завдання до практичного заняття 5

Завдання 1.

Методом Поларда , ρ -1 Поларда, Ферма та Діксона факторизувати число, надане у наступній таблиці. Варіант обирати у залежності від номеру за списком у журналі.

№ вар	1	2	3	4	5	6	7	8	9
число	209	187	437	589	253	493	323	437	391

№ вар	10	11	12	13	14	15	16	17	18
число	209	133	247	319	589	217	377	391	667

№ вар	19	20	21	22	23	24	25	26	27
число	119	403	527	299	319	247	377	391	217

\

Практичне заняття 6

Операції у групі точок ЕК

Теоретичні відомості

Нагадаємо, що еліптичною кривою E над полем F називається гладка крива, що задається рівнянням вигляду

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_i \in F. \qquad (6.1)$$

Іноді замість (6.1) зручно користуватися рівнянням алгебри для функції двох змінних.

$$F(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0. \qquad (6.2)$$

Позначатимемо ε F безліч точок (x, y) ∈ F^2 , які задовольняють цьому рівнянню і що містить крім того нескінченно видалену точку.

Точка на нескінченості позначається О. Якщо K - розширення поля F, то ε K позначає безліч точок (x, y) ∈ K^2, що задовольняють рівнянню разом з точкою О. Замість загального запису рівняння часто розглядають канонічні рівняння трьох типів кривих

$$E: y^2 = x^3 + ax + b, p \neq 2,3;$$
$$E_S: y^2 + y = x^3 + a_4x + b, p = 2;$$
$$E_N: y^2 + xy = x^3 + a_2x^2 + a_6, a_6 \neq 0, p = 2,$$

де $p -$ характеристика поля.

Нехай E еліптична крива над полем дійсних чисел, задана рівнянням (6.2), і нехай P і Q - дві точки на еліптичній кривій. Визначимо протилежний елемент до P (тобто зворотний елемент) і суму $P + Q$ за наступним правилом:

1) Якщо P є точкою O , то ми визначимо $-P$ як O. Для кожної точки Q ми вважатимемо $Q + O = Q$, тобто точка O виконує роль одиниці по додаванню;

2) Точка $-P$ є точкою з тією ж x - координатою, але із запереченням y-координати, тобто – (x, y) = (x,–y). Якщо $Q = -P$, то ми визначаємо суму $P + Q$ як точку на нескінченності O;

3) Якщо P і Q мають різні x-координати, то можна показати, що лінія, що проходить через P та Q, перетинає криву тільки в одній точці R.

(Ця точка може співпадати з P або Q і тоді пряма є дотичною до кривої в точці P або Q і тоді ми вважатимемо $R = P$ або $R = Q$ відповідно).

Потім ми визначаємо $P = Q$ як $-R$, тобто як дзеркальне щодо осі x відображення точки перетину R;

4) Остання можливість це $P = Q$. Нехай L є дотичною до кривої в точці

P, та нехай R – єдина точка перетину прямої з еліптичною кривою, тоді ми вважатимемо, що $2P = -R$. (В цьому випадку точка P є точкою інфлекції).

Сума будь-яких трьох точок на еліптичній кривій, що належать одній прямій, рівна O. Визначимо групову операцію, традиційно звану додаванням точок еліптичної кривої.

Сумою двох точок $P = (x_1, y_1)$ и $Q = (x_2, y_2)$ називається точка

$R = P + Q = (x_3, y_3)$, зворотна третій точці перетину EC прямою лінією, що проходить через точки P та Q.

Знайдемо координати точки $R = P + Q = (x_3, y_3)$. Будемо виражати їх через координати точок P та Q. При цьому точки P та Q можуть бути різними або співпадати. Ми опустимо доведення цих формул.

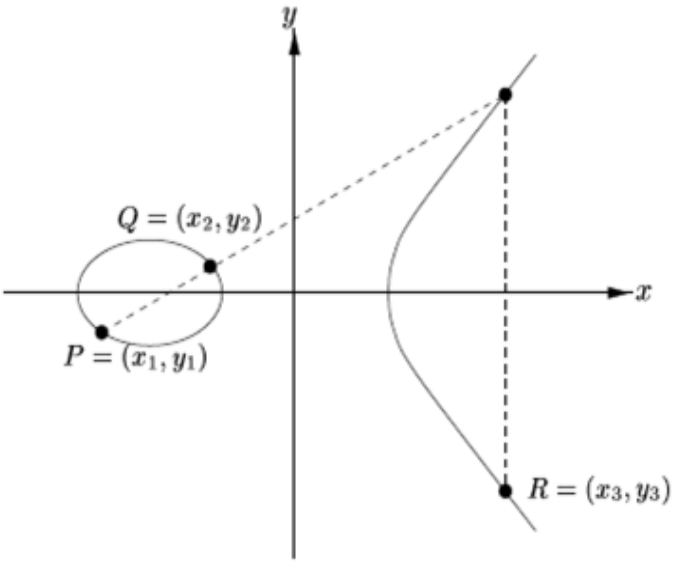


Рис.6.1–Геометрична інтерпретація додавання двох різних точок P та Q

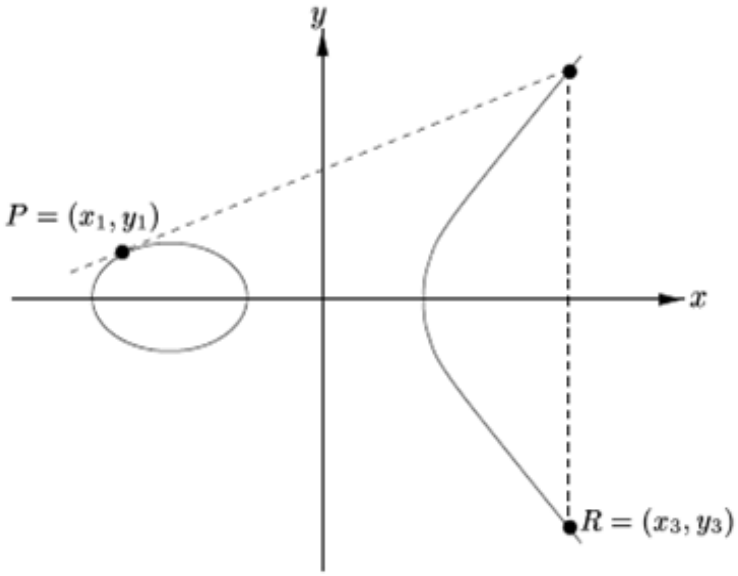


Рис.6.2 –Геометрична інтерпретація подвоєння точки кривої

Закони додавання та подвоєння точок для кривої Е

$$1.\begin{cases} x_3 = \lambda^2 - x_1 - x_{2,} P \neq Q; \\ y_3 = -y_1 - \lambda(x_3 - x_1), \lambda = \frac{y_2 - y_1}{x_2 - x_1} \end{cases} \quad (6.3)$$

$$2.\begin{cases} x_3 = v^2 - 2x_1, P = Q; \\ y_3 = -y_1 - v(x_3 - x_1), v = \frac{3x_1^2 + a.}{2y_1} \end{cases} \quad (6.4)$$

Ці формули справедливі для кривих E над всіма полями, у тому числі і кінцевими, окрім полів характеристик 2 і 3.

