

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт з дисципліни
“Прикладна криптографія”
для студентів спеціальності 125 «Кібербезпека»
усіх форм навчання

2019

Методичні вказівки до виконання лабораторних робіт з дисципліни “Прикладна криптографія” для студентів спеціальності 125 «Кібербезпека» усіх форм навчання / Укл.: Г.Л.Козіна. – Запоріжжя: НУ «Запорізька політехніка», 2019. – 34 с.

Укладач: Г.Л.Козіна, доцент, канд. фіз.-мат. наук

Рецензент: Л.М. Карпуков, проф., доктор техн. наук

Відповідальний

за випуск: Г.Л.Козіна, доцент, канд. фіз.-мат. наук

Затверджено
на засіданні кафедри
захисту інформації
Протокол № 2
від 26.09.2019 р.

Рекомендовано до видання
НМК факультету
радіоелектроніки і телекомунікацій
Протокол № 3
від 03.10.2019 р.

ЗМІСТ

Вступ	4
Лабораторна робота №1. Поняття теорії чисел	5
Лабораторна робота №2. Прості шифри	7
Лабораторна робота №3. Лінійні рекурентні послідовності	8
Лабораторна робота №4. Асиметричний алгоритм шифрування RSA.....	11
Лабораторна робота №5. Схема Діффі-Хеллмана в мультиплікативній групі.....	14
Лабораторна робота №6. Еліптичні криві над простим полем	16
Лабораторна робота №7. Стандарт цифрового підпису ECDSA над простим полем.....	18
Лабораторна робота №8. Еліптичні криві над розширеним полем.....	20
Лабораторна робота №9. Український стандарт цифрового підпису ДСТУ 4145-2002.....	22
Лабораторна робота №10. Основні криптоперетворення в американському стандарті шифрування FIPS 197 (алгоритм RIJNDAEL).....	25
Лабораторна робота №11. Основні криптоперетворення в українському стандарті шифрування ДСТУ 7624:2014	29
Література.....	33

ВСТУП

*Єдина гарантія надійності
криптографічних алгоритмів –
це їх абсолютна відкритість.*

Криптологія - наука , що складається з двох гілок : криптографія і криптоаналіз.

Криптографія – наука про способи перетворення інформації з метою її захисту від незаконних користувачів .

Сучасна криптографія розвивається за такими напрямками: шифрування, генерування [псевдо]випадкових послідовностей, хешування, цифровий підпис.

Шифрування (зашифрування) – процес застосування шифру до інформації (відкритого тексту), що захищається, в шифроване повідомлення (шифртекст, криптограму) за допомогою певних правил та ключової інформації.

Дешифрування – процес, зворотний шифруванню, тобто перетворення шифрованого повідомлення в інформацію, що захищається, за допомогою певних правил та ключової інформації.

Під ключем в криптографії розуміють змінний елемент шифру, який застосовується для криптоперетворення конкретного повідомлення.

[Псевдо]випадкові послідовності широко використовуються в криптоалгоритмах.

Хешування – криптоперетворення повідомлення в бітовий образ фіксованої довжини – використовується в схемах цифрового підпису, при зберіганні паролів.

Криптоаналіз – наука (і практика її застосування) про методи та способи розкриття криптоалгоритмів.

Здатність криптоалгоритму протистояти всіляким атакам на нього називають стійкістю алгоритму. Під атакою розуміють спробу розкриття криптоперетворення.

ЛАБОРАТОРНА РОБОТА № 1

ПОНЯТТЯ ТЕОРІЇ ЧИСЕЛ

Мета роботи: Ознайомитися з основними поняттями теорії чисел.

1.1 Завдання на лабораторну роботу

1. Представити власне прізвище записане латиницею у вигляді десяткового числа.
2. Перетворити десяткове число T на текст.
3. Виписати в конспект всі прості числа від 2 до 99.
4. Виписати в конспект таблицю відповідності шістнадцятирічних цифр десятковим числам та двійковим тетрадам (наприклад, $8_{16} = 8_{10} = 1000_2$, $C_{16} = 12_{10} = 1100_2$).
5. Знайти серед чисел a , b , c , d пари взаємно простих чисел.
6. Знайти $НСД(a, b)$, $НСД(a, b + c)$.
7. Знайти серед чисел $a + b$, c , d пари чисел, порівняних за модулем m .
8. Знайти суму і добуток чисел a , b , c , d за модулем m .
9. Знайти $a^b \bmod m$.
10. Обчислити значення функції Ейлера для кожного з чисел a , b , c , d .

Значення параметрів T, a, b, c, d, m візьміть із таблиці 1.1 згідно з номером варіанту N.

1.2 Зміст звіту

1. Титульний лист, тема і мета роботи.
2. Результати обчислень.
3. Висновки по роботі.

1.3 Контрольні питання

1. Які числа називаються простими? Взаємно простими?
2. Для чого використовується алгоритм Евкліда?
3. Які числа називаються порівняними за модулем m ?
4. За яким модулем всі цілі числа порівняні між собою?
5. Якими властивостями володіють порівняння?
6. Що таке клас залишків за модулем?
7. Що показує функція Ейлера? Як її обчислити?
8. Як формулюється теорема Ейлера?
9. Як формулюється мала теорема Ферма?
10. Як пов'язані теорема Ейлера і мала теорема Ферма?

Таблиця 1.1 – Варіанти завдань

N	T	a	b	c	d	m
1	6009318633877632121	45	37	27	111	17
2	88772934743480459988660078	76	24	19	33	9
3	22066599077835371	41	26	15	69	11
4	4859222852730381682	42	36	70	53	14
5	22643820939338093	71	52	39	87	15
6	5291294591267267956	18	67	35	49	4
7	24604245826172787	90	45	28	73	14
8	1206849699407272896621	35	23	92	15	8
9	5792036358531605868	64	79	39	22	6
10	91712171958636	77	42	59	60	17
11	1483985444626882588530	34	63	45	29	11
12	5071443942490206059	30	78	61	55	12
13	23775192852751730	51	91	43	27	8
14	360696279886943885423225	25	31	46	50	7
15	5075397850727279724	47	82	28	39	9
16	1280064142332243046254	55	71	9	34	23
17	1351521362425256502642	62	12	56	17	30
18	100833766215126275709825637	21	14	56	35	7

ЛАБОРАТОРНА РОБОТА № 2

ПРОСТІ ШИФРИ

Мета роботи: Ознайомитися з прикладами простих шифрів.

