МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет «Запорізька політехніка»

Методичні вказівки

до лабораторних робіт з дисципліни
“Методи побудови і аналізу криптосистем”
для студентів усіх форм навчання
спеціальності 125 – «Кібербезпека
та захист інформації»

2024

Методичні вказівки до лабораторних робіт з дисципліни “Методи побудови і аналізу криптосистем” для студентів усіх форм навчання спеціальності 125 – «Кібербезпека та захист інформації» / Укл.: Г.Л. Козіна. - Запоріжжя: НУ «Запорізька політехніка», 2024. – 54 с.

Укладачі: Г.Л.Козіна, доцент, к.ф.-м.н.

Рецензент: Л.М. Карпуков, проф, д.т.н.

Відповідальний за випуск: А.В. Коротун, доц., канд. фіз.-матем. наук

Затверджено
на засіданні кафедри
інформаційної безпеки
та наноелектроніки
Протокол № 4
від 21.12.2023 р.

Рекомендовано до видання
НМК ФРЕТ
Протокол № 5
від 24.02.2024 р.

ЗМІСТ

ЛАБОРАТОРНА РОБОТА № 1

АТАКА НА ГЕШ-ФУНКЦІЮ НА БАЗІ «ПАРАДОКСА ДНІВ НАРОДЖЕННЯ»

Мета роботи: ознайомлення з «Парадоксом днів народження», створення атаки на зменшену геш-функцію на базі парадокса.

Використовуване програмне забезпечення: програма hash.exe.

1.1 Завдання на лабораторну роботу

1. Створити Документ1 для гешування (див. Додаток В).
2. Знайти k геш-образів модифікованих документів змістовно відповідних Документу1. В якості геш-образу взяти перші 8 (-12) біт результату гешування за допомогою геш-функції MD5.
3. Створити Документ2 для гешування.
4. Знайти k геш-образів модифікованих документів змістовно відповідних Документу2. В якості геш-образу взяти також перші 8 (-12) біт результату гешування за допомогою геш-функції MD5.
5. Результати обчислення занести в таблицю.
6. Якщо є колізії, виписати їх; якщо ні, збільшити число модифікованих документів.

1.2 Зміст звіту

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

1.3 Контрольні питання

1. Що є геш-функція?
2. Опишіть «Парадокс днів народження».
3. Опишіть атаку на геш-функцію на базі парадокса.
4. Як розрахувати мінімальне значення модифікованих документів для гешування?

ЛАБОРАТОРНА РОБОТА № 2

ДИСКРЕТНЕ ЛОГАРИФМУВАННЯ НА БАЗІ «ПАРАДОКСА ДНІВ НАРОДЖЕННЯ»

Мета роботи: ознайомлення з методом розв'язання задачі дискретного логарифмування на базі «Парадокса днів народження».

Використовуване програмне забезпечення: пакет математичних обчислень Maple.

2.1 Завдання на лабораторну роботу

1. Розв'язати задачу дискретного логарифмування в мультиплікативній групі залишків по простому модулю

$$a^x = b \bmod n,$$

де n – модуль порівняння, просте число; число a має порядок $n-1$, $1 < a,b < n$ за допомогою методу на базі «Парадокса днів народження» (див. Додаток Г).

Параметри a, b, n взяти із таблиці 2.1 згідно з номером варіанта N.

Таблиця 2.1 – Варіанти для завдання 1

N	a	b	n		N	a	b	n		N	a	b	n
1	85	7	109		6	7	42	67		11	5	72	103
2	29	45	73		7	50	3	101		12	85	10	109
3	60	31	79		8	35	5	83		13	7	50	67
4	50	26	101		9	45	35	107		14	10	6	97
5	6	78	89		10	60	15	79		15	45	4	107
Додаткове завдання													
$a = 5 \quad b = 155075 \quad n = 313127$													

2. Розв’язати задачу дискретного логарифмування в групі точок еліптичної кривої $y^2 = x^3 + 35x + 8 \bmod 83$,

$$z \cdot P = Q,$$

де P і Q – точки еліптичної кривої $y^2 = x^3 + 35x + 8 \bmod 83$ над простим полем $GF(83)$; точка кривої P має простий порядок $n = 37$, за допомогою метода на базі «Парадокса днів народження» (див. Додаток Г).

Значення точок кривої P і Q взяти із таблиці 2.2 згідно з номером варіанту N.

2.2 Зміст звіту

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

2.3 Контрольні питання

1. В чому полягає задача дискретного логарифмування?
2. Назвіть методи розв’язання задачі дискретного логарифмування.
3. Поясніть метод розв’язання задачі дискретного логарифмування на базі «Парадокса днів народження».

Таблиця 2.2 – Варіанти для завдання 2

N	P,Q	N	P,Q
1	(61,25), (48,75)	26	(76,1), (70,26)
2	(21,25), (68,3)	27	(68,3), (11,8)
3	(61,25), (68,3)	28	(43,57), (10,69)
4	(76,1), (5,68)	29	(24,75), (13,81)
5	(10,69), (76,82)	30	(15,16), (10,14)
6	(48,75), (68,3)	31	(53,26), (43,26)
7	(10,14), (78,17)	32	(17,72), (12,9)
8	(68,80), (78,17)	33	(11,8), (76,1)
9	(76,82), (68,3)	34	(17,11), (10,69)
10	(61,58), (11,8)	35	(11,8), (78,17)
11	(12, 9), (43,26)	36	(68, 3), (15,16)
12	(53,57), (10,69)	37	(76,82), (61,25)
13	(1,58), (76,82)	38	(1,25), (17,72)
14	(78,17), (1,58)	39	(53,26), (10,14)
15	(21,25), (1,25)	40	(17,72), (12,9)
16	(12,74), (24,75)	41	(76,82), (48,75)
17	(11,75), (48,75)	42	(61,25), (48,75)
18	(17,72), (21,25)	43	(24,75), (78,17)
19	(70,57), (43,57)	44	(68, 3),(61,25)
20	(21,25), (76,82)	45	(1,58), (15,16)
21	(70,26), (15,16)	46	(21,25), (5,68)
22	(48,75), (68, 3)	47	(43,57), (10,14)
23	(43,26), (76,1)	48	(48, 8), (76,82)
24	(15,67), (10,69)	49	(48,75), (21,25)
25	(24,8), (13,81)	50	(13,81), (76,82)

ЛАБОРАТОРНА РОБОТА № 3

ДИСКРЕТНЕ ЛОГАРИФМУВАННЯ МЕТОДОМ ρ-ПОЛЛАРДА

Мета роботи: ознайомлення з методом дискретного логарифмування на еліптичній кривій методом ρ-Полларда.

Використовуване програмне забезпечення: пакет математичних обчислень Maple.

3.1 Завдання на лабораторну роботу

Розв'язати задачу дискретного логарифмування в групі точок еліптичної кривої $y^2 = x^3 + 35x + 8 \bmod 83$,

$$z \cdot P = Q,$$

де P і Q – точки еліптичної кривої $y^2 = x^3 + 35x + 8 \bmod 83$ над простим полем $GF(83)$; точка кривої P має простий порядок $n = 37$, за допомогою метода ρ-Полларда (див. Додаток Д).

Значення точок кривої P і Q взяти із таблиці 2.2 згідно з номером варіанту N.

3.2 Зміст звіту

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

3.3 Контрольні питання

1. В чому полягає задача дискретного логарифмування?
2. Назвіть методи розв'язання задачі дискретного логарифмування.
3. Поясніть метод ρ-Полларда.