Закони додавання та подвоєння точок для кривої E_S

$$1. \quad \begin{cases} x_3 = \lambda^2 + x_1 + x_{2,} P \neq Q; \\ y_3 = y_1 + 1 + \lambda(x_3 + x_1), \lambda = \frac{y_1 + y_2}{x_1 + x_2} \end{cases} \quad (6.5)$$

$$2. \quad \begin{cases} x_3 = v^2, v = x_1^2 + a_4, P = Q; \\ y_3 = y_1 + 1 + v(x_3 + x_1). \end{cases} \quad (6.6)$$

Закони додавання та подвоєння точок для кривої E_N

$$1. \begin{cases} x_3 = \lambda^2 + \lambda + x_1 + x_2 + a_2, P \neq Q; \\ y_3 = y_1 + x_3 + \lambda(x_3 + x_1), \lambda = \frac{y_1 + y_2}{x_1 + x_2}. \end{cases} \quad (6.7)$$

$$2.\begin{cases} x_3 = v^2 + v + a_2, v = x_1 + \frac{y_1}{x_1}, P = Q; \\ y_3 = y_1 + x_3 + v(x_3 + x_1) = x_1^2 + x_3(v+1). \end{cases} \quad (6.8)$$

Ще деякі важливі визначення.

Порядком точки Q еліптичної кривої називається найменше число k, таке що $k \cdot Q = O$. O – точка на нескінченості.

Приклад 1

Нехай $P_1 = (0,1)$, $P_2 = (4,2)$ на кривій $y^2 = x^3 + x + 1 (mod\ 5)$.

а) Знайти $P_1 + P_2 = (x_3, y_3)$.

Це крива вигляду Е. Формули для додавання на цій кривій:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}(mod\ 5) = \frac{2-1}{4-0}\ (mod\ 5) = \frac{1}{4}\ \ (mod\ 5) = \frac{1 + \alpha \cdot 5}{4} =$$
$$= 4\ (\text{при } \alpha = 3).$$

$$x_3 = \lambda^2 - x_1 - x_2\ (mod\ 5) = (4^2 - 0 - 4)\ (mod\ 5) = 2;$$
$$y_3 = -y_1 - \lambda(x_3 - x_1)\ (mod\ 5) = -1 - 4(2-0)\ (mod\ 5) = 1.$$

Можна перевірити, що точка (2,1) теж належить цій кривій.

$$y^2 = x^3 + x + 1\ (mod\ 5)$$
$$1^2\ (mod\ 5) = (2^3 + 2 + 1)\ (mod\ 5)$$
$$1 = 1$$

а) Знайти $2\ P_1 = (x_3, y_3)$.

Формули для подвоєння на цій кривій:

$$v = \frac{3x_1^2 + a}{2y_1}(mod\ 5) = \frac{3 \cdot 0^2 + 1}{2 \cdot 1}(mod\ 5) = \frac{1}{2}(mod\ 5) = \frac{1 + \alpha \cdot 5}{2} =$$
$$= 3\ (\text{при } \alpha = 1).$$

$$x_3 = v^2 - 2 \cdot x_1\ (mod\ 5) = (3^2 - 2 \cdot 0)\ (mod\ 5) = 4;$$
$$y_3 = -y_1 - v(x_3 - x_1)\ (mod\ 5) = -1 - 3(4-0)\ (mod\ 5) = 2.$$

Також можна перевірити, що ця точка належить кривій.

$$y^2 = x^3 + x + 1\ (mod\ 5)$$

$$2^2\ (mod\ 5) = (4^3 + 4 + 1)\ (mod\ 5)$$

$$4 = 4$$

Приклад 2

Знайти порядок точки Q = (17,20) на кривій $y^2 = x^3 + x + 1$ (*mod* 23).

Будемо подвоювати та додавати точки на кривій до отримання точки на нескінченості.

Це крива вигляду Е, тобто для подвоєння та додавання використовуємо формули (6.3) та (6.4).

1. Розраховуємо 2 Q . Подвоюємо точку Q =(17,20).

$$v = \frac{3x_1^2 + a}{2y_1}(mod\ 23) = \frac{3 \cdot 17^2 + 1}{2 \cdot 20}(mod\ 23) = \frac{217}{10}(mod\ 23) = \frac{10}{10}(mod\ 23) = 1.$$

$$x_3 = v^2 - 2 \cdot x_1\ (mod\ 23) = (1^2 - 2 \cdot 17)\ (mod\ 23) = 13;$$

$$y_3 = -y_1 - v(x_3 - x_1)\ (mod\ 23) = -20 - 1(13 - 17)\ (mod\ 23) = 7.$$

Тобто 2 Q=(13,7).

2. Розраховуємо 3 Q = 2 Q + Q.

2 Q=(13,7) Q =(17,20)

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}(mod\ 23) = \frac{20 - 7}{17 - 13}\ (mod\ 23) = \frac{13}{4}\ \ (mod\ 23) == \frac{13 + \alpha \cdot 23}{4} = 9\ (\text{ при } \alpha = 1).$$

$$x_3 = \lambda^2 - x_1 - x_2\ (mod\ 23) = (9^2 - 13 - 17)\ (mod\ 23) = 51(mod\ 23) = 5;$$

$$y_3 = -y_1 - \lambda(x_3 - x_1)\ (mod\ 23) = -7 - 9(5 - 13)\ (mod\ 23) = 19.$$

Тобто 3 Q=(5,19).

3. Розраховуємо 4 Q. Це можна зробити двома способами або подвоїти точку 2 Q, або до точки 3 Q додати точку Q.

Подвоїмо 2 Q.

2 Q (13, 7)

$$v = \frac{3x_1^2 + a}{2y_1}(mod\ 23) = \frac{3 \cdot 13^2 + 1}{2 \cdot 7}(mod\ 23) = \frac{508}{14}(mod\ 23)$$
$$= \frac{254}{7}(mod\ 23) = \frac{1}{7}(mod\ 23) = \frac{1 + \alpha \cdot 23}{7} == 10 \text{ (при } \alpha = 3).$$

$x_3 = v^2 - 2 \cdot x_1\ (mod\ 23) = (10^2 - 2 \cdot 13)\ (mod\ 23) = 5;$

$y_3 = -y_1 - v(x_3 - x_1)\ (mod\ 23) = -7 - 10(5 - 13)\ (mod\ 23) = 4.$

Тобто 4 Q=(5,4).