Використовуване програмне забезпечення: програми «Шифр_Полібія» та «Частотний криптоаналіз».

2.1 Завдання на лабораторну роботу

1. Запустити програму «Шифр_Полібія» (див. Додаток В).
2. Обрати мову, задати ключ, сформувати квадрат Полібія.
3. Виконати шифрування та розшифрування повідомлення.
4. Запустити програму «Частотний криптоаналіз».
5. Завантажити один з зашифрованих текстових файлів.
6. Скориставшись методом частотного криптоаналізу розкрити зашифрований текст. Виписати отриману таблицю заміन.
7. Порівняти частоти заміненних літер з еталоном.

2.2 Зміст звіту

1. Титульний лист, тема і мета роботи.
2. Повідомлення у відкритому та зашифрованому за квадратом Полібія вигляді.
3. Таблиця замін з частотами зустрічання літер. Уривок розкритого тексту.
4. Висновки по роботі.

2.3 Контрольні питання

1. Що є ключем в шифрі Полібія? Які вимоги висуваються до ключа?
2. За яким принципом формується квадрат Полібія?
3. Які ще відомі варіанти шифра Полібія?
4. Що таке таблиця замін? Які до неї вимоги?
5. Які різновиди шифру простої заміни існують?
6. Що таке частотний криптоаналіз?
7. Чи є шифр Полібія різновидом шифру простої заміни?

ЛАБОРАТОРНА РОБОТА № 3

ЛІНІЙНІ РЕКУРЕНТНІ ПОСЛІДОВНОСТІ

Мета роботи: Ознайомитися з генеруванням псевдовипадкових послідовностей, що задаються лінійними рекурентними співвідношеннями.

3.1 Завдання на лабораторну роботу

1. Визначити глибину n лінійної рекурентної послідовності S . Сформувати характеристичний многочлен лінійної рекурентної послідовності S і перевірити його на незвідність. Обчислити період лінійної рекурентної послідовності S при довільних n початкових значеннях x_i , $i = 1, 2, \dots, n$. З'ясувати, чи зміниться і як саме період лінійної рекурентної послідовності S при інших початкових значеннях x_i , $i = 1, 2, \dots, n$.

Зашифрувати повідомлення M , використовуючи в якості гами шифру сформовану послідовність.

Послідовність S та повідомлення M взяти із таблиці 3.1 згідно з номером варіанта N .

2. Визначити рекурентне співвідношення, що задає лінійну рекурентну послідовність глибини $n = 3$, ділянкою якої є $x_1, x_2, x_3, x_4, x_5, x_6$. Параметри $x_1, x_2, x_3, x_4, x_5, x_6$ взяти із таблиці 3.2 згідно з номером варіанта N .

3. Криптоаналітик перехопив шифртекст C . Йому відомо, що використалось шифрування за допомогою гами шифру – лінійної рекурентної послідовності $x_{k+3} = x_{k+2} \oplus x_k$, але невідомий ключ, тобто початкові значення послідовності. Криптоаналітик використав атаку «груба сила» («brute force»): перебрав всі можливі ключі і знайшов відповідний відкритий текст.

Який текст був зашифровано і на якому ключі?

Шифртекст C взяти із таблиці 3.2 згідно з номером варіанта N .

Таблиця 3.1 – Варіанти для завдання 1

N	S	M
1	$x_{k+6} = x_{k+3} \oplus x_{k+1} \oplus x_k$	emir
2	$x_{k+4} = x_{k+3} \oplus x_{k+1} \oplus x_k$	iron
3	$x_{k+5} = x_{k+4} \oplus x_{k+3} \oplus x_{k+2} \oplus x_k$	firm
4	$x_{k+6} = x_{k+5} \oplus x_{k+3} \oplus x_{k+2} \oplus x_{k+1}$	cuke
5	$x_{k+6} = x_{k+2} \oplus x_k$	airy
6	$x_{k+7} = x_{k+1} \oplus x_k$	disk
7	$x_{k+7} = x_{k+4} \oplus x_{k+3}$	beam
8	$x_{k+6} = x_{k+5} \oplus x_k$	acid
9	$x_{k+7} = x_{k+5} \oplus x_{k+2}$	ache
10	$x_{k+7} = x_{k+3} \oplus x_k$	dirk
11	$x_{k+7} = x_{k+2} \oplus x_k$	chap
12	$x_{k+5} = x_{k+4} \oplus x_{k+3} \oplus x_{k+1} \oplus x_k$	soon
13	$x_{k+7} = x_{k+5} \oplus x_k$	acme
14	$x_{k+6} = x_{k+5} \oplus x_{k+2}$	bear
15	$x_{k+6} = x_{k+5} \oplus x_{k+4} \oplus x_{k+1} \oplus x_k$	soot
16	$x_{k+8} = x_{k+5} \oplus x_{k+3} \oplus x_{k+2}$	wow
17	$x_{k+8} = x_{k+7} \oplus x_{k+2}$	will
18	$x_{k+7} = x_{k+6} \oplus x_{k+5} \oplus x_{k+3} \oplus x_{k+2}$	beta

3.2 Зміст звіту

1. Титульний лист, тема і мета роботи.
2. Результати обчислень.
3. Висновки по роботі.