ЛАБОРАТОРНА РОБОТА № 4
АНАЛІЗ КРИПТОСТІЙКОСТІ RSA

Мета роботи: ознайомлення з атакою на асиметричний алгоритм RSA.

Використовуване програмне забезпечення: пакет математичних обчислень Maple.

4.1 Завдання на лабораторну роботу

Нехай криптоаналітику відомі відкриті ключі e_1 і e_2 користувачів A1 і A2 відповідно, які створені на спільному модулі $n = 12162272489$ за алгоритмом RSA, а також відповідні шифрограми C_1 і C_2.

Провести атаку з розкриттям секретного повідомлення M (див. Додаток Е).

Значення відкритих ключів e_1 і e_2 та відповідних шифрограм C_1 і C_2 візьміть із таблиці 4.1 згідно з номером варіанту N.

4.2 Зміст звіту

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

4.3 Контрольні питання

1. Опишіть процедуру генерації ключів в RSA.
2. Опишіть процедури зашифрування та розшифрування в RSA.
3. Опишіть атаку на схему RSA з відомими відкритими ключами.

Таблиця 4.1 – Варіанти завдань

N	e_1	C_1	e_2	C_2
1	5475889	6091436646	23468903	6977126607
2	67689745	3471845557	134325463	847033404
3	464896961	7670557938	7646453621	7641167527
4	4647653	9065273591	1767431	8608374364
5	245463461	623759231	6524413	3006354849
6	4367568815	6893111790	876635231	1924847759
7	4564747423	2454058322	8556353	1240467970
8	558775	11195390998	265367	9782955589
9	3657586795	1880126857	635201	3959933249
10	23234647	7661936254	76574563	183998716
11	23219047	7086447156	746403421	2392912308
12	75647017	2419077363	43645703	7421700266
13	746403421	175526806	8556453241	7705525963
14	564563437	4002446316	946541	9473147619
15	86360563	11860971151	254656705	4971302099
16	354691	1315543290	23234647	9033967542
17	76574563	7951899063	23219047	6087951280
18	8556453241	465276200	546765803	6003680953
19	763456457	3985260736	23547803	2695092648
20	84654407	3640701575	234051161	5296760740

ЛАБОРАТОРНА РОБОТА № 5
АТАКИ НА СЛАБКІ ПІДПИСИ

Мета роботи: ознайомлення з методами криптоаналізу слабких схем цифрового підпису.

Використовуване програмне забезпечення: пакет математичних обчислень Maple.

5.1 Завдання на лабораторну роботу

Завдання виконуються в групі із 2-3 осіб.

1. Створить підробку підпису повідомлення M з хеш-образом $h = H(M)$ за допомогою відкритого ключа y користувача А за схемою Прикладу 1 Додатка Ж.

Відкритими загально-системними параметрами схеми є просте число $p = 398261$ і $g = 235$ – генератор мультиплікативної групи залишків за модулем p.

Значення відкритого ключа y користувача А і хеш-образу h повідомлення M візьміть із таблиці 5.1 згідно з номером варіанту N.

Створений підроблений підпис $\langle r, s \rangle$ передайте особі в групі для перевірки.

2. Отримайте підроблений підпис $\langle r, s \rangle$ за схемою Прикладу 1 Додатка Ж та необхідні параметри – $p = 398261$, $g = 235$, y, h – і здійсніть його перевірку.

3. Знайдіть секретний ключ x користувача А, якщо відомі справжні підписи $\langle r, s_1 \rangle$, $\langle r, s_2 \rangle$ документів M_1, M_2 з хеш-образами h_1, h_2 відповідно.

Відкритими загально-системними параметрами схеми є прості числа $p = 686519$, $q = 49037$ і $g = 200$ – генератор підгрупи порядку q мультиплікативної групи залишків за модулем p.

Створить «справжній підпис» повідомлення T з хеш-образом H за допомогою секретного ключа x користувача А за схемою Прикладу 2 Додатка Ж.

Значення підписів $\langle r, s_1 \rangle$, $\langle r, s_2 \rangle$ документів M_1, M_2 з хеш-образами h_1, h_2 , а також хеш-образ H повідомлення T візьміть із таблиці 5.1 згідно з номером варіанту N.

Створений «справжній» підпис $\langle r, s \rangle$ користувача А передайте особі в групі для перевірки.

4. Отримайте підроблений підпис $\langle r, s \rangle$ за схемою Прикладу 2 Додатка Ж, відкритий ключ $Y = 6527$ користувача А, хеш-образ H повідомлення T та необхідні параметри – $p = 686519$, $q = 49037$, $g = 200$ – і здійсніть його перевірку.

5.2 Зміст звіту

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

5.3 Контрольні питання

1. Які схеми цифрового підпису називаються слабкими?
2. Опишіть атаки на цифровий підпис.
3. Що називається екзистенційною підробкою цифрового підпису?
4. Що називається селективною підробкою цифрового підпису?
5. Чим відрізняється універсальна підробка від підробки «повне розкриття»?

Таблиця 5.1 – Варіанти завдань

N	y	h	r	s_1	s_2	h_1	h_2	H
1	54673	1056	8257	2011	44847	5465	5757	265
2	9732	83618	30967	42076	2709	4646	778	476
3	54758	9462	17128	3620	24108	86	7848	342
4	9045	26545	16984	18502	48910	575	474	806
5	65768	64657	44598	24241	33936	464	4874	34
6	2067	47703	36832	47377	19172	9574	4784	657
7	5877	302	3847	31149	13004	363	4378	986
8	2956	50473	12258	41469	13911	5895	474	960
9	28756	47435	2918	31856	28573	8046	4374	357
10	35435	32563	16317	35856	1979	353	4378	86
11	44647	489	20688	32903	26992	874	367	905
12	2535	57867	11493	37260	34653	625	4784	44
13	36757	5478	34885	39789	8387	5853	763	643
14	5757	87676	5694	33158	21483	5772	34	856
15	88585	656	10879	25145	27148	4746	96	25
16	58757	47656	36672	36439	48581	4747	356	854
17	39837	365	36583	22507	16805	3646	242	657
18	353	5478	34576	39616	37944	4674	6986	436
19	8678	808	37233	9003	30933	4473	6354	655
20	57543	64	7394	24728	28724	4748	9068	678
21	2073	46746	37969	15816	38245	4883	3653	56
22	7587	366	41743	27221	21314	324	3676	21
23	5785	46367	25728	13635	40979	3873	2536	567
24	76476	76443	30893	22684	30349	478	9868	100
25	76467	474	6527	19682	36493	473	7854	555

ЛАБОРАТОРНА РОБОТА № 6
АЛГОРИТМ БЕРЛЕКЕМПА – МЕССІ

Мета роботи: ознайомлення з алгоритмом Берлекемпа – Мессі формування характеристичного многочлена по першим елементам лінійної рекурентної послідовності.

Використовуване програмне забезпечення: пакет математичних обчислень Maple.

6.1 Завдання на лабораторну роботу

Дано $2k$ елементів лінійної рекурентної послідовності: s_0, s_1, s_2, …, s_{2k-1}. Знайти характеристичний многочлен та лінійне рекурентне співвідношення за допомогою алгоритма Берлекемпа – Мессі (див. Додаток К).

Знайти період послідовності s.