Помітимо, що у точок 3 Q=(5,19) та 4 Q=(5,4) однакові x координати. Тобто при додаванні цих точок і підрахунку λ

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

у знаменнику буде "0".

3 Q + 4 Q = 7 Q.

Порядок точки Q (17,20) на ЕК $y^2 = x^3 + x + 1$ (*mod* 23) дорівнює 7.

Завдання до практичного заняття 6

Завдання 1.

Знайти порядки точок на кривих:
1. P = (3, 8) на $y^2 = x^3 - 43x + 166$
2. P = (0,4) на $y^2 = 4x^3 + 16$
3. P = (2, 8) на $y^2 = 4x^3 + 16x$
4. P = (2, 3) на $y^2 = x^3 + 1$
5. P = (2, 4) на $y^2 = x^3 + 4x$
6. P = (7,2) на $y^2 = x^3 + 3x + 3$ (mod 11)
7. P = (7,9) на $y^2 = x^3 + 3x + 3$ (mod 11)
8. P = (0,6) на $y^2 = x^3 + 3x + 3$ (mod 11)
9. P = (3, 6) на $y^2 = x^3 + x+6$ (mod 11)
10. P = (8.3) на $y^2 = x^3 + x+6$ (mod 11)
12. P = (2,2) на $y^2 = x^3 + 2x + 6$ (mod 7)
13. P = (2,5) на $y^2 = x^3 + 2x + 6$ (mod 7)
14. P = (3,5) на $y^2 = x^3 + 2x + 6$ (mod 7)
15. P = (4,1) на $y^2 = x^3 + 2x + 6$ (mod 7)
16. P = (4,6) на $y^2 = x^3 + 2x + 6$ (mod 7)
17. P = (0,5) на $y^2 = x^3 + 3x + 3$ (mod 11)
19. P = (4,9) на $y^2 = x^3 + 17$.
20. P = (2,5) на $y^2 = x^3 + 17$.

21. $P = (-1,4)$ на $y^2 = x^3 + 17$.
22. $P = (2, 2)$ на $y^2 = x^3 + x + 1 \pmod 7$
23. $P = (2, 2)$ на $y^2 = x^3 + 1 \pmod 5$
24. $P = (1, 3)$ на $y^2 = x^3 + 1 \pmod 7$
25. $P = (3, 4)$ на $y^2 = x^3 + x \pmod 7$

Завдання 2.

Перевірити , чи належать точки кривій. Знайти координати точки $R = P + Q = (x_3, y_3)$ та $2P\ (x_4, y_4)$ на кривій $y^2 = x^3 + x + 1 \pmod{23}$, якщо

№	1	2	3	4	5	6	7	8
P	(6,4)	(11,3)	(7,12)	(11,20)	(13,7)	(6,4)	(12,4)	(11,20)
Q	(13,16)	(18,20)	(5,19)	(12,4)	(7,11)	(18,20)	(5,19)	(5,19)

№	9	10	11	12	13	14	15	16
P	(6,4)	(11,3)	(7,12)	(11,20)	(13,7)	(18,20)	(5,19)	(12,4)
Q	((13,16)	(18,20)	(5,19)	(12,4)	(7,11)	(6,4)	(7,11)	(18,20)

№	17
P	(6,4)
Q	((13,16)

Перевірити , чи належать точки кривій. Знайти координати точки $R = P + Q = (x_3, y_3)$ та $2P\ (x_4, y_4)$ на кривій $y^2 = x^3 + 17$, якщо

№	18	1
P	(-1,4)	(4,9)
Q	(4,9)	(2,5)

Перевірити , чи належать точки кривій. Знайти координати точки $R = P + Q = (x_3, y_3)$ та $2P\ (x_4, y_4)$ на кривій $y^2 = x^3 + 3x+3 \pmod{11}$, якщо

№	20	21	22	23	23	25
P	(7,9)	(7,2)	(8,0)	(9,0)	(0,6)	(0,5)
Q	(5,0)	(9,0)	(0,5)	(7,9)	(7,2)	(7,9)

Практичне заняття 7

Сліди і базиси розширеного поля

Теоретичні відомості

Операції в розширених полях вимагають введення таких понять, як слід елемента поля та базису поля.

Нехай $F = F_p$ - просте поле і $K = F_p^n$- його розширення.

Визначення. Слідом елемента $\alpha \in K$ над полем F називається сума сполучених елементів поля K

$$Tr_{K/F}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \ldots + \alpha^{p^{m-1}}.$$

Зокрема, слід елемента над полем F_2 визначається сумою

$$Tr(\alpha) = \alpha + \alpha^2 + \alpha^4 + \ldots + \alpha^{2^{n-1}}.$$

Розширене поле Галуа F_p^n є n - мірним векторним простором над полем F_p. Базисом цього поля називається будь-яка множина з n лінійно незалежних елементів поля $\{\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n\}$. Кожен елемент поля надається як n - мірний вектор з координатами з поля F_p (або поліном степеня $n-1$ з коефіцієнтами з F_p). Його також можна виразити як лінійну комбінацію векторів базису.

$$\beta = c_1\alpha_1 + c_2\alpha_2 + c_3\alpha_3 + \ldots + c_n\alpha_n, c_i \in F_p.$$

Теорема 7.1

Елементи $\{\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n\}$ поля F_p^n утворюють його базис над полем F_p тоді і тільки тоді, коли визначник матриці Вандермонда

$$det(A) = \begin{vmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^p & \alpha_2^p & \ldots & \alpha_n^p \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_1^{p^{n-1}} & \alpha_2^{p^{n-1}} & \ldots & \alpha_n^{p^{n-1}} \end{vmatrix} \neq 0,$$

або визначник

$$\Delta \quad (\alpha_1, \alpha_2, \ldots, \alpha_n) = \begin{vmatrix} Tr(\alpha_1\alpha_1) & Tr(\alpha_1\alpha_2) & \ldots & Tr(\alpha_1\alpha_n) \\ Tr(\alpha_2\alpha_1) & Tr(\alpha_2\alpha_2) & \ldots & Tr(\alpha_2\alpha_n) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ Tr(\alpha_n\alpha_1) & Tr(\alpha_n\alpha_2) & \ldots & Tr(\alpha_n\alpha_n) \end{vmatrix} \neq 0.$$

Із множини всяких базисів найбільш розповсюдженими є поліноміальний і нормальний базиси поля F_p^n.

Поліноміальний базис

Поліноміальний базис, звичайно, будується за допомогою послідовних степенів примітивного елементу поля $\{1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{n-1}\}$. Його назва зв'язана з тим , що при $x = \alpha$ всі операції в полі здійснюються за модулем мінімального полінома елемента α. Примітивний елемент α тут є утворюючим елементом мультиплікативної групи поля.

Наприклад.

Розглянемо поле F_2^4. Елементами цього поля є 16 векторів.

Використовуємо при обчисленнях поліном $f(x) = x^4 + x + 1$ (незвідний).