Таблиця 3.2 – Варіанти для завдань 2, 3

N	x_1	x_2	x_3	x_4	x_5	x_6	C
1	1	1	1	1	1	1	C62DF45E
2	1	1	0	0	1	1	3DF2551A
3	1	1	1	0	0	1	581188A1
4	1	0	1	0	1	0	D421F24E
5	0	1	1	0	0	1	B2C423F8
6	1	0	0	1	0	1	C223F448
7	0	0	1	1	0	0	B7CE3DF6
8	1	1	1	0	1	0	FE4F1F8C
9	1	0	0	1	1	0	FE521599
10	1	0	1	1	1	0	1D9BBCC9
11	0	0	1	1	1	0	2FF4480D
12	0	1	1	1	0	0	8FBAD523
13	0	1	0	1	0	1	158ABBC2
14	0	0	1	0	1	1	581188BE
15	1	0	0	1	1	1	8DBAD525
16	1	1	0	0	0	1	CB21F251
17	0	0	1	1	1	1	E953198C
18	0	0	0	1	0	1	EE550185

3.3 Контрольні питання

1. Як задається бітова лінійна рекурентна послідовність (ЛРП)?
2. Для чого використовуються ЛРП в криптографії?
3. Що таке глибина ЛРП?
4. Що таке характеристичний многочлен ЛРП?
5. Який многочлен називається незвідним?
6. Як перевірити многочлен на незвідність?
7. Що таке період лінійної рекурентної послідовності і від чого він залежить?
8. Що таке регістри зсуву?

ЛАБОРАТОРНА РОБОТА № 4

АСИМЕТРИЧНИЙ АЛГОРИТМ ШИФРУВАННЯ RSA

Мета роботи: ознайомитися з асиметричним алгоритмом шифрування RSA.

4.1 Завдання на лабораторну роботу

1. Оберіть із таблиці 4.1 прості числа p і q , $p, q > 100$. Обчисліть модуль n і функцію Ейлера $\varphi(n)$. За алгоритмом RSA знайдіть асиметричну пару ключів e і d .

2. Оберіть повідомлення M , $\frac{n}{2} < M < n$. Здійсніть зашифрування повідомлення за допомогою відкритого ключа e .

3. Розшифруйте обчислену криптограму за допомогою секретного ключа d .

4. Відомі відкритий параметр алгоритму RSA модуль N та відкритий ключ E абонента А. Знайдіть секретний ключ D абонента А і розшифруйте повідомлення C .

Значення модуля N , відкритого ключа E та повідомлення C візьміть із таблиці 4.2 згідно з номером варіанту N.

4.2 Зміст звіту

4. Титульний лист, тема і мета роботи.
5. Вибрані значення параметрів.
6. Проведені обчислення.
7. Сформовані відкритий і секретний ключі.
8. Результати зашифрування і розшифрування.
9. Результат пошуку секретного ключа.
10. Висновки по роботі.

Таблица 4.1 – Таблица простых чисел

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541
547	557	563	569	571	577	587	593	599	601
607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733
739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863
877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997	1009	1013
1019	1021	1031	1033	1039	1049	1051	1061	1063	1069
1087	1091	1093	1097	1103	1109	1117	1123	1129	1151
1153	1163	1171	1181	1187	1193	1201	1213	1217	1223
1229	1231	1237	1249	1259	1277	1279	1283	1289	1291
1297	1301	1303	1307	1319	1321	1327	1361	1367	1373
1381	1399	1409	1423	1427	1429	1433	1439	1447	1451
1453	1459	1471	1481	1483	1487	1489	1493	1499	1511
1523	1531	1543	1549	1553	1559	1567	1571	1579	1583
1597	1601	1607	1609	1613	1619	1621	1627	1637	1657
1663	1667	1669	1693	1697	1699	1709	1721	1723	1733
1741	1747	1753	1759	1777	1783	1787	1789	1801	1811
1823	1831	1847	1861	1867	1871	1873	1877	1879	1889
1901	1907	1913	1931	1933	1949	1951	1973	1979	1987
1993	1997	1999	2003	2011	2017	2027	2029	2039	2053
2063	2069	2081	2083	2087	2089	2099	2111	2113	2129
2131	2137	2141	2143	2153	2161	2179	2203	2207	2213
2221	2237	2239	2243	2251	2267	2269	2273	2281	2287

Таблиця 4.2 – Варіанти для завдання 4

N	<i>N</i>	<i>E</i>	<i>C</i>
1	117343	112739	26660
2	107311	60007	104510
3	30397	21367	17607
4	69133	863	29813
5	116617	59579	94667
6	64507	22647	3317
7	104353	41327	13039
8	107413	65299	8904
9	105169	8967	60911
10	105799	58139	13200
11	198691	12667	78606
12	107567	81467	67969
13	116509	77931	26647
14	112711	3755	4201
15	67591	26735	30469
16	188549	125819	182492
17	70747	28967	32071
18	110839	15407	31156
19	93661	24641	51991
20	53357	34031	36601
21	183641	166631	44594
22	188131	125803	79193
23	98699	25367	70433
24	204223	116087	22996

4.3 Контрольні питання

1. Опишіть процедуру генерації ключів в RSA.
2. Опишіть процедури зашифрування та розшифрування в RSA.
3. Побудуйте схему криптосистеми з відкритим ключем.
4. Від чого залежить криптостійкість алгоритму RSA?

ЛАБОРАТОРНА РОБОТА № 5

СХЕМА ДІФФІ-ХЕЛЛМАНА В МУЛЬТИПЛІКАТИВНІЙ ГРУПІ

Мета роботи: ознайомитися зі схемою Діффі-Хеллмана в мультиплікативній групі для генерування спільного секретного ключа для пари користувачів.

5.1 Завдання на лабораторну роботу

1. Для заданих відкритих параметрів p , g згенеруйте спільний секретний ключ за схемою Діффі-Хеллмана. Параметр p – просте число, g – генератор мультиплікативної групи залишків за модулем p

2. По перехопленим значенням y та z знайдіть спільний секретний ключ абонентів А і В.

Значення параметрів p , g , y , z візьміть в таблиці 5.1 згідно з номером варіанту N.

Таблиця 5.1 – Варіанти завдань

N	p, g	y, z	N	p, g	y, z	N	p, g	y, z
1	47,10	5,14	11	59,23	28,42	21	59,37	13,27
2	59,6	51,2	12	47,15	21,40	22	59,8	39,20
3	47,22	38,29	13	59,14	18,51	23	47,11	22,16
4	59,10	32,54	14	47,29	20,11	24	59,31	58,44
5	47,30	13,32	15	59,13	55,44	25	47,19	33,14
6	59,30	28,3	16	47,35	8,24	26	59,11	18,55
7	47,13	44,10	17	59,33	31,49	27	47,5	3,13
8	59,18	17,51	18	47,23	46,17	28	47,31	2,8
9	47,20	17,29	19	59,2	34,53	29	59,24	9,13
10	59,32	43,12	20	47,33	32,19	30	47,26	34,28

5.2 Зміст звіту

1. Титульний лист, тема і мета роботи.
2. Обрані значення параметрів.
3. Проведені обчислення.
4. Сформований секретний ключ.
5. Висновки по роботі.