Елементи послідовності взяти із таблиці згідно з номером варіанта N:

Таблиця 6.1 – Варіанти завдань

N	s	N	s
1	(1100110100)	6	(1011011011)
2	(0101110010)	7	(0110010001)
3	(0101111000)	8	(1101001110)
4	(1001101111)	9	(0010111001)
5	(1001111100)	10	(0011110011)

6.2 Зміст звіту

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

6.3 Контрольні питання

1. Яким є призначення алгоритма Берлекемпа – Мессі?
2. Опишить алгоритм Берлекемпа – Мессі.

ЛАБОРАТОРНА РОБОТА № 7
АТАКА НА АЛГОРИТМ ЦИФРОВОГО ПІДПИСУ ЕЛЬГАМАЛЯ

Мета роботи: Ознайомитися з атакою на алгоритм цифрового підпису ЕльГамаля.

Використовуване програмне забезпечення: пакет математичних обчислень Maple.

7.1 Завдання на лабораторну роботу

Відкритим загально-системним параметром алгоритму є просте число

$p = 123657876889879868766137$.

Тоді

$p - 1 = 154572346111234983595767*8,$

$q = 15457234611234983595767,\ u = 8.$

1. Створить підробку підпису повідомлення M за допомогою відкритого ключа y користувача А за алгоритмом цифрового підпису ЕльГамаля (див. Додатка М).

Для цього задайте параметри $\alpha < p,\ c < u$ та обчисліть β і g.

Перевірте, що g є генератором мультиплікативної групи залишків за модулем p, тобто виконуються умови

$$g^{\frac{p-1}{q}} = g^8 \bmod p \neq 1,\ g^{\frac{p-1}{2}} = g^{4*q} \bmod p \neq 1.$$

Сформуйте та розв'яжіть задачу дискретного логарифмування відносно z

$$\left(g^q\right)^z = y^q \bmod p.$$

Зауважимо, що елемент $a = g^q \bmod p$ має порядок, не більший $u = 8$.

Отримане значення параметру z використайте для створення підробленого підпису $\langle r, s \rangle$ від імені абонента А.

2. Здійсніть перевірку підробленого підпису $\langle r, s \rangle$.

Значення відкритого ключа y користувача А і повідомлення M візьміть із таблиці 7.1 згідно з номером варіанту N.

7.2 Зміст звіту

1. Титульний лист, тема і мета роботи.
2. Обрані значення параметрів.
3. Сформовані значення параметрів.
4. Сформований підпис.
5. Результат перевірки підпису.
6. Висновки по роботі.

7.3 Контрольні питання

1. Які параметри є загальносистемними в алгоритмі цифрового підпису ЕльГамаля?
2. Опишіть атаку на алгоритм цифрового підпису ЕльГамаля.

Таблиця 7.1 – Варіанти завдань

N	y	M	N	y	M	N	y	M
1	34536	153	10	45643	78	19	6755	144
2	857	47	11	67575	223	20	53657	68
3	4225	218	12	8068	189	21	5766	95
4	976	103	13	356	30	22	6536	151
5	246246	188	14	467	162	23	53647	139
6	8756	252	15	24636	297	24	536467	160
7	68574	129	16	8544	273	25	5647	234
8	67754	306	17	7547	178	26	5347	227
9	6475	312	18	46357	35	27	357	183

ЛІТЕРАТУРА

1. Козіна Г.Л. Криптографія від історії до сучасних стандартів: навч.посібник/ Г.Л. Козіна. – Запоріжжя: НУ «Запорізька політехніка», 2020. – 192 с. – http://eir.zntu.edu.ua/handle/123456789/6528.
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. Topics in cryptography http://en.wikipedia.org/wiki/Topics_in_cryptography
6. Вербіцький О.В. Вступ до криптології. – Львів: ВНТЛ, 1998. – 248с.

Додаток А
Криптоатаки та їх складність

Атаки на симетричні алгоритми

В симетричній криптосистемі розрізняють 5 рівнів атак з боку криптоаналітика.

1. *Атака на основі тільки шифртексту* (ciphertext-only attack): криптоаналітику відомі декілька шифртекстів, що зашифровані на єдиному ключі;
2. *Атака на основі відомого (необраного) відкритого тексту* (known-plaintext attack): криптоаналітику відомі декілька шифртекстів, що зашифровані на єдиному ключі, а також відповідні їм відкриті тексти;
3. *Атака, на основі обраного відкритого тексту* (chosen-plaintext attack): криптоаналітик може вибрати необхідне число відкритих текстів й одержати відповідні їм шифровки (при цьому у випадку простої атаки такого типу всі відкриті тексти можуть бути обрані до одержання першої шифровки; у випадку адаптивної атаки криптоаналітик вибирає черговий відкритий текст, знаючи шифровки всіх попередніх);
4. *Атака на основі обраного шифртексту* (chosen-ciphertext attack): криптоаналітик може вибрати необхідну кількість шифровок й одержати відповідні їм відкриті тексти (у випадку простої атаки такого типу всі шифровки повинні бути обрані до одержання першого відкритого тексту; у випадку адаптивної атаки супротивник вибирає чергову шифровку, знаючи відкриті тексти всіх попередніх);
5. *Атака на основі обраного тексту* (chosen-text attack): криптоаналітик може атакувати криптосистему по обидва боки, тобто вибирати шифровки й дешифрувати їх, а також вибирати відкриті тексти й шифрувати їх (атака такого типу може бути простою, адаптивною, простою з однієї сторони й адаптивною з іншої).

В кожному випадку криптоаналітик повинен або визначити ключ, або виконати дешифрування деякого нового шифротексту, зашифрованого на тім же ключі, що й повідомлення, надані йому для дослідження на початковій стадії криптоаналізу.

Атаки перераховані в порядку зростання їхньої сили. Розходження в ступені дієвості, наприклад, атаки перших трьох рівнів можна показати на прикладі шифру простої заміни. При аналізі на основі тільки шифротексту для розкриття цього найпростішого шифру потрібно провести частотний криптоаналіз. У випадку атаки на основі відомого відкритого тексту розкриття шифру стає тривіальним особливо після того, як у відкритих текстах зустрінеться більшість символів використовуваного алфавіту. При атаці на основі обраного відкритого тексту шифр буде розкритий відразу після зашифрування алфавіту.

Складність атак

Тимчасова складність атаки на шифр є число кроків, необхідних для атакуючого алгоритму, щоб зламати шифр. Вона часто зводиться до визначення необхідної кількості розшифрувань. Тимчасова складність може бути розділена на: складність передобчислень, що визначається як об'єм обробки, самостійно проведеної криптоаналітиком, перш ніж він може захопити дані в законних сторін; і складність постобчислень, що визначається як об'єм обробки, необхідний криптоаналітику для одержання кінцевих даних. Звичайно більша з них використається як тимчасова складність.;

Складність пам'яті, необхідної для атаки на шифр, вимірюється по сумарній пам'яті, необхідній для виконання алгоритму атаки (кількість комірок пам'яті (у деякому відповідному пристрої), необхідна для збереження всіх даних, використовуваних під час атаки);

Складність даних визначається кількістю текстів (плайнтекстів, шифртекстів), які має у розпорядженні криптоаналітик при виконанні атаки (які він має у розпорядженні апріорно).

Іншими параметрами, використовуваними для виміру обчислювальних зусиль атаки є:

Імовірність успіху: частота здійснення цілей атаки.

Тип інформації: вид відновлюваної інформації (біти ключа, еквівалентний ключ, фрагменти відкритого тексту) і його кількість (повний ключ або тільки його частина).