Помітимо, що молодший розряд у поліноміальному базисі звичайно записується праворуч.

Зображення елементів будуються наступним чином. "0" – 0000.

"1" – одиниця тільки в розряді x^0, "α" – одиниця тільки в розряді x^1 і т. д.

Можна помітити , що при нульовому старшому розряді наступний елемент утворюється зсувом ліворуч попереднього на один розряд з додаванням праворуч нуля. Загальне правило. Зображення елементу – це остача від ділення на незвідний поліном.

Побудуємо, наприклад, елемент α^5.

α^5	$\alpha^4 + \alpha + 1$
$\alpha^5 + \alpha^2 + \alpha$	α
$\alpha^2 + \boldsymbol{\alpha}$	

Остача від ділення у даному разі $\alpha^2 + \boldsymbol{\alpha}$. Тобто α^5 запишеться у поліноміальному базисі як 0110. Дивимося таблицю 7.1.

Таблиця 7.1

Експоненціальна та векторна форми надання елементів поля F_2^4 (поліноміальне надання)

α^i	x^3, x^2, x^1, x^0	α^i	x^3, x^2, x^1, x^0
0	0000	α^7	1011
1	0001	α^8	0101
α	0010	α^9	1010
α^2	0100	α^{10}	0111
α^3	1000	α^{11}	1110
α^4	0011	α^{12}	1111
α^5	0110	α^{13}	1101
α^6	1100	α^{14}	1001

Зауваження. Ми працюємо в двійковому полі. Тому завжди пишемо "+" ($-1\ (mod\ 2) = 1$). Парна кількість однакових членів скорочується, непарна залишається в одному екземплярі.

Розглянемо основні операції у поліноміальному базисі.

Додавання:

(0101)+(1101)=(1000).

Множення :

(0101)(1101)=$(x^2 + 1) \cdot (x^3 + x^2 + 1)(mod\ f\ (x)) = x^5 + x^4 + x^2 + x^3 + x^2 + 1(mod\ f\ (x)) = (x^4 + x + 1)(x + 1) + (x^3 + x^2)(mod\ f\ (x)) = x^3 + x^2 = 1100.$

Зведення в степінь: $(0010)^2 = (0010)(0010) = x \cdot x(mod\ f\ (x)) = (x^2)(mod\ f\ (x)) = x^2 = (0100).(0010)^4 = (0010)^2 \cdot (0010)^2 = x^2 \cdot x^2(mod\ f\ (x) = (x^4 + x + 1) \cdot 1 + (x + 1)(mod\ f\ (x)) = x + 1 = (0011)$

$(0010)^5 = (0010)^4 \cdot (0010) = (0011) \cdot (0010) = (x + 1) \cdot x(mod\ f\ (x)) =$

$= (x^2 + x)\ mod\ f\ (x) = (x^4 + x + 1) \cdot 0 + (x^2 + x)\big(mod\ f\ (x)\big) = x^2 + x =$

$= (0110)$

Мультиплікативна інверсія:

Мультиплікативною інверсією для $g^7 = (1011)$ є $g^{-7(mod\,15)} = g^{8(mod\,15)} = (0101)$.

Дійсно $g^7 \cdot g^8 = (1011) \cdot (0101) = g^0$.

Нормальний базис

Нормальний базис над полем F_p визначається як множина сполучених елементів поля $N = \{\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{n-1}}\}$ з підходящим вибором елемента α. Розглянемо далі властивості НБ $N = \{\beta, \beta^2, \beta^4, \ldots, \beta^{2^{n-1}}\}$ над полем F_2.

На елемент β тут накладається необхідна умова: $Tr(\beta) = 1$. У той же час β не обов'язково є примітивним.

Помітимо, що молодший розряд НБ звичайно записується ліворуч (на відміну від поліноміального, у якому молодший розряд прийнятий записувати праворуч). Кожен наступний елемент базису є циклічним зрушенням праворуч попереднього.

Так як $Tr(\beta) = \beta + \beta^2 + \beta^4 + \beta^8 + \ldots + \beta^{2^{n-1}} = 1$, елемент 1 поля F_2^n визначається координатами $1 = (1,1,1,\ldots,1)$. Як бачимо, векторне надання елемента 1 поля F_2^n в поліноміальному і нормальному базисах різні.

Для порівняння двійкове надання елементів у поліноміальному і нормальному базисах надані в таблиці 7.2.

Таблиця 7.2

Двійкове надання елементів у поліноміальному і нормальному базисах

α^i	$x^3, x^2, x,\ 1$	$\beta, \beta^2, \beta^4, \beta^8$	α^i	$x^3, x^2, x,\ 1$	$\beta, \beta^2, \beta^4, \beta^8$
0	0000	0000	α^7	1011	1110
1	0001	1111	α^8	0101	0011
α	0010	1001	α^9	1010	0001
α^2	0100	1100	α^{10}	0111	1010
α^3	1000	1000	α^{11}	1110	1101
α^4	0011	0110	α^{12}	1111	0010
α^5	0110	0101	α^{13}	1101	1011
α^6	1100	0100	α^{14}	1001	0111

Довільний елемент поля в базисі N представляється як

$$A = a_0\beta + a_1\beta^2 + a_2\beta^4 + \ldots + a_{n-1}\beta^{2^{n-1}}, a_i \in F_2.$$

Зведення у квадрат елемента A в нормальному базисі дає

$$A^2 = a_0\beta^2 + a_1\beta^4 + a_2\beta^8 + \ldots + a_{n-2}\beta^{2^{n-1}} + a_{n-1}\beta^{2^n}$$

$$= a_{n-1}\beta + a_0\beta^2 + a_1\beta^4 + a_2\beta^8 + \ldots + a_{n-2}\beta^{2^{n-1}}, a_i \in F_2.$$

Таким чином, операція зведення у квадрат (або витягу кореня квадратного зводиться до циклічного зрушення вправо (або вліво) векторного представлення елемента. Це одне з важливих технологічних переваг нормального базису перед поліноміальним. Іншим його достоїнством є простота визначення сліду елемента.

Слід елемента дорівнює 0 при парній вазі його векторного представлення в НБ , або 1 – при непарній вазі. Це властивість радикально спрощує визначення сліду елемента в НБ.

Наприклад: елемент $\alpha^4 = 0110$ у нормальному базисі (парна вага векторного надання). Слід елемента дорівнює 0, дійсно $Tr(\alpha) = \alpha + \alpha^2 + \alpha^4 + \ldots + \alpha^{2^{n-1}} = \alpha^4 + \alpha^8 + \alpha^{16} + \alpha^{32} = \alpha^4 + \alpha^8 + \alpha^1 + \alpha^2 =$

$$0011 + 0101 + 0010 + 0100 = 0000.$$

Приклад 1

Визначимо елементи поля $F_q, q = 2^4$, прийняв у якості утворюючого незвідний поліном $P(x) = x^4 + x + 1 = 10011$. Тобто будуємо поліноміальне надання.