5.3 Контрольні питання

1. Опишіть схему Діффі-Хеллмана генерування спільного секретного ключа.
2. На чому заснована криптографічна стійкість схеми Діффі-Хеллмана?
3. Як впливає розмір простого числа N на криптостійкість?
4. Як визначити бітовий розмір спільного ключа по вхідних відкритих параметрах?

ЛАБОРАТОРНА РОБОТА № 6

ЕЛІПТИЧНІ КРИВІ НАД ПРОСТИМ ПОЛЕМ

Мета роботи: Ознайомитися з математичним апаратом еліптичних кривих над простим полем Галуа $GF(p)$.

6.1 Завдання на лабораторну роботу

Дано еліптичну криву над простим полем $GF(p)$

$$y^2 = x^3 + ax + b \bmod p.$$

1. Знайти всі точки, що належать заданій кривій, за допомогою функції `msolve`. Визначити порядок кривої.
2. Знайти базову точку.
3. Визначити порядок окремих точок кривої.

Параметри a , b , p взяти із таблиці 6.1 згідно з номером варіанта N.

6.2 Зміст звіту

1. Титульний лист, тема і мета роботи.
2. Результати обчислень.
3. Висновки по роботі.

6.3 Контрольні питання

1. Дати визначення еліптичної кривої.
2. Як визначити точку, протилежну даній?
3. Які параметри еліптичної кривої необхідно знати для її застосування?
4. Дати визначення порядку групи точок еліптичної кривої?
5. Опишіть алгоритм пошуку точки еліптичної кривої над простим полем $GF(p)$.
6. Дати визначення порядку точки еліптичної кривої.
7. Як визначити базову точку?

Таблиця 6.1 – Варіанти завдань

N	a	b	p
1	3	8	101
2	23	42	103
3	7	44	107
4	5	67	127
5	4	5	11
6	17	3	19
7	3	16	29
8	5	17	31
9	4	31	37
10	6	30	43
11	5	34	59
12	15	45	67
13	7	18	71
14	33	4	79
15	56	2	83

N	a	b	p
16	56	13	101
17	45	47	103
18	50	32	107
19	23	100	127
20	4	7	11
21	13	3	19
22	2	14	29
23	14	3	31
24	5	18	37
25	16	28	43
26	5	41	59
27	7	54	67
28	65	5	71
29	34	8	79
30	66	6	83

ЛАБОРАТОРНА РОБОТА № 7

СТАНДАРТ ЦИФРОВОГО ПІДПISУ ECDSA НАД ПРОСТИМ ПОЛЕМ

Мета роботи: Ознайомитися з чинним американським стандартом цифрового підпису ECDSA над простим полем.

7.1 Завдання на лабораторну роботу

Дано еліптичну криву $y^2 = x^3 + 6x + 5 \bmod 43$ і базову точку кривої P порядку $n = 37$.

1. Згенеруйте відкритий та секретний ключі абонента A за схемою ECDSA. Обчисліть електронний цифровий підпис з використанням секретного ключа абонента A . Перевіріть отриманий цифровий підпис з використанням відкритого ключа абонента A .

Значення базової точки P та числа h , яке відповідає хеш-образу повідомлення, візьміть з таблиці 7.1 згідно з номером варіанту N .

2. Перевірте цифровий підпис $\langle r, s \rangle$, отриманий за алгоритмом цифрового підпису ECDSA, використовуючи відкритий ключ підписувача $Q = (9, 10)$. Базова точка $T = (37, 22)$ має порядок $n = 37$.

Значення цифрового підпису $\langle r, s \rangle$ та числа H , яке відповідає хеш-образу повідомлення, візьміть із таблиці 7.2 згідно з номером варіанту N .

7.2 Зміст звіту

1. Титульний лист, тема і мета роботи.
2. Результати обчислень.
3. Висновки по роботі.

7.3 Контрольні питання

1. Які параметри є загальносистемними ?
2. Опишіть процедуру генерації ключів у ECDSA.
3. Опишіть процедуру формування і перевірки підпису в ECDSA.
4. Які параметри впливають на криптостійкість підпису?

Таблиця 7.1 – Варіанти для завдання 1

N	P	h	N	P	h	N	P	h	N	P	h
1	2,38	15	7	8,7	12	13	18,21	3	19	35,2	14
2	13,42	4	8	42,27	30	14	29,31	16	20	31,21	6
3	26,8	21	9	22,32	31	15	9,10	29	21	31,22	9
4	30,40	10	10	37,21	7	16	5,17	27	22	35,41	15
5	20,16	18	11	28,25	22	17	5,26	17	23	22,11	13
6	14,34	25	12	24,16	18	18	9,33	3	24	42,16	16

Таблиця 7.2 – Варіанти для завдання 2

N	r	s	H	N	r	s	H	N	r	s	H
1	8	3	15	10	13	35	17	19	29	10	9
2	2	15	6	11	29	26	22	20	29	22	28
3	31	16	19	12	29	32	13	21	8	23	10
4	35	20	30	13	30	3	4	22	18	20	29
5	5	3	26	14	18	11	12	23	29	29	12
6	35	14	8	15	5	22	5	24	13	27	14
7	24	14	3	16	30	35	20	25	14	34	25
8	20	11	21	17	5	31	24	26	30	10	16
9	24	33	7	18	5	33	11	27	24	2	23

ЛАБОРАТОРНА РОБОТА № 8

ЕЛІПТИЧНІ КРИВІ НАД РОЗШИРЕНИМ ПОЛЕМ

Мета роботи: Ознайомитися з математичним апаратом еліптичних кривих над розширеним полем Галуа $GF(2^m)$.