Не всі параметри складності можуть бути підходящими для всіх типів атак. За повну складність атаки звичайно приймається найбільша

з тимчасової складності, складності пам'яті й складності даних. Помітимо, що для деяких контекстів атак об'єм пам'яті не так важливий, як важлива низька тимчасова складність. В інших ситуаціях можуть бути обмеженими і пам'ять, і час. Тому краще порівнювати різні атаки на основі «параметр-параметр» або залежно від конкретного застосування й контексту атаки.

В якості одного із критеріїв оцінки безпеки шифрів використовується співвідношення ресурсів, необхідних для злому шифру в розглянутій криптоаналітичній атаці, і ресурсів, необхідних для проведення на шифр атаки груба сила (прямого перебору ключів). Шифр вважається надійним, якщо не існує атак, складність яких менше прямого перебору ключів.

Додаток Б
Парадокс днів народження

Задача. «Яка повинна бути мінімальна кількість осіб у групі, щоб, принаймні, у двох з них збіглися дні народження з імовірністю, більшої $\frac{1}{2}$?»

Нехай n – число різних днів народжень (n = 365), r – кількість осіб у групі.

Усього комбінацій для r людей дорівнює n^r.

З них комбінацій з незбіжними значеннями

$$n\cdot(n-1)\cdot(n-2)\cdot\ldots\cdot(n-(r-1)).$$

Звідси ймовірність того, що в групі не буде людей з однаковими днями народження

$$P\{\text{не збігу}\} = \frac{n\cdot(n-1)\cdot(n-2)\cdot\ldots\cdot(n-(r-1))}{n^r} =$$

$$=1\cdot\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\ldots\left(1-\frac{r-1}{n}\right).$$

При більших n

$$P\{\text{не збігу}\}\approx$$

$$\approx 1-\frac{1}{n}-\frac{2}{n}\ldots-\frac{r-1}{n}=1-\frac{1+2+\ldots+(r-1)}{n}=1-\frac{(r-1)r}{2n}$$

Звідси

$$P\{\text{збігу}\} = \frac{(r-1)r}{2n},$$

1+2+3+…+m=m*(m+1)/2

P(A)=1-P(A)

За умовою задачі маємо

$$\frac{(r-1)r}{2n} > 1/2 \Rightarrow (r-1)r > n \Rightarrow r > \sqrt{n}.$$

$r > \sqrt{n}$

При $n = 365$ $r > 20$.

Більш точно $r \geq 23$:

```
n:=365;
for r from 2  to 52 do
  P:=1.:
  for i from 1  to r-1 do P:=P*(1-i/n) end do:
  print(r,1-P):
end do:
```

n := 365

2, 0.0027397260	19, 0.3791185261	36, 0.8321821064
3, 0.0082041659	20, 0.4114383836	37, 0.8487340082
4, 0.0163559125	21, 0.4436883352	38, 0.8640678211
5, 0.0271355737	22, 0.4756953077	39, 0.8782196644
6, 0.0404624837	23, 0.5072972344	40, 0.8912318098
7, 0.0562357031	24, 0.5383442580	41, 0.9031516115
8, 0.0743352924	25, 0.5686997041	42, 0.9140304716
9, 0.0946238339	26, 0.5982408203	43, 0.9239228556
10, 0.1169481777	27, 0.6268592824	44, 0.9328853686
11, 0.1411413783	28, 0.6544614725	45, 0.9409758995
12, 0.1670247888	29, 0.6809685376	46, 0.9482528434
13, 0.1944102752	30, 0.7063162428	47, 0.9547744028
14, 0.2231025120	31, 0.7304546338	48, 0.9605979729
15, 0.2529013198	32, 0.7533475279	49, 0.9657796093
16, 0.2836040053	33, 0.7749718542	50, 0.9703735796
17, 0.3150076653	34, 0.7953168646	51, 0.9744319933
18, 0.3469114179	35, 0.8143832389	52, 0.9780045093

Додаток В
Атака на геш-функцію

Криптоаналітик підготовлює два документа M і M'.

Нехай, документ M має вигляд :
«Зубенко Тетяна Олександрівна. Заробітна плата – 6500»,
а документ M' є підробкою документу M , наприклад,
«Зубенко Тетяна Олександрівна. Заробітна плата – 20000».

За допомогою певного генератора Криптоаналітик формує дві множини модифікованих документів (включення додаткових пробілів, заміна латиницею букв «о», «е», тощо). Перша множина відповідає за сенсом документу M , друга – M'.

Криптоаналітик обчислює геш-образи документів першої та другої множин.

Якщо знайдено співпадіння геш-образів документів із різних множин, задача криптоаналітика виконано.

Кількість r необхідних документів обчислюється за формулою

$$r \geq 2^{l/2},$$

де l – кількість двійкових розрядів відповідної геш-функції.

Якщо геш-образ має 8 розрядів, достатнє сформувати 2^4 документів кожної множини.

Модифікації початкового документу	Геши	Модифікації підробленого документу	Геши
Документ1.1	40	Документ2.1	54
Документ1.2	e3	Документ2.2	b3
Документ1.3	c2	Документ2.3	c5
Документ1.4	99	Документ2.4	4c
Документ1.5	8f	Документ2.5	84
Документ1.6	fe	Документ2.6	eb
Документ1.7	73	Документ2.7	07
Документ1.8	c3	Документ2.8	6f

Документ1.9	f9	Документ2.9	9f
Документ1.10	c4	Документ2.10	15
Документ1.11	86	Документ2.11	f9
Документ1.12	9a	Документ2.12	43
Документ1.13	75	Документ2.13	d0
Документ1.14	14	Документ2.14	ab
Документ1.15	54	Документ2.15	54
Документ1.16	59	Документ2.16	90

Колізії виникли з: «Документ1.9» та «Документ2.11», «Документ1.15» та «Документ2.1» або «Документ2.15»

В подальшому Документ з першої множини після отримання цифрового підпису може бути замінений на Документ з другої множини з тим самим геш-образом.

Наприклад, Документ1.9
«Зубенко Тетяна Олександрівна. Заробітна плата – 6500» (заміна - англійська буква і)

може бути замінений на Документ2.11.
«Зубенко Тетяна **О**лександрівна. Зар**о**бітна плата – 20000» (заміни - дві англійські букви о).

Підпис при цьому пройде перевірку, оскільки в формуванні підпису використовується не саме документ, а його геш-образ.

Додаток Г
Метод розв'язання задачі дискретного логарифмування на базі «Парадокса днів народження»

Задача 1. Знайти x, якій задовільняє порівнянню

$$a^x = b \bmod n,$$

де n – модуль порівняння, просте число; число a має порядок $n-1$, $1 < a,b < n$.

Метод базується на властивості порівнянь

$a^x = b \bmod n \Leftrightarrow a^{x \cdot z} = b^z \bmod n$, якщо $(z, n-1) = 1$.

Позначимо $y = x \cdot z$.

Тоді отримуємо $a^y = b^z \bmod n$.

Оберемо $2r$ випадковіх чисел $\{y_i\}$, $i = 1,...,r$, і $\{z_j\}$, $(z_j, n-1) = 1$, $j = 1,...,r$.

Обчислимо відповідно $2r$ значень $a^{y_i} \bmod n$ і $b^{z_j} \bmod n$.

Якщо буде знайдено співпадіння $a^{y_i} = b^{z_j} \bmod n$, то розв'язок задачі x обчислюється за формулою

$$x = \frac{y_i}{z_j} \bmod (n-1).$$

Згідно з парадоксом днів народження, $r \geq \sqrt{n-1}$.