Рішення

Нуль поля можна надати вектором 0000, одиницю – 0001. Нехай ненульові елементи поля визначаються як степені x^k, $k = 1,2,3, \ldots, 14$. Тоді $x = 0010$, $x^2 = 0100$, $x^3 = 1000$, и далі

$$x^4 \, mod \, P\,(x) = res\{x^4/(x^4 + x + 1)\} = x + 1 = 0011.$$

$$x^5 \, mod \, P\,(x) = res\{x^5/(x^4 + x + 1)\} = x^2 + 1 = 0110 \qquad (*)$$

Подібним чином визначаються всі елементи.

Співвідношення (*) означає, що $x = \alpha$ є коренем рівняння $x^4 + x + 1 = 0$, для котрого $\alpha^4 = \alpha + 1$. Таким чином ненульові елементи поля можна

розглядати як степені кореня утворюючого полінома. Згідно з обчисленнями можна заповнити таблицю 7.1.

Приклад 2

Побудувати нормальний базис поля F_2^4 над полем F_2. Поліноміальне надання поля надано в попередньому завданні. Тобто заповнити третю колонку наступної таблиці.

α^i	$x^3, x^2, x, 1$	$\beta, \beta^2, \beta^4, \beta^8$	α^i	$x^3, x^2, x, 1$	$\beta, \beta^2, \beta^4, \beta^8$
0	0000	0000	α^7	1011	1110
1	0001	1111	α^8	0101	0011
α	0010	1001	α^9	1010	0001
α^2	0100	1100	α^{10}	0111	1010
α^3	1000	1000	α^{11}	1110	1101
α^4	0011	0110	α^{12}	1111	0010
α^5	0110	0101	α^{13}	1101	1011
α^6	1100	0100	α^{14}	1001	0111

У якості утворюючого елементу для переходу до нормального базису потрібно взяти елемент зі слідом 1. Половина елементів в таблиці має слід «0», половина «1».

Для $\beta = \alpha^2$ рахуємо слід за формулою:

$$Tr(\alpha) = \alpha + \alpha^2 + \alpha^4 + \ldots + \alpha^{2^{n-1}}$$

$$\boldsymbol{Tr}(\alpha^2) = \alpha^2 + \alpha^4 + \alpha^8 + \alpha^{16-15} = \alpha^2 + \alpha^4 + \alpha^8 + \alpha^1 = 0100$$

$$0011$$

$$0101$$

$$\underline{0010}$$

$$0000$$

$$Tr(\alpha^2) = 0$$

Зображення елементів виписуємо з таблиці 6.1 (поліноміальне надання). Додавання за правилом: 0⊕0=0, 0⊕1=1, 1⊕0=1, 1⊕1=0.

Слід $\alpha^2 = \mathbf{0}$. Його неможна взяти за утворюючий**.**

Перевіряємо елемент α^3.

$Tr(\beta) = Tr(\alpha^3) = \beta + \beta^2 + \beta^4 + \beta^8 + ... + \beta^{2^{n-1}} = \alpha^3 + \alpha^6 + \alpha^{12} + \alpha^{24} =$

$\alpha^3 + \alpha^6 + \alpha^{12} + \alpha^9 = 1000 + 1100 + 1010 + 1111 = 1$)

Слід $\alpha^3 = 1$.

Так як $Tr(\alpha^3) = 1$, елемент $\beta = \alpha^3$ можна взяти за утворюючий для переходу до нормального базису.

У якості нормального базису потрібно взяти набір сполучених елементів поля.

Перевіримо такий набір сполучених елементів $N = \{\beta, \beta^2, \beta^4, \beta^8\}$.

(F_2^4, p=2).

Розрахуємо визначник матриці Вандермонда за допомогою теореми 7.1.

Елементи $\{\alpha_1, \alpha_2, \alpha_3, ..., \alpha_n\}$ поля F_p^n утворюють базис над полем F_p тоді і тільки тоді, коли визначник матриці Вандермонда

$$\Delta(\alpha_1, \alpha_2, ..., \alpha_n) = \begin{vmatrix} Tr(\alpha_1\alpha_1) & Tr(\alpha_1\alpha_2) & ... & Tr(\alpha_1\alpha_n) \\ Tr(\alpha_2\alpha_1) & Tr(\alpha_2\alpha_2) & ... & Tr(\alpha_2\alpha_n) \\ ..... & ..... & ..... & ..... \\ Tr(\alpha_n\alpha_1) & Tr(\alpha_n\alpha_2) & ... & Tr(\alpha_n\alpha_n) \end{vmatrix} \neq 0.$$

Перевіряємо:

α_1 α_2 α_3 α_4

β, β^2, β^4, β^8

Тут буде подвійна підстановка:

Tr ($\alpha_1\alpha_1$) = Tr (β^2).

Tr ($\alpha_1\alpha_2$) = Tr (β^3).

…

$Tr(\beta^2) = \beta^2 + \beta^4 + \beta^8 + \beta^{16-15} = \beta^2 + \beta^4 + \beta^8 + \beta^1 =$

$= (\alpha^3)^2 + (\alpha^3)^4 + (\alpha^3)^8 + (\alpha^3)^1 = \alpha^6 + \alpha^{12} + \alpha^{24-15} + \alpha^3 =$

$$=\alpha^{6}+\alpha^{12}+\alpha^{9}+\alpha^{3}=\begin{array}{r}1100\\1111\\1010\\\underline{1000}\\0001\end{array}$$

І так далі. Переходимо до визначника з нуликами та одиничками.

Згідно з теоремою:

$$\Delta(\alpha_1,\alpha_2,\alpha_3,\alpha_4)=\begin{vmatrix} Tr(\beta^2) & Tr(\beta^3) & Tr(\beta^5) & Tr(\beta^9)\\ Tr(\beta^3) & Tr(\beta^4) & Tr(\beta^6) & Tr(\beta^{10})\\ Tr(\beta^5) & Tr(\beta^6) & Tr(\beta^8) & Tr(\beta^{12})\\ Tr(\beta^9) & Tr(\beta^{10}) & Tr(\beta^{12}) & Tr(\beta)\end{vmatrix}=\begin{vmatrix}1&1&0&1\\1&1&1&0\\0&1&1&1\\1&0&1&1\end{vmatrix}=$$

$$\begin{vmatrix}1&1&0\\1&1&1\\0&1&1\end{vmatrix}+\begin{vmatrix}1&1&0\\0&1&1\\1&1&1\end{vmatrix}+\begin{vmatrix}1&1&1\\0&1&1\\1&0&1\end{vmatrix}=1.$$

Сукупність елементів $N=\{\beta\ ,\beta^2\ ,\beta^4\ ,\beta^8\},\beta=\alpha^3$,утворюють базис і є системою лінійно незалежних векторів. $N=\{\beta\ ,\beta^2\ ,\beta^4\ ,\beta^8\}-$ можна взяти у якості базису з утворюючим елементом $\beta=\alpha^3$

Для переходу до нормального базису пишеться 3 рівняння.