8.1 Завдання на лабораторну роботу

Дано еліптичну криву над розширеним полем $GF(2^m)$

$$y^2 + xy = x^3 + ax^2 + b \bmod(2, f(t)).$$

1. Знайти всі точки, що належать заданій кривій.
2. Визначити порядок кривої.
3. Знайти порядок довільної точки кривої.

Параметри a , b , m , f взяти із таблиці 8.1 згідно з номером варіанта N.

8.2 Зміст звіту

4. Титульний лист, тема і мета роботи.
5. Результати обчислень.
6. Висновки по роботі.

8.3 Контрольні питання

8. Дати визначення еліптичної кривої над розширеним полем.
9. Як визначити точку, протилежну даній?
10. Дати визначення порядку групи точок еліптичної кривої.
11. Дати визначення порядку точки еліптичної кривої.
12. У яких криптографічних алгоритмах застосовуються еліптичні криві?

Таблиця 8.1 – Варіанти завдань

N	a	b	m	f
1	1	1	3	$t^3 + t^2 + 1$
2	1	t	3	$t^3 + t^2 + 1$
3	1	$1 + t$	3	$t^3 + t^2 + 1$
4	1	t^2	3	$t^3 + t^2 + 1$
5	1	$1 + t^2$	3	$t^3 + t^2 + 1$
6	1	$t + t^2$	3	$t^3 + t^2 + 1$
7	1	$1 + t + t^2$	3	$t^3 + t^2 + 1$
8	0	1	3	$t^3 + t^2 + 1$
9	0	t	3	$t^3 + t^2 + 1$
10	0	$1 + t$	3	$t^3 + t^2 + 1$
11	0	t^2	3	$t^3 + t^2 + 1$
12	0	$1 + t^2$	3	$t^3 + t^2 + 1$
13	0	$t + t^2$	3	$t^3 + t^2 + 1$
14	0	$1 + t + t^2$	3	$t^3 + t^2 + 1$
15	1	1	5	$t^5 + t^3 + 1$
16	1	t	5	$t^5 + t^3 + 1$
17	1	$1 + t$	5	$t^5 + t^3 + 1$
18	1	t^2	5	$t^5 + t^3 + 1$
19	1	$1 + t^2$	5	$t^5 + t^3 + 1$
20	1	$t + t^2$	5	$t^5 + t^3 + 1$
21	1	$1 + t + t^2$	5	$t^5 + t^3 + 1$
22	1	t^3	5	$t^5 + t^3 + 1$
23	0	$1 + t^3$	5	$t^5 + t^3 + 1$
24	0	$t + t^3$	5	$t^5 + t^3 + 1$
25	0	$1 + t + t^3$	5	$t^5 + t^3 + 1$
26	0	$t^2 + t^3$	5	$t^5 + t^3 + 1$

ЛАБОРАТОРНА РОБОТА № 9

УКРАЇНСЬКИЙ СТАНДАРТ ЦИФРОВОГО ПІДПISУ ДСТУ 4145-2002

Мета роботи: Ознайомитися з чинним стандартом цифрового підпису ДСТУ 4145-2002.

9.1 Завдання на лабораторну роботу

Дано еліптичну криву

$$y^2 + xy = x^3 + x^2 + 1 + t^4 \bmod(2, t^5 + t^2 + 1)$$

і базову точку кривої $P = (t^3, t + t^2)$ порядку $n = 19$.

1. Згенеруйте відкритий та секретний ключі абонента А за схемою ДСТУ 4145-2002. Обчисліть електронний цифровий підпис з використанням секретного ключа абонента А. Перевірте отриманий цифровий підпис з використанням відкритого ключа абонента А.

Значення елемента поля h , яке відповідає хеш-образу повідомлення, візьміть з таблиці 9.1 згідно з номером варіанту N.

2. Перевірте цифровий підпис $\langle r, s \rangle$, отриманий за алгоритмом цифрового підпису ДСТУ 4145-2002, використовуючи відкритий ключ підписувача $Q = (1 + t + t^4, 1 + t)$. Базова точка $T = (t^3 + t^4, t^4)$ має порядок $n = 19$.

Значення цифрового підпису $\langle r, s \rangle$ та числа H , яке відповідає хеш-образу повідомлення, візьміть із таблиці 9.2 згідно з номером варіанту N.

9.2 Зміст звіту

4. Титульний лист, тема і мета роботи.
5. Обрані значення параметрів.
6. Проведені обчислення.
7. Сформовані відкритий і секретний ключі.
8. Сформований підпис.
9. Результат перевірки підпису.
10. Висновки по роботі.

9.3 Контрольні питання

5. Які параметри є загальносистемними ?
6. Опишіть процедуру генерації ключів у ДСТУ 4145-2002.
7. Опишіть процедуру формування підпису в ДСТУ 4145-2002.
8. Опишіть процедуру перевірки підпису в ДСТУ 4145-2002.
9. Які параметри впливають на криптостійкість підпису?

Таблиця 9.1 – Варіанти для завдання 1

N	h	N	h	N	h
1	t	10	$1+t+t^2$	19	$1+t+t^3$
2	$1+t$	11	t^4	20	$1+t^2+t^3$
3	t^2	12	$1+t^4$	21	$t+t^2+t^3$
4	$1+t^2$	13	$t+t^4$	22	$1+t+t^2+t^3$
5	$t+t^2$	14	t^2+t^4	23	$t+t^3+t^4$
6	t^3	15	t^3+t^4	24	$t+t^2+t^4$
7	$1+t^3$	16	$1+t+t^4$	25	$t^2+t^3+t^4$
8	$t+t^3$	17	$1+t^2+t^4$	26	$1+t+t^2+t^4$
9	t^2+t^3	18	$1+t^3+t^4$	27	$1+t+t^3+t^4$

Таблиця 9.2 – Варіанти для завдання 2

N	r	s	H
1	12	10	$1+t^4$
2	12	1	$1+t+t^3$
3	14	10	$t+t^4$
4	13	18	$1+t+t^4$
5	7	15	$1+t^3$
6	14	17	$1+t+t^2$
7	1	14	t^2+t^3
8	13	19	t^3
9	6	13	$1+t^4$
10	15	3	$1+t+t^4$
11	1	15	t^2+t^4
12	1	8	t
13	7	14	$1+t^2+t^3$
14	9	4	$1+t+t^2+t^3$
15	8	2	t^4