Якщо співпадіння не буде знайдено, необхідно додати випадкових чисел $\{y_i\}$ і $\{z_j\}$.

Приклад 1.

Знайдемо x із порівняння $10^x = 8 \bmod 59$, ord 10 = 58.

Мінімальна кількість необхідних випадкових чисел r дорівнює $9 > \sqrt{58}$, $r = 9$, для кожної множини $\{y_i\}$ і $\{z_j\}$.

Результати обчислень зведемо в таблицю Г.1.

Таблиця Г.1 – Обчислення значень $a^{y_i} \bmod n$ та $b^{z_j} \bmod n$ для метода розв'язання задачі дискретного логарифмування в мультиплікативній групі залишків на базі «Парадокса днів народження»

i	y_i	$a^{y_i} \bmod n$
1	38	27
2	30	49
3	6	9
4	34	5
5	41	37
6	14	17
7	56	36
8	**39**	**34**
9	25	2

j	z_j	$b^{z_j} \bmod n$
1	35	52
2	23	42
3	27	47
4	**33**	**34**

$$a^{y_8} = b^{z_4} \bmod n$$

$$x = \frac{39}{33} \bmod 58$$

$$x = 17$$

Звідси $x = 17$.

Перевірка. $10^{17} \bmod 59 = 8$.

Задача 2. Знайти x, який задовільняє порівнянню

$$d \cdot P = Q,$$

де P і Q – точки еліптичної кривої $y^2 = x^3 + ax + b \bmod p$ над простим полем $GF(p)$; точка кривої P має простий порядок n.

Метод базується на властивості порівнянь

$$d \cdot P = Q \Leftrightarrow d \cdot z \cdot P = z \cdot Q, \text{ якщо } (z, n) = 1.$$

Позначимо $y = d \cdot z$.

Тоді отримуємо $y \cdot P = z \cdot Q$.

Оберемо $2r$ випадковіх чисел $\{y_i\}$, $i = 1,...,r$, і $\{z_j\}$, $y_i, z_j < n$, $j = 1,...,r$.

Обчислимо відповідно $2r$ значень $y_i \cdot P$ і $z_j \cdot Q$.

Якщо буде знайдено співпадіння $y_i \cdot P = z_j \cdot Q$, то розв'язок задачі x обчислюється за формулою

$$d = \frac{y_i}{z_j} \bmod n.$$

Згідно з парадоксом днів народження, $r \geq \sqrt{n-1}$.

Якщо співпадіння не буде знайдено, необхідно додати випадкових чисел $\{y_i\}$ і $\{z_j\}$.

Приклад 2.

Знайдемо x із порівняння

$$d \cdot (3,16) = (44,14),$$

де $P = (3,16)$ і $Q = (44,14)$ – точки еліптичної кривої $y^2 = x^3 + x + 38 \bmod 47$ над простим полем $GF(47)$; точка $P = (3,16)$ має простий порядок $n = 61$.

Мінімальна кількість необхідних випадкових чисел r дорівнює $8 > \sqrt{60}$, $r = 8$, для кожної множини $\{y_i\}$ і $\{z_j\}$.

Результати обчислень зведемо в таблицю Г.2.

Таблиця Г.2 – Обчислення значень $y_i \cdot P$ та $z_j \cdot Q$ для метода розв'язання задачі дискретного логарифмування в групі точок еліптичної кривої на базі «Парадокса днів народження»

i	y_i	$y_i \cdot P$
1	3	(34,32)
2	8	(5,36)
3	28	(29,43)
4	1	(3,16)
5	29	(32,28)
6	**53**	**(5,11)**
7	16	(40,8)
8	2	(19,17)

j	z_j	$z_j \cdot Q$
1	24	(23,14)
2	**20**	**(5,11)**

$$y_6 \cdot P = z_2 \cdot Q$$

$$d = \frac{53}{20} \bmod 61$$

$$d = 24$$

Звідси $d = 24$.

Перевірка.

$24 \cdot (3,16) = (44,14)$.

$$24 \cdot (3,16) = 16 \cdot (3,16) + 8 \cdot (3,16) = (40,8) + (5,36) = (44,14)$$

Додаток Д
Метод ρ-Полларда розв'язання задачі дискретного логарифмування

Розглянемо задачу дискретного логарифмування на еліптичній кривій.

Нехай задана еліптична крива $y^2 = x^3 + ax + b \bmod p$ над простим полем $GF(p)$ і точка P є базовою точкою порядку n адитивної групи точок еліптичної кривої.

Нехай точка Q належить заданій групі точок еліптичної кривої.

Задача: знайти число d , $1 \le d \le n-1$, таке, що:

$$d \cdot P = Q$$

Складність методу ρ – Полларда оцінюється як $I_\rho = \sqrt{\frac{\pi n}{4}}$.

Ідея методу полягає в процесі побудови послідовності точок Z_i еліптичної кривої : $Z_i = A_i P + B_i Q$, який забезпечує знаходження пари рівних точок $Z_i = Z_j$ (або $Z_i = -Z_j$, або $Z_i = P$, або $Z_i = Q$, або $Z_i = \mathrm{O}$).

1. Нехай $Z_i = Z_j$.

У цьому випадку одержимо $A_i P + B_i Q = A_j P + B_j Q$.

Якщо $B_i \neq B_j$, тоді $Q = \frac{A_j - A_i}{B_i - B_j} P$.

Таким чином,

$$d = \frac{A_j - A_i}{B_i - B_j} \bmod n .$$

2. Нехай $Z_i = -Z_j$.

У цьому випадку одержимо $A_iP + B_iQ = -A_jP - B_jQ$.

Якщо $B_i \neq -B_j$, тоді $Q = -\dfrac{A_j + A_i}{B_i + B_j} P$.

Таким чином,

$$d = -\frac{A_i + A_j}{B_i + B_j} \bmod n .$$

3. Нехай $Z_i = P$.

У цьому випадку одержимо $A_iP + B_iQ = P$.

Якщо $B_i \neq 0$, тоді $Q = \dfrac{1 - A_i}{B_i} P$.

Таким чином,

$$d = \frac{1 - A_i}{B_i} \bmod n .$$

4. Нехай $Z_i = Q$.

У цьому випадку одержимо $A_iP + B_iQ = Q$.

Якщо $B_i \neq 1$, тоді $Q = \dfrac{A_i}{1 - B_i} P$.

Таким чином,

$$d = \frac{A_i}{1 - B_i} \bmod n .$$

5. Нехай $Z_i = \mathrm{O}$.

У цьому випадку одержимо $A_iP + B_iQ = \mathrm{O}$.

Якщо $B_i \neq 0$, тоді $Q = -\frac{A_i}{B_i} P$.

Таким чином,

$$d = -\frac{A_i}{B_i} \bmod n .$$

Метод ρ – Полларда

Оберемо два випадкових числа A_0 і $B_0 \in [0, n-1]$, так щоб одночасно A_0 і B_0 не були рівними нулю:

$$Z_0 = A_0 P + B_0 Q .$$

Розіб'ємо відрізок $(0, p)$ на три рівних множини S_1, S_2 й S_3 і обчислимо Z_{i+1} рекурентне за правилом

$$Z_{i+1} = \begin{cases} 2Z_i, & \text{если} \quad Z_i^{\,x} \in S_1; \\ Z_i + P, & \text{если} \quad Z_i^{\,x} \in S_2; \\ Z_i + Q, & \text{если} \quad Z_i^{\,x} \in S_3; \end{cases}$$

де $Z_i^{\,x}$ визначає x - координату точки на еліптичній кривій.