1. $M_1(\alpha)=\alpha^4+\alpha+1=0$ (незвідний поліном, за яким ми будували поліноміальне надання дорівнюємо до 0).

2. $\beta+\beta^2+\beta^4+\beta^8=1$ (Сума елементів нормального базису завжди 1).

3. $\beta=\alpha^3$ (Рівняння записано згідно обраного елементу для переходу до нормального базису).

Визначимо елементи нормального базису.

$\alpha^{6}=\beta^{2}$.

$\alpha^{12}=\beta^{4}$.

$\alpha^{24-16=9}=\beta^{8}$.

$\alpha^0 = 1 \quad \beta + \beta^2 + \beta^4 + \beta^8 = 1.$

Перше рівняння помножимо почлено на α^2.

$\alpha^6 + \alpha^3 = \alpha^2.$

$\alpha^6 = \beta^2$, а $\alpha^3 = \beta.$

$\alpha^2 = \alpha^6 + \alpha^3 = \beta + \beta^2.$

$\alpha^4 = \beta^2 + \beta^4.$

$\alpha^8 = \beta^4 + \beta^8.$

$\alpha^{16-15=1} = \beta + \beta^8.$

Неважко впевнитися, що зведення у квадрат довільного елемента поля зводиться у НБ к циклічному зсуву праворуч двійкового вектору. Крім того, всі елементи у НБ парної ваги мають слід 0, а непарної ваги – слід 1.

Завдання до практичного заняття 7

Завдання 1.

Взяти незвідний поліном у полі F_2^4 . Поліном $f(x)=x^4+x^3+1$. Побудувати поліноміальне надання. Обрати утворюючій елемент, перейти до нормального базису.

1. $A=\beta^{12}, B=\beta^{10}$
2. $A=\beta^{7}, B=\beta^{10}$
3. $A=\beta^{12}, B=\beta^{17}$
4. $A=\beta^{8}, B=\beta^{14}$
5. $A=\beta^{9}, B=\beta^{13}$
6. $A=\beta^{7}, B=\beta^{14}$
7. $A=\beta^{12}, B=\beta^{5}$
8. $A=\beta^{11}, B=\beta^{4}$

Взяти незвідний поліном у полі F_2^3 . Поліном $f(x)=x^3+x+1$. Побудувати поліноміальне надання. Обрати утворюючій елемент, перейти до нормального базису.

9. $A=\beta^{4}, B=\beta^{6}$
10. $A=\beta^{5}, B=\beta^{6}$

11. $A=\beta^5, B=\beta^2$

12. $A=\beta^3, B=\beta^6$

13 . $A=\beta^5, B=\beta$

14. $A=\beta^4, B=\beta^2$

Взяти незвідний поліном у полі F_2^3 . Поліном $f(x)=x^3+x^2+1$. Побудувати поліноміальне надання. Обрати утворюючій елемент, перейти до нормального базису.

15. $A=\beta^4, B=\beta^6$

16 . $A=\beta^5, B=\beta^6$

17. $A=\beta^5, B=\beta^2$.

18. $A=\beta^5, B=\beta^2$

19. $A=\beta^3, B=\beta^6$

20 . $A=\beta^5, B=\beta$

21. $A=\beta^4, B=\beta^2$

22. $A=\beta^4, B=\beta^6$

23 . $A=\beta^5, B=\beta^6$

24. $A=\beta^5, B=\beta^2$.

25. $A=\beta^4, B=\beta^6$

Практичне заняття 8

Оптимальний нормальний базис поля F_2^n

Теоретичні відомості

Означення. Нормальний базис $\{\beta, \beta^2, \beta^4, \ldots, \beta^{2^{n-1}}\}$ поля F_2^n називається оптимальним , якщо виконується умова

$$\beta^{2^i}\beta^{2^k} = \beta^{2^r} + \beta^{2^s}, \quad i \neq k, \quad r \neq s.$$

Відповідно до означення нормальний базис складається із сполучених елементів поля.

Нехай ми маємо нормальний базис

$$N = \{\beta, \beta^2, \beta^4, \ldots, \beta^{2^{n-1}}\}.$$

Нехай елементи A і B у оптимальному нормальному базисі представлені у вигляді лінійних комбінацій або векторів $A = (a_0, a_1, a_2, \ldots, a_{n-1})$, $B = (b_0, b_1, b_2, \ldots, b_{n-1})$, причому $A = AN^T$, $B = BN^T$, де T – знак транспонування. Тоді добуток елементів A і B поля $C = AB = \sum_{i=0}^{n-1} c_i \beta^{2^i}$ з урахуванням, що

$$A = a_0\beta + a_1\beta^2 + a_2\beta^4 + \ldots + a_{n-1}\beta^{2^{n-1}},$$
$$B = b_0\beta + b_1\beta^2 + b_2\beta^4 + \ldots + b_{n-1}\beta^{2^{n-1}},$$

можна представити в матричній формі

$$C = A\Delta B^T,$$

де Δ-матриця визначається наступним чином

$$\Delta = N^T N = \left[\beta^{2^i+2^k}\right] = \begin{bmatrix} \beta^2 & \beta^3 & \beta^5 & \cdots & \beta^{2^{n-1}+1} \\ \beta^3 & \beta^4 & \beta^6 & \cdots & \beta^{2^{n-1}+2} \\ \cdots & \cdots & \cdots & \cdots & \\ \beta^{2^{n-1}+1} & \beta^{2^{n-1}+2} & \cdots & \beta & \end{bmatrix}, \quad i, \quad k = 0, \quad n-1.$$

Можемо обчислити елементи Δ-матриці. Елементами її першого рядка дорівнюватимуть:

$$\beta^3 = \beta\beta^2 = (\theta + \theta^{-1})(\theta^2 + \theta^{-2}) = (\theta^3 + \theta^{-3}) + (\theta + \theta^{-1});$$
$$\beta^5 = \beta\beta^4 = (\theta + \theta^{-1})(\theta^4 + \theta^{-4}) = (\theta^5 + \theta^{-5}) + (\theta^3 + \theta^{-3}); \qquad (8.1)$$
$$\beta^9 = \beta\beta^8 = (\theta + \theta^{-1})(\theta^8 + \theta^{-8}) = (\theta^9 + \theta^{-9}) + (\theta^7 + \theta^{-7}).$$

Виявляється, щоб виразити елементи Δ-матриці у вигляді суми , немає необхідності визначати елемент θ розширення.

Суть методу, запропонованого А. Бессаловим й А. Теліженко, складається в побудові таблиці відповідності послідовних степенів елементів β й θ, при цьому степені елемента β зростають як $2^i \, mod \ (2^m - 1)$, тоді як редукція степенів θ береться за $mod\, p$, тому що $\theta^p = 1$.