N	r	s	H
16	10	15	t^3
17	7	17	$1+t^2$
18	12	9	t^2
19	6	15	$1+t+t^2$
20	5	8	$t+t^2$
21	14	9	t^3
22	9	10	t^3
23	2	13	$1+t+t^3$
24	14	18	t^3
25	10	18	$t+t^3$
26	4	7	$1+t^3$
27	9	15	$1+t^2+t^4$
28	7	16	t^2
29	14	7	t^2+t^4
30	9	18	$1+t^3+t^4$

ЛАБОРАТОРНА РОБОТА № 10

ОСНОВНІ КРИПТОПЕРЕТВОРЕННЯ В АМЕРИКАНСЬКОМУ СТАНДАРТІ ШИФРУВАННЯ FIPS 197 (АЛГОРИТМ RIJNDAEL)

Мета роботи: Ознайомитися з чинним стандартом шифрування США – блочним алгоритмом RIJNDAEL.

10.1 Завдання на лабораторну роботу

1. Оберіть довільний текст довжиною 16 літер. Кожну літеру замініть відповідним шістнадцятирічним ASCII-кодом. Сформуйте матрицю – 4 стовпця по 4 шістнадцятирічних числа. Отримуєте початковий State S_0 .

За заданим 128-бітним ключем нульового раунду

$R_0 = \text{"000102030405060708090A0B0C0D0E0F"}$

сформуйте відповідну State матрицю – 4 стовпця по 4 шістнадцятирічних числа.

Обчисліть перетворення додавання раундового ключа $\text{AddRoundKey}(S_0, R_0)$. Новий State позначте S_1 .

2. Обчисліть перетворення заміна байтів $\text{ByteSub}(S_1)$ для кожного елементу State S_1 . Новий State позначте S_2 .

3. Обчисліть перетворення зрушення рядків $\text{ShiftRow}(S_2)$ для рядків матриці State S_2 . Новий State позначте S_3 .

4. Обчисліть перетворення $\text{MixColumn}(S_3)$ перемішування стовпців матриці State S_3 . Новий State позначте S_4 .

5. За заданим 128-бітним ключем першого раунду

$R_1 = \text{"D6AA74FDD2AF72FADAA678F1D6AB76FE"}$

сформуйте відповідну State матрицю – 4 стовпця по 4 шістнадцятирічних числа.

Обчисліть перетворення додавання раундового ключа $\text{AddRoundKey}(S_4, R_1)$. Кінцевий State позначте S^* .

6. Перетворити кінцевий внутрішній стан S^* на текст.

7. Отримано 128-бітне зашифроване повідомлення C .

Після 9-того раунду розшифрування обчислено State $\bar{S}$ (візьміть із таблиці 10.1 згідно з номером варіанту N).

Відомі ключі першого і нульового раундів відповідно R_1 і R_0 :

$R_1 = \text{"D6AA74FDD2AF72FADAA678F1D6AB76FE"} ,$

$R_0 = \text{"000102030405060708090A0B0C0D0E0F"} .$

Знайдіть відкритий текст повідомлення T .

Для цього:

– обчисліть перетворення додавання раундового ключа $\text{AddRoundKey}(\bar{S}, R_1)$, новий State позначте $\bar{S}_4$;

– обчисліть зворотне перетворення $\text{InvMixColumn}(\bar{S}_4)$ – перемішування стовпців матриці State $\bar{S}_4$, новий State позначте $\bar{S}_3$;

– обчисліть зворотне перетворення зрушення рядків $\text{InvShiftRow}(\bar{S}_3)$ для рядків матриці State $\bar{S}_3$, новий State позначте $\bar{S}_2$;

– обчисліть зворотне перетворення заміна байтів $\text{InvByteSub}(\bar{S}_2)$ для кожного елементу State $\bar{S}_2$, новий внутрішній стан позначте $\bar{S}_1$;

– обчисліть перетворення додавання раундового ключа $\text{AddRoundKey}(\bar{S}_1, R_0)$, новий State позначте $\bar{S}_0$;

Кінцевий State $\bar{S}_0$ відповідає відкритому тексту повідомлення.

Перетворити внутрішній стан $\bar{S}_0$ на текст T .

10.2 Зміст звіту

1. Титульний лист, тема і мета роботи.
2. Проведені обчислення.
3. Результати перетворень.

Таблиця 10.1 – Варіанти для завдання 7 ($N, \bar{S}$)

1,

6C	DE	CE	53
4C	77	5E	30
A	F4	7B	4F
85	DD	91	2E

2,

47	B7	10	FA
60	1D	80	B9
24	DE	FC	A2
4D	32	BC	94

3,

3C	74	7E	EE
D2	C2	97	50
8B	D1	B8	5F
71	93	BB	4

4,

AD	5F	C8	E7
D6	65	6D	25
91	AA	2C	AC
7	4C	99	FF

5,

8E	EB	29	D0
89	BB	4A	2A
6B	CB	39	9F
98	9D	25	54

6,

71	C6	C0	3B
8F	12	5C	E6
31	4F	A9	7B
4F	5B	5C	24

7,

7E	9E	94	E
10	E3	8A	75
44	57	FF	F0
4	8A	D5	51

8,

21	F6	FC	B0
FB	AF	D	D2
B5	F8	6E	4F
67	C2	A3	AB

9,

FC	6B	CD	A3
F3	63	29	1F
6A	3E	9E	4C
47	BA	29	F4

10,

3A	C0	DA	35
E7	AD	F6	34
2B	2F	94	22
32	23	30	6

11,

A7	9	C7	B7
61	D3	31	F4
A9	FD	E8	75
8E	76	AD	E

12,

6	FB	63	8F
E3	9	5E	95
13	94	A2	D3
81	24	7A	7C

$$13, \begin{bmatrix} 77 & 43 & 5E & 85 \\ 48 & 2E & 13 & 93 \\ 0 & E4 & AB & E8 \\ BA & 23 & 6B & D6 \end{bmatrix}$$

$$14, \begin{bmatrix} C4 & F2 & 93 & CC \\ 83 & E & 2C & CE \\ C4 & 3 & 86 & 60 \\ FA & B6 & 1C & C8 \end{bmatrix}$$

$$15, \begin{bmatrix} 2D & 2D & A9 & 1E \\ 29 & 78 & 6C & DE \\ 20 & BB & BF & F5 \\ B9 & 3A & B & 53 \end{bmatrix}$$

10.3 Контрольні питання

1. Як знайти мультиплікативно обернений елемент в розширеному полі?
2. Як перетворити шістнадцятеричне число на елемент розширеного поля?
3. Опишіть операції над елементами розширеного поля.
4. Опишіть раундові перетворення алгоритму RIJNDAEL.
5. В якій послідовності виконуються перетворення в алгоритмі RIJNDAEL?
6. Які параметри алгоритму RIJNDAEL впливають на його криптостійкість?