Звідси

$$A_{i+1} = \begin{cases} 2A_i, & \text{если} \quad Z_i^{\,x} \in S_1; \\ A_i + 1, & \text{если} \quad Z_i^{\,x} \in S_2; \\ A_i, & \text{если} \quad Z_i^{\,x} \in S_3; \end{cases}$$

$$B_{i+1} = \begin{cases} 2B_i, & \text{если} \quad Z_i^{\,x} \in S_1; \\ B_i, & \text{если} \quad Z_i^{\,x} \in S_2; \\ B_i + 1, & \text{если} \quad Z_i^{\,x} \in S_3. \end{cases}$$

Приклад 1.

Візьмемо еліптичну криву $y^2 = x^3 + 2x + 6 \bmod 17$.

Базова точка $P = (2,1)$ має порядок $n = 11$.

Точка еліптичної кривої $Q = (13,6)$ задовольняє співвідношенню

$$d \cdot P = Q,\ 1 \le d \le n-1.$$

Тобто необхідно знайти число d, $1 \le d \le 10$:

$$d \cdot (2,1) = (13,6).$$

Знайдемо число d.

$$S_1 = [0,5],\ S_2 = [6,11],\ S_3 = [12,16].$$

Нехай $A_0 = 2$, $B_0 = 1$,

$$Z_0 = 2P + Q = (11,13).$$

$$Z_0^x = 11 \in S_2 \Rightarrow A_1 = 3, B_1 = 1,$$
$$Z_1 = Z_0 + P = (11,13) + (2,1) = (2,16).$$

$$Z_1^x = 2 \in S_1 \Rightarrow A_2 = 6, B_2 = 2,$$
$$Z_2 = 2Z_1 = 2 \cdot (2,16) = (11,13).$$

$$Z_2 = Z_0 \Rightarrow$$

$$d = \frac{A_2 - A_0}{B_0 - B_2} \bmod 11 = \frac{6-2}{1-2} \bmod 11 = -4 \bmod 11 = 7.$$

Звідси $d = 7$.

Результати обчислень зведені в таблицю Д.1.

Таблиця Д.1 - Обчислення коефіцієнтів за методом ρ-Полларда

i	A_i	B_i	Z_i	S
0	**2**	**1**	(11,13)	S_2
1	3	1	(2,16)	S_1
2	**6**	**2**	(11,13)	
$d = \frac{6-2}{1-2} \bmod 11 = 7$				

Перевірка.

$7 \cdot (2,1) = (13,6)$.

Приклад 2.

Нехай $P = (3,16)$ – базова точка еліптичної кривої $y^2 = x^3 + x + 38 \bmod 47$ порядку $n = 61$, точка $Q = (44,14)$ еліптичної кривої задовольняє співвідношенню

$d \cdot (3,16) = (44,14)$, $1 \le d \le 60$.

Знайдемо число *d*.

$S_1 = [0,15]$, $S_2 = [16,30]$, $S_3 = [31,46]$.

Результати обчислень зведені в таблицю Д.2.

Таблиця Д.2 - Обчислення коефіцієнтів за методом ρ-Полларда

i	A_i	B_i	Z_i	S
0	1	0	(3,16)	S_1
1	2	0	(19,17)	S_2
2	3	0	(34,32)	S_3
3	3	1	(23,14)	S_2
4	4	1	(29,43)	S_2
5	5	1	(32,28)	S_3
6	5	2	(5,11)	S_1
7	**10**	**4**	(40,39)	S_3
8	10	5	(5,36)	S_1
9	**20**	**10**	(40,8)	
$d = -\frac{20+10}{10+4} \bmod 61 = 24$				

$Z_9 = -Z_7 \Rightarrow$

$$d = -\frac{A_9 + A_7}{B_9 + B_7} \bmod 61 = -\frac{20+10}{10+4} \bmod 61 = 24.$$

Звідси $d = 24$.

Перевірка.

$24 \cdot (3,16) = (44,14)$.

Додаток Е
Атака на алгоритм RSA

Нехай в асиметричній криптосистемі з використанням алгоритму шифрування RSA пари ключів – секретний та відкритий – генеруються на спільному модулі n.

Покажемо, що в цьому випадку можлива атака на розкриття секретного повідомлення M.

Нехай користувачі системи A1, A2, …, Ai,… отримали пари ключів – секретний d_i та відкритий e_i, які генеруються на спільному модулі n: $d_i \cdot e_i = 1 \bmod \phi(n)$.

Нехай далі користувачеві D необхідно передати секретне повідомлення M деякій групі користувачів A1, A2, …, Ai,… асиметричної криптосистеми. Для цього він отримує відкриті ключі e_1, e_2, …, e_i, …. користувачів A1, A2, …, Ai,… відповідно і відкритий параметр – спільний модуль n.

Користувач D зашифровує повідомлення M за алгоритмом RSA: $C_i = M^{e_i} \bmod n$ та відправляє шифрограми C_1, C_2, …, C_i, …. користувачам системи A1, A2, …, Ai,… .

Криптоаналітик має можливість перехопити відкриті ключі e_1, e_2, …, e_i, … користувачів A1, A2, …, Ai,… відповідно і відкритий параметр – спільний модуль n, а також шифрограми C_1, C_2, …, C_i, …..

Нехай ключі e_1 і e_2 взаємно прості: $(e_1, e_2) = 1$. Тоді За алгоритмом Евкліда існують цілі числа x та y такі, що $e_1 \cdot x + e_2 \cdot y = 1$.

Тоді згідно з алгоритмом шифрування RSA маємо порівняння

$$C_1^x \cdot C_2^y \bmod n = M .$$

Таким чином, якщо криптоаналітику відомі відкриті ключі, спільний модуль і відповідні шифрограми, то він має можливість провести успішну атаку з розкриттям секретного повідомлення.

Приклад 1.

Нехай криптоаналітику відомі відкриті ключі $e_1 = 5646703$ і $e_2 = 85564645$ користувачів A1 і A2 відповідно, які створені на спільному модулі $n = 12162272489$ за алгоритмом RSA, та відповідні шифрограми $C_1 = 8653343404$ і $C_2 = 3323031838$. Проведемо атаку з розкриттям секретного повідомлення M.

Спочатку перевірімо взаємну простоту ключів e_1 і e_2: (5646703, 85564645) = 1.

Знайдемо x і y, що задовольняють умові $e_1 \cdot x + e_2 \cdot y = 1$:

$x = -22302953$, $y = 1471848$.

Тоді отримуємо повідомлення M в десятковому вигляді згідно з формулою $C_1^x \cdot C_2^y \bmod n = M$:

$$M = 8653343404^{-22302953} \cdot 3323031838^{1471848} \bmod 12162272489 =$$
$$= 5292019530 \cdot 8559378358 \bmod 12162272489 = 1718187621_{10}.$$

$$M = 1718187621_{10} = \text{`}66697665\text{`}_{16}.$$

Після декодування маємо

$M =$" *five*".

Атака проведена успішно.

Розв'язання рівняння $a \cdot x + b \cdot y = 1$.

Нехай необхідно розв'язати рівняння $a \cdot x + b \cdot y = 1$ для заданих a і b відносно x і y в цілих числах, при цьому $a > b$.

Рівняння $a \cdot x + b \cdot y = 1$ має розв'язок, якщо a і b взаємно прості: $(a, b) = 1$.