Умова означає, що степені $deg \ (\theta)$ $(mod\, p)$ пробігають або всі значення від 1 до $2m$ мультиплікативної циклічної групи F_p^* при послідовному подвоєнні (якщо $2^m = -1$), або половину всіх значень (якщо $2^m = 1$).

В обох випадках в області $i = 0,1, \ . \ . \ . \ , \ m - 1$ половина інших значень степенів $r = 2^i \, mod\, p$ може бути представлена від'ємними значеннями $(-r)\, mod\, p \equiv (p - r)\, mod\, p$. Співвідношення дозволяє при цьому однозначно виразити елементи Δ-матриці через елементи нормального базису у вигляді

$$\begin{bmatrix} \beta \\ \beta^2 \\ \beta^4 \\ \beta^8 \\ \beta^{16} \end{bmatrix} \cdot [\beta \ \beta^2 \ \beta^4 \ \beta^8 \ \beta^{16}] = \begin{bmatrix} \beta^2 & \beta^3 & \beta^5 & \beta^9 & \beta^{17} \\ \beta^3 & \beta^4 & \beta^6 & \beta^{10} & \beta^{18} \\ \beta^5 & \beta^6 & \beta^8 & \beta^{12} & \beta^{20} \\ \beta^9 & \beta^{10} & \beta^{12} & \beta^{16} & \beta^{24} \\ \beta^{17} & \beta^{18} & \beta^{20} & \beta^{24} & \beta \end{bmatrix}$$

Важливо відзначити, що якщо ОНБ існує при даному m, то він єдиний (з точністю до циклічного зрушення елементів β^{2^i}).

Приклад 1

Визначимо Δ-матрицю для нормального базису $N = \{\beta \ , \beta^2 \ , \beta^4 \ , \beta^8\}$, $\beta = \alpha^3$. Далі знайдемо добуток елементів $A = 1110$, $B = 0101$ у нормальному базисі.

Спочатку потрібно побудувати таблицю поліноміального та нормального надання елементів за відповідним незвідним поліномом. У нас для прикладу взято незвідний поліном у полі F_2^4 $f(x) = x^4 + x + 1$. Як це можна зробити пояснюється на практиці 7. Таблицю теж взято із прикладу заняття 7 (таблиця 8.1).

Таблиця 8.1

Двійкове надання елементів у поліноміальному і нормальному базисах

α^i	$x^3, x^2, x,\ 1$	$\beta, \beta^2, \beta^4, \beta^8$	α^i	$x^3, x^2, x,\ 1$	$\beta, \beta^2, \beta^4, \beta^8$
0	0000	0000	α^7	1011	1110
1	0001	1111	α^8	0101	0011
α	0010	1001	α^9	1010	0001
α^2	0100	1100	α^{10}	0111	1010
α^3	1000	1000	α^{11}	1110	1101
α^4	0011	0110	α^{12}	1111	0010
α^5	0110	0101	α^{13}	1101	1011
α^6	1100	0100	α^{14}	1001	0111

Для нашого прикладу Δ - матриця має вигляд :

$$\begin{bmatrix} \beta \\ \beta^2 \\ \beta^4 \\ \beta^8 \end{bmatrix} \cdot \begin{bmatrix} \beta & \beta^2 & \beta^4 & \beta^8 \end{bmatrix} = \begin{bmatrix} \beta^2 & \beta^3 & \beta^5 & \beta^9 \\ \beta^3 & \beta^4 & \beta^6 & \beta^{10} \\ \beta^5 & \beta^6 & \beta^8 & \beta^{12} \\ \beta^9 & \beta^{10} & \beta^{12} & \beta \end{bmatrix}.$$

Так як β – елемент 5-го порядку $\left(\beta^5 = 1\right)$, і відповідно до таблиці 8.1 маємо:

$$\beta^3 = \alpha^9 = \beta^8;$$
$$\beta^6 = \left(\beta^3\right)^2 = \left(\alpha^9\right)^2 = \alpha^{18} = \alpha^3 = \beta;$$
$$\beta^{10} = \left(\beta^5\right)^2 = 1^2 = 1;$$
$$\beta^{12} = \left(\beta^6\right)^2 = \beta^2;$$
$$\beta^9 = \beta^6\beta^3 = \beta\beta^3 = \beta^4.$$

Дану матрицю можна виразити через елементи НБ:

$$\Delta = \begin{bmatrix} \beta^2 & \beta^8 & 1 & \beta^4 \\ \beta^8 & \beta^4 & \beta & 1 \\ 1 & \beta & \beta^8 & \beta^2 \\ \beta^4 & 1 & \beta^2 & \beta \end{bmatrix}.$$

Тут $\beta + \beta^2 + \beta^4 + \beta^8 = 1$, тому в розкладанні $\Delta = \sum_{i=0}^{n-1} \Delta^{(i)} \beta^{2^i}$ матриця $\Delta^{(0)}$ має одиниці на позиціях, у яких є доданок β.

$$\Delta^{(0)} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}.$$

Інші матриці $\Delta^{(i)}$, $i = 1,2,3$ утворюються із $\Delta^{(0)}$ циклічним зсувом позицій уздовж головної діагоналі $(i,k) \to (i+1, k+1)\ (mod\, n)$.

Наприклад,

$$\Delta^{(1)} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1` \\ 0 & 1 & 1 & 0 \end{bmatrix}.$$

Можна побачити, що $\Delta^{(1)}$ має одиниці на позиціях, у яких є доданок β^2. $\Delta^{(2)}$ має одиниці на позиціях, у яких є доданок β^4, а $\Delta^{(3)}$ має одиниці на позиціях, у яких є доданок β^8.

Ваги всіх матриць $\Delta^{(i)}$ (число одиниць) однакові. У нашому прикладі вага матриць мінімальна й дорівнює $W_0 = 2n - 1 = 7$. Нормальні базиси з мінімальною вагою матриці $\Delta^{(0)}$ називають оптимальними (тому що гарантують мінімальний об'єм обчислень). Тепер просто записати формули для обчислення коефіцієнтів c_j добутку $C = AB$.

Запишемо c_0.

$$c_0 = (a_0, a_1, a_2, \dots, a_{n-1})\ \Delta^{(0)} \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix} =$$

$$= (a_0, a_1, a_2, \ldots, a_{n-1}) \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} =$$

$= a_0 b_2 + a_1(b_2 + b_3) + a_2(b_0 + b_1) + a_3(b_1 + b_3)$.

Аналогічно розраховуються c_1, c_2, c_3 з використанням матриць $\Delta^{(1)}$, $\Delta^{(2)}, \Delta^{(3)}$.