ЛАБОРАТОРНА РОБОТА № 11

ОСНОВНІ КРИПТОПЕРЕТВОРЕННЯ В УКРАЇНСЬКОМУ СТАНДАРТІ ШИФРУВАННЯ ДСТУ 7624:2014

Мета роботи: Ознайомитися зі стандартом шифрування України ДСТУ 7624:2014 – симетричним блочним алгоритмом.

11.1 Завдання на лабораторну роботу

1. Оберіть довільний текст довжиною 16 літер. Кожну літеру замініть відповідним шістнадцятирічним ASCII-кодом. Сформууйте 2 стовпця по 8 шістнадцятирічних чисел. Отримуєте початковий внутрішній стан G_0 .

За заданим 128-бітним ключем нульового циклу

$K_0 = \text{"16505E6B9B3AB1E6865B77DCE082A0F4"}$

сформууйте 2 стовпця по 8 шістнадцятирічних чисел.

Обчисліть функцію $\eta_l^{(K_0)}$ додавання циклового ключа K_0 і початкового внутрішнього стану G_0 . Новий внутрішній стан позначте G_1 .

2. Обчисліть функцію підстановки π' для кожного елементу $g_{i,j}$ матриці внутрішнього стану G_1 . Новий внутрішній стан позначте G_2 .

3. Обчисліть функцію зсуву τ_l для рядків матриці внутрішнього стану G_2 . Новий внутрішній стан позначте G_3 .

4. Обчисліть функцію ψ_l лінійного перетворення стовпців матриці внутрішнього стану G_3 . Новий внутрішній стан позначте G_4 .

5. Обчисліть функцію $\kappa_l^{(K_1)}$ побітового додавання циклового ключа $K_1 = \text{"E6865B77DCE082A0F416505E6B9B3AB1"}$ і матриці

внутрішнього стану G_4 за модулем 2. Кінцевий внутрішній стан позначте G^* .

6. Перетворити кінцевий внутрішній стан G^* на текст.

7. Отримано 128-бітне зашифроване повідомлення C .

Після 9-ти ітерацій розшифрування обчислено внутрішній стан $\bar{G}$ (візьміть із таблиці 11.1 згідно з номером варіанту N).

Відомі ключі першої і нульової ітерацій відповідно K_1 і K_0 :

$K_1 = \text{"E6865B77DCE082A0F416505E6B9B3AB1"}$,

$K_0 = \text{"16505E6B9B3AB1E6865B77DCE082A0F4"}$.

Знайдіть відкритий текст повідомлення T .

Для цього:

– обчисліть функцію $\kappa_l^{(K_1)}$ побітового додавання циклового ключа K_1 і матриці внутрішнього стану $\bar{G}$ за модулем 2, новий внутрішній стан позначте $\bar{G}_4$;

– обчисліть функцію ψ_l^{-1} оберненого лінійного перетворення стовпців матриці внутрішнього стану $\bar{G}_4$, новий внутрішній стан позначте $\bar{G}_3$;

– обчисліть обернену функцію зсуву τ_l^{-1} для рядків матриці внутрішнього стану $\bar{G}_3$, новий внутрішній стан позначте $\bar{G}_2$;

– обчисліть обернену функцію підстановки π'_{-1} для кожного елементу $\bar{g}_{i,j}$ матриці внутрішнього стану $\bar{G}_2$, новий внутрішній стан позначте $\bar{G}_1$;

– обчисліть функцію $\eta_l^{(-K_0)}$ віднімання циклового ключа K_0 від внутрішнього стану $\bar{G}_1$, новий внутрішній стан позначте $\bar{G}_0$.

Внутрішній стан $\bar{G}_0$ відповідає T – відкритому тексту повідомлення. Перетворити внутрішній стан $\bar{G}_0$ на текст T .

Таблиця 11.1 – Варіанти для завдання 7 (N, $\bar{G}$)

$$\begin{array}{c}
1, \begin{bmatrix} 54 & B4 \\ 86 & 10 \\ 3A & 6C \\ 8A & 67 \\ DF & FD \\ 82 & 3A \\ BF & DE \\ 31 & 2B \end{bmatrix}
\end{array}$$

$$\begin{array}{c}
2, \begin{bmatrix} 54 & 25 \\ B & 47 \\ F3 & 7B \\ EF & 8C \\ 65 & F1 \\ 87 & B4 \\ 88 & E5 \\ C2 & 54 \end{bmatrix}
\end{array}$$

$$\begin{array}{c}
3, \begin{bmatrix} BA & AE \\ D2 & 46 \\ 7A & F6 \\ D5 & BF \\ 1 & EC \\ 35 & AD \\ 1D & CB \\ E6 & BA \end{bmatrix}
\end{array}$$

$$\begin{array}{c}
4, \begin{bmatrix} 22 & 96 \\ F & 20 \\ 2F & E9 \\ 4C & CB \\ B9 & 4A \\ 4D & 42 \\ E7 & F9 \\ F8 & 7D \end{bmatrix}
\end{array}$$

$$\begin{array}{c}
5, \begin{bmatrix} A4 & 77 \\ 87 & E \\ E3 & 47 \\ 26 & 1C \\ 54 & 44 \\ 3B & 0 \\ E0 & 6B \\ 90 & 68 \end{bmatrix}
\end{array}$$