Для розв'язання рівняння $a \cdot x + b \cdot y = 1$ використовується розширений алгоритм Евкліда.

Згідно з алгоритмом Евкліда знаходимо залишки від ділення

$a = b \cdot q_0 + r_1$

$b = r_1 \cdot q_1 + r_2$

$r_1 = r_2 \cdot q_2 + r_3$

$r_2 = r_3 \cdot q_3 + r_4$

…….

$r_{n-2} = r_{n-1} \cdot q_{n-1} + r_n$

$r_{n-1} = r_n \cdot q_n$

Заповнюємо таблиці Е.1 та Е.2 за правилами:

положимо $(x_0, x_1) := (1,0)$, $(y_0, y_1) := (0,1)$, далі оновлення значень $(x_0, x_1) := (x_1, x_0 - x_1 \cdot q)$, $(y_0, y_1) := (y_1, y_0 - y_1 \cdot q)$.

Розв'язком рівняння є x_0, y_0.

Розглянемо роботу цього алгоритму на прикладі.

Приклад 2.

Розглянемо рівняння $17 \cdot x + 13 \cdot y = 1$.

Знайдемо залишки від ділення

$17 = 13 \cdot 1 + 4$

$13 = 4 \cdot 3 + 1$

$4 = 1 \cdot 4$

Побудуємо таблицю Е.1.

Звідси $x = x_0 = -3$.

Звідси $y = y_0 = 4$.

Таким чином, $x = -3$, $y = 4$.

Перевірка : $17 \cdot x + 13 \cdot y = 17 \cdot (-3) + 13 \cdot 4 = -51 + 52 = 1$.

Таблиця Е.1 – Пошук розв'язку x рівняння $17 \cdot x + 13 \cdot y = 1$

q_i		1	3	4
x_0	1	0	1	**-3**
x_1	0	1	-3	13

Таблиця Е.2 – Пошук розв'язку y

рівняння $17 \cdot x + 13 \cdot y = 1$

q_i		1	3	4
y_0	0	1	-1	**4**
y_1	1	-1	4	-17

Допоміжні функції пакету MAPLE

Приклад процедури, що реалізує зведення числа x в ступінь k по модулю p за допомогою алгоритму послідовного зведення в квадрат :

```
xkp:=proc(x,k,p) local i, mk, kb,lkb,bkb,a,b,bb;
if (k=0) then return(1) end if;
mk:=`if`(k>0,k,-k); kb:=convert(mk, binary):
lkb:=length(kb): bkb:=convert(mk,base,2):
a:=x; b:=1;
if (bkb[1] = 1) then b:=x mod p: end if:
for i from 2 to lkb do
  a:=a*a mod p: if (bkb[i] = 1) then b:=b*a mod p: end
if:
end do:
bb:=`if`(k>0,b,1/b mod p); return(bb): end proc;
```

Приклад програми, що реалізує атаку на RSA:

```
n:=12162272489:
e1:=5646703:  e2:=85564645:
gcd(e1, e2);
```

1

```
c1:=8653343404: c2:=3323031838:
igcdex(e1,e2,'s','t'):
s,t;
```

-22302953 , 1471848

```
m:=xkp(c1,s,n)*xkp(c2,t,n) mod n;
```

$m := 1718187621$

```
ma:=convert(m,hex);
```

$ma := 66697665$

```
att="five";
```

Додаток Ж
Атаки на слабкі підписи

Під слабкими схемами електронного цифрового підпису розуміють ті з них, які допускають підробку підпису. Це означає формування справжнього підпису деякого апріорі заданого повідомлення без знання секретного ключа. Багато систем електронного цифрового підпису, розглянуті як стійкі, допускають можливість сформувати без знання секретного ключа випадкові значення хеш-образу h й складових підпису $\langle r, s \rangle$, які задовольняють рівнянню перевірки підпису, тобто $\langle r, s \rangle$ є правильним підписом до h. Однак ці ж системи електронного цифрового підпису практично не дозволяють обчислити справжній підпис заданого документа, якщо секретний ключ є невідомим.

Розглянуті нижче приклади слабких схем електронного цифрового підпису складені в близькій аналогії до побудови стійких схем підпису. Однак деякі зовнішні незначні відмінності вносять неприпустиму слабість – можливість формування потенційним порушником (який не знає секретного ключа) справжнього підпису до заданого значення h.

Основні види атак на електронний цифровий підпис

1. *Атака на основі відомого відкритого ключа* (key-only attack) – сама слабка з атак, практично завжди доступна криптоаналітику;
2. *Атака на основі відомих підписаних повідомлень* (known-message attack) – у розпорядженні криптоаналітика є якесь (поліноміальне від k) число пар (повідомлення, підпис), при цьому криптоаналітик не може впливати на вибір повідомлення;
3. *Проста атака з вибором підписаних повідомлень* (generic chosen-message attack) – криптоаналітик має можливість вибрати деяку кількість підписаних повідомлень, при цьому відкритий ключ він одержує після цього вибору;
4. *Спрямована атака з вибором повідомлень* (directed chosen-message attack) – вибираючи підписані повідомлення, криптоаналітик знає відкритий ключ;
5. *Адаптивна атака з вибором повідомлень* (adaptive chosen-message attack) – криптоаналітик знає відкритий ключ, вибір кожного наступного підписаного повідомлення він може робити на основі

знання припустимого підпису попереднього обраного повідомлення.

6. *Атака на зв'язаних ключах* (related-key attack) – атакуючому відомий деякий математичний зв'язок між ключами.

Основні види загроз

1. *Екзистенціальна підробка* (existential forgery) – створення криптоаналітиком підпису для якого-н., можливо безглуздого, повідомлення, відмінного від перехопленого.
2. *Селективна підробка* (existential forgery) – створення підпису для заздалегідь обраного повідомлення.
3. *Універсальна підробка* (universal forgery) – знаходження ефективного алгоритму формування підпису, функціонально еквівалентного запропонованій схемі.
4. *Повне розкриття* (total break) – обчислення секретного ключа, що дає можливість формувати підпис для будь-яких повідомлень.

Атаки на цифровий підпис та загрози наведено в порядку складності. Найбільш надійними є схеми електронного цифрового підпису, стійкі проти екзистенційної підробки на основі адаптивної атаки.

Розглянемо приклади схем цифрового підпису, для яких можна зробити підробку.

Приклад 1.

Схема підпису

Загальносистемні параметри

Просте число p, g – генератор мультиплікативної групи залишків за модулем p, H – функція хешування.

Генерація ключів

Підписувач має асиметричну пару ключів: особистий $x : 1 < x < p$ та відкритий y: $y = g^x \bmod p$.

Формування цифрового підпису

Нехай підписувач має підписати електронний документ M з хеш-образом $H(M)$. Молодші $|p|-1$ розряди хеш-образу $H(M)$ формують десяткове число h, яке використається при обчисленні цифрового підпису.

Підписувач обирає одноразовий випадковий секретний ключ k $1<k<p-1$, обчислює число $r=g^k \bmod p$. Число r повинно бути взаємно простим з $(p-1)$. Якщо r і $(p-1)$ не взаємно прості, обирають інше k.

Підпис $s=\dfrac{k-x\cdot h}{r}\bmod(p-1)$.

Справжній підпис $\langle r,s\rangle$.

Перевірка цифрового підпису

Перевірка підпису $\langle r,s\rangle$ під електронним документом M здійснюється за допомогою відкритого ключа y підписувача.

Для перевірки обчислюються хеш-образ документу $H(M)$ та відповідне десяткове число h_M.