Отримуємо:

$$c_0 = a_0 b_2 + a_1(b_2 + b_3) + a_2(b_0 + b_1) + a_3(b_1 + b_3);$$
$$c_1 = a_1 b_3 + a_2(b_3 + b_0) + a_3(b_1 + b_2) + a_0(b_2 + b_0);$$
$$c_2 = a_2 b_0 + a_3(b_0 + b_1) + a_0(b_2 + b_3) + a_1(b_3 + b_1);$$
$$c_3 = a_3 b_1 + a_0(b_1 + b_2) + a_1(b_3 + b_0) + a_2(b_0 + b_2).$$

Вирази для розрахунку кожного наступного коефіцієнта c_j пов'язане з попереднім приростом на $1(mod\ 4)$ всіх індексів коефіцієнтів a_i, b_k .

У нашому прикладі $A = 1110, B = 0101$. Тоді

$$c_0 = 1 \cdot 0 + 1 \cdot (0 + 1) + 1 \cdot (0 + 1) + 0 \cdot (1 + 1) = 0;$$
$$c_1 = 1 \cdot 1 + 1 \cdot (0 + 1) + 0 \cdot (1 + 0) + 1 \cdot (0 + 0) = 0;$$
$$c_2 = 1 \cdot 0 + 0 \cdot (0 + 1) + 1 \cdot (0 + 1) + 1 \cdot (1 + 1) = 1;$$
$$c_3 = 0 \cdot 1 + 1 \cdot (1 + 0) + 1 \cdot (1 + 0) + 1 \cdot (0 + 0) = 0.$$

У такий спосіб $C = 0010$. Перевіримо цей результат, користуючись експонентним поданням елементів. Відповідно до таблиці $A = \alpha^7, B = \alpha^5$, тоді $C = \alpha^{7+5} = \alpha^{12} = 0010$.

Іншими словами, кожен елемент Δ -матриці (крім елементів головної діагоналі) представляється лише двома доданками в НБ, що забезпечує мінімальне число одиниць у матриці $\Delta^{(0)}$, що дорівнює $C_N = 2m - 1$ (одна одиниця в першому рядку і по двох – в інших). Тим самим досягається мінімальне число парціальних додавань в операції множення або, іншими словами, мінімальна обчислювальна складність множення.

Завдання до практичного заняття 8

Завдання 1.

Продовжити виконання завдання з попередньої практики.

Взяти незвідний поліном у полі F_2^4 . Поліном $f(x)=x^4+x^3+1$. Побудувати поліноміальне надання. Обрати утворюючій елемент, перейти до нормального базису. Перемножити елементи A та B у нормальному базисі $\{\beta, \beta^2, \beta^4, \beta^8\}$ поля F_2^4.

1. $A=\beta^{12}, B=\beta^{10}$
2. $A=\beta^{7}, B=\beta^{10}$
3. $A=\beta^{12}, B=\beta^{17}$
4. $A=\beta^{8}, B=\beta^{14}$
5. $A=\beta^{9}, B=\beta^{13}$
6. $A=\beta^{7}, B=\beta^{14}$
7. $A=\beta^{12}, B=\beta^{5}$
8. $A=\beta^{11}, B=\beta^{4}$

Взяти незвідний поліном у полі F_2^3 . Поліном $f(x)=x^3+x+1$. Побудувати поліноміальне надання. Обрати утворюючій елемент, перейти до нормального базису. Перемножити елементи A та B у нормальному базисі $\{\beta, \beta^2, \beta^4\}$ поля F_2^3.

9. $A=\beta^{4}, B=\beta^{6}$
10. $A=\beta^{5}, B=\beta^{6}$
11. $A=\beta^{5}, B=\beta^{2}$
12. $A=\beta^{3}, B=\beta^{6}$
13. $A=\beta^{5}, B=\beta$
14. $A=\beta^{4}, B=\beta^{2}$

Взяти незвідний поліном у полі F_2^3 . Поліном $f(x)=x^3+x^2+1$. Побудувати поліноміальне надання. Обрати утворюючій елемент, перейти до нормального базису. Перемножити елементи A та B у нормальному базисі $\{\beta, \beta^2, \beta^4\}$ поля F_2^3.

15. $A=\beta^{4}, B=\beta^{6}$
16. $A=\beta^{5}, B=\beta^{6}$
17. $A=\beta^{5}, B=\beta^{2}$.

18. $A=\beta^5, B=\beta^2$

19. $A=\beta^3, B=\beta^6$

20 . $A=\beta^5, B=\beta$

21. $A=\beta^4, B=\beta^2$

22. $A=\beta^4, B=\beta^6$

23 . $A=\beta^5, B=\beta^6$

24. $A=\beta^5, B=\beta^2$.

25. $A=\beta^4, B=\beta^6$

Рекомендована література

1. Горбенко І. Д. ″ Криптографічний захист інформації ″. Навч. посібник Харків, ХНУРЕ, 2004 р.

2. Вербіцький О. В. Всуп до криптології. - Львів.: Видавництво науково-технічної літератури, 1998. - 247 с.

3. Бессалов А.В., Телиженко А.Б. Криптосистеми на еліптичних кривих: Навч. посібн. – К.: ІВЦ «Політехніка», 2004. – 224с.

4. Криптологія: навч. посібник / М.Н. Курко, П.М. Лісовський, Ю.П. Лісовська. — К.: Видавничий дім «Кондор», 2020. — 248 с.

5. Безпека інформаційних систем і технологій: Навч. посібник / В. І. Єсін, О. О. Кузнецов, Л. С. Сорока. – Х. : ХНУ імені В. Н. Каразіна, 2013. – 632 с.

6. Горбенко І. Д. Прикладна криптологія. Теорія. Практика. Застосування : Монографія / І. Д. Горбенко, Ю. І. Горбенко. – Харків : Видавництво “Форт”, 2012. – 880 с.: іл.

7. Богуш В. М. Криптографічні застосування елементарної теорії чисел : Навч. посібник / В. М. Богуш, В. А. Мухачов. – К. : Державний ун-т інформаційно-комунікаційних технологій, 2006. – 126 с.: іл.

Електронне навчальне видання комбінованого використання
Можна використовувати в локальному та мережному режимі

Лисицький Костянтин Евгенійович
Лисицька Ірина Вікторівна
Узлов Дмитро Юрійович

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

Методичні вказівки
до практичних занять з дисципліни для здобувачів вищої освіти першого (бакалаврського) рівня за спеціальністю 151 «Автоматизація та комп'ютерно-інтегровані технології» (174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка»)

В авторській редакції

Підписано до розміщення 23.04.2025. Гарнітура Times New Roman.
Ум. друк. арк. 3,99. Обсяг 2,632 Мб. Зам. № 160/25.

Харківський національний університет імені В. Н. Каразіна,
61022, м. Харків, майдан Свободи, 4.
Свідоцтво суб'єкта видавничої справи ДК № 3367 від 13.01.2009
Видавництво ХНУ імені В. Н. Каразіна