$$\begin{array}{c}
6, \begin{bmatrix} 93 & 28 \\ B & B3 \\ 66 & E4 \\ 3C & 55 \\ A9 & C5 \\ 35 & 46 \\ 8F & 6D \\ AB & E0 \end{bmatrix}
\end{array}$$

$$\begin{array}{c}
7, \begin{bmatrix} 57 & 3F \\ 8C & AA \\ 7E & CB \\ 92 & 57 \\ AC & 6A \\ 44 & CB \\ 5C & 2E \\ EB & C5 \end{bmatrix}
\end{array}$$

$$\begin{array}{c}
8, \begin{bmatrix} 2C & F3 \\ 6 & 5F \\ 76 & 14 \\ 62 & EF \\ AE & C3 \\ BF & 4B \\ 0 & DB \\ 66 & 5F \end{bmatrix}
\end{array}$$

$$\begin{array}{c}
9, \begin{bmatrix} B2 & 0 \\ 21 & F3 \\ 30 & E6 \\ 1C & AC \\ 83 & EF \\ 3F & 76 \\ 66 & E0 \\ 9B & 84 \end{bmatrix}
\end{array}$$

$$\begin{array}{c}
10, \begin{bmatrix} 17 & 25 \\ FD & 9C \\ 82 & F6 \\ AB & 98 \\ EB & 63 \\ 7C & 17 \\ E1 & EC \\ 19 & B \end{bmatrix}
\end{array}$$

$$\begin{array}{c}
11, \begin{bmatrix} 7B & 4E \\ A9 & 28 \\ 0 & 2 \\ 42 & 6B \\ 94 & 58 \\ D & B9 \\ 5A & BC \\ 76 & D7 \end{bmatrix}
\end{array}$$

$$\begin{array}{c}
12, \begin{bmatrix} 41 & 39 \\ 63 & B3 \\ 37 & C8 \\ 3 & 7F \\ 29 & D2 \\ 39 & 4 \\ B3 & 8 \\ 8 & 1E \end{bmatrix}
\end{array}$$

$$\begin{array}{c}
13, \begin{bmatrix} 85 & 52 \\ 90 & 59 \\ C6 & C2 \\ A7 & 1A \\ 2 & B5 \\ 96 & E7 \\ 95 & FB \\ 33 & 64 \end{bmatrix}
\end{array}$$

$$\begin{array}{c}
14, \begin{bmatrix} 3C & 29 \\ 19 & C5 \\ 85 & AD \\ CE & 4C \\ 4 & 1F \\ 69 & 1F \\ BE & 26 \\ A7 & 1E \end{bmatrix}
\end{array}$$

$$\begin{array}{c}
15, \begin{bmatrix} BE & C9 \\ CA & 18 \\ C2 & 13 \\ E9 & F3 \\ 8 & 7D \\ 13 & D6 \\ 69 & 5D \\ D5 & 7B \end{bmatrix}
\end{array}$$

11.2 Зміст звіту

1. Титульний лист, тема і мета роботи.
2. Проведені обчислення.
3. Результати перетворень.
4. Висновки по роботі.

11.3 Контрольні питання

1. Яке розширене поле використається в алгоритмі ДСТУ 7624:2014?
2. Як перетворити шістнадцятеричне число на елемент розширеного поля?
3. Опишіть ітераційні перетворення алгоритму ДСТУ 7624:2014.
4. В якій послідовності виконуються перетворення в алгоритмі ДСТУ 7624:2014?
5. Які параметри алгоритму ДСТУ 7624:2014 впливають на його криптостійкість?

ЛІТЕРАТУРА

1. Горбенко І.Д. Прикладна криптологія / Горбенко І.Д., Горбенко Ю.І. – Харків: Видавництво «Форт», 2012. – 878 с.
2. Математичні основи криптоаналізу: навч. посібник для студ. вищ. навч. закл.: рек. МОНУ / С.О. Сушко, Г.В. Кузнецов, Л.Я. Фомичова, А.В. Корабльов. -Дніпропетровськ: НГУ, 2010.-466с.
3. Фергюсон Н., Шнайер Б. Практическая криптография – М.: Диалектика, 2005. – 424 с.
4. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. М.Ж КУДИЦ-ОБРАЗ, 2001 – 386с.
5. Баричев С.Г., Гончаров В.В. Основы современной криптографии. М.: Горячая линия - Телеком, 2001.
6. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина. – 2-е изд., перераб. и доп. – М.: Радио и связь, 2001. – 376 с.
7. Виноградов И.М. Основы теории чисел. – М.: Наука, 1981. – 168 с.
8. Курош А.Г. Курс высшей алгебры. – М.:Наука, 1971. – 423 с.
9. Ростовцев А.Г. Алгебраические основы криптографии. – СПб.: НПО «Мир и семья, ООО «Интерлайн», 2000. – 354 с.
10. Menezes A., van Oorschot P., Vanstone S. Handbook of applied cryptography. CRC Press, 1997.
11. Штанько С.В. Эллиптические кривые в криптографии // Проблемы информационной безопасности. Компьютерные системы. 2003. № 2. С. 65 – 74.
12. Тарабанько А.В., Кучеров М.М. Реализация протокола проверки знания с использованием эллиптических кривых // Безопасность информационных технологий. 2001. № 2. С.61 – 63.
13. Введение в криптографию / Под общ. Ред. В.В. Ященко. – 2-е изд., испр. – М.:МЦНМО: «ЧеРо», 1999. – 272с.
14. Нечаев В.И. Элементы криптографии (Основы теории защиты информации): Учеб. пособие для ун-тов и пед. вузов / Под ред. В.А.Садовниченко – М.: Высш.шк., 1999. – 109с.
15. Вербіцький О.В. Вступ до криптології. – Львів: ВНТЛ, 1998. – 248.
16. Саломая А. Криптография с открытым ключом: Пер. с англ. – М.: Мир, 1995. – 318с.

17. Shamir A. How to share a secret // Communications of the ACM. – New York, NY, USA: ACM, 1979. – В. 11. - Т. 22. – С. 612 - 613.
18. Сمارт Н. Криптографія. – Москва: Техносфера, 2005. -528 с.