Якщо $r=g^{r\cdot s}\cdot y^{h_M} \bmod p$, цифровий підпис електронного документу M признається справжнім.

Підробка

«Справжній» підпис $\langle R,S\rangle$ під повідомленням T з хеш-образом $H(T)$ та відповідним значенням h_T від імені підписувача, якій має відкритий ключ y, формується таким чином.

Криптоаналітик обирає довільне ціле число z, $1<z<p-1$, таке що $\gcd(z,p-1)=1$, де $\gcd(a,b)$ – найбільш спільний дільник чисел a й b, та обчислює $R=g^z\cdot y^{h_T} \bmod p$.

Якщо $\gcd(R, p-1)=1$, підпис обчислюється за формулою $S=\frac{z}{R}\bmod(p-1)$.

Підробкою підпису є пара $\langle R,S\rangle$.

Якщо умова $\gcd(R, p-1)=1$ не виконується, Криптоаналітик обирає інше число z.

Покажемо, що підроблений підпис $\langle R,S\rangle$ задовольняє формулі перевірки підпису:

$$R = g^{z}\cdot y^{h_T} \bmod p = g^{R\cdot S}\cdot y^{h_T} \bmod p$$

В цьому прикладі наведена атака на основі відомого відкритого ключа. Криптоаналітик здійснив універсальну підробку підпису.

Приклад 2.

Схема підпису

Загальносистемні параметри

Просте число p, таке що $p=cq+1$, q – просте число, $q>2^{64}$, g – генератор підгрупи порядку q мультиплікативної групи залишків за модулем p, H – функція хешування.

Генерація ключів

Підписувач має асиметричну пару ключів: особистий $x: 1<x<p$ та відкритий y: $y=g^{-x}\bmod p$.

Формування цифрового підпису

Нехай підписувач має підписати електронний документ M з хеш-образом $H(M)$. Молодші $|p|-1$ розряди хеш-образу $H(M)$ формують десяткове число h_M, яке використається при обчисленні цифрового підпису.

Підписувач обирає одноразовий випадковий секретний ключ k, $1 < k < q$, обчислює число $r = (g^k \bmod p) \bmod q.$

Підпис $s = (k + x \cdot r \cdot h_M) \bmod q$.

Справжній підпис $\langle r, s \rangle$.

Перевірка цифрового підпису

Перевірка підпису $\langle r, s \rangle$ під електронним документом M здійснюється за допомогою відкритого ключа y підписувача.

Для перевірки обчислюються хеш-образ документу $H(M)$ та відповідне десяткове число h_M.

Якщо $(y^{r \cdot h_M} \cdot g^s \bmod p) \bmod q = r$, цифровий підпис електронного документу M признається справжнім.

Підробка

Передбачається, що в розпорядженні криптоаналітика є два справжніх підписи $\langle r, s_1 \rangle$, $\langle r, s_2 \rangle$ повідомлень $M1$, $M2$ з хеш-образами $H(M1)$, $H(M2)$ та відповідними значеннями h_1, h_2, $h_1 \neq h_2$, які сформовано підписувачем А.

Для значень s_1 та s_2 виконується співвідношення

$$s_1 = (k + x \cdot r \cdot h_1) \bmod q,$$
$$s_2 = (k + x \cdot r \cdot h_2) \bmod q.$$

Звідси знайдемо секретний ключ підписувача А

$$x = \frac{s_1 - s_2}{r \cdot (h_1 - h_2)} \bmod q.$$

В цьому прикладі наведена атака на основі відомих підписаних повідомлень та на зв'язаних ключах.

Криптоаналітик здійснив загрозу повного розкриття.

Додаток К
Алгоритм Берлекемпа – Мессі

Алгоритм Берлекемпа – Мессі дозволяє по $2k$ елементам лінійної рекурентної послідовності s_0, s_1, s_2, …, s_{2k-1} побудувати характеристичний многочлен $f(\lambda)$, якщо його степінь не перевищує k.

При виконанні алгоритму обчислюються послідовності многочленів $f_0(\lambda)$, $f_1(\lambda)$, $f_2(\lambda)$, …, $f_{2k}(\lambda)$ та цілих чисел l_0, l_1, l_2, …, l_{2k}, після чого формується характеристичний многочлен

$f(\lambda) = \lambda^{l_{2k}} \cdot f_{2k}(1/\lambda)$

степеня n .

Алгоритм Берлекемпа – Мессі

1. Положимо

$f_{-1}(\lambda) = 1$, $l_{-1} = -1$, $f_0(\lambda) = 1$, $l_0 = 0$.

2. Виконуємо в циклі для $t = 0, 1, 2, \ldots, 2k\text{-}1$:

2.1 обчислимо

$e_t = s_t \oplus \alpha_{t,1} \cdot s_{t-1} \oplus \alpha_{t,2} \cdot s_{t-2} \oplus \ldots \oplus \alpha_{t,l_t} \cdot s_{t-l_t}$,

де $\alpha_{t,i}$ – коефіцієнт при λ^i в многочлені $f_t(\lambda)$;

2.2 обчислимо число τ – максимальне число із множини $\{-1,0,1,2,\ldots,t\text{-}1\}$ таке, що $l_\tau < l_t$,

2.3 побудуємо многочлен

$$f_{t+1}(\lambda) = \begin{cases} f_t(\lambda) + f_\tau(\lambda) \cdot \lambda^{t-\tau}, & \text{якщо } e_t = 1 \\ f_t(\lambda), & \text{якщо } e_t = 0 \end{cases};$$

2.4 обчислимо число

$$l_{t+1} = \begin{cases} t+1-l_t, & \text{якщо } e_t = 1 \text{ і } l_t \le t/2 \\ l_t, & \text{інакше} \end{cases}.$$

Після виконання циклу побудуємо характеристичний многочлен

$f(\lambda) = \lambda^{l_{2k}} \cdot f_{2k}(1/\lambda)$.

Приклад.

Нехай дано 8-бітна послідовність 01001110.

$f_{-1}(\lambda) = 1,\ l_{-1} = -1,\ f_0(\lambda) = 1,\ l_0 = 0.$

Складемо таблицю

t	-1	0	1	2	3	4	5	6	7	8
l	-1	0								
$f_t(\lambda)$	1	1								

При $t = 0$

$e_0 = s_0 = 0,\ e_0 = 0;$

$\tau = -1;$

$f_1(\lambda) = f_0(\lambda) = 1,\ \ f_1(\lambda) = 1;$

$l_1 = l_0 = 0.$

t	-1	0	1	2	3	4	5	6	7	8
l	-1	0	0							
$f_t(\lambda)$	1	1	1							

При $t = 1$ індекс $t - l_t = 1$

$e_1 = s_1 = 1,\ e_1 = 1;$

$\tau = -1;$

$f_2(\lambda) = f_1(\lambda) + f_{-1}(\lambda) \cdot \lambda^2 = 1 + 1 \cdot \lambda^2 = 1 + \lambda^2,\ \ f_2(\lambda) = 1 + \lambda^2;$

$l_2 = t + 1 - l_1 = 2 - 0 = 2.$

t	-1	0	1	2	3	4	5	6	7	8
l	-1	0	0	2						
$f_t(\lambda)$	1	1	1	$1+\lambda^2$						

При $t = 2$ індекс $t - l_t = 0$, коефіцієнти $\alpha_{2,1} = 0,\ \alpha_{2,2} = 1$

$e_2 = s_2 \oplus \alpha_{2,1} \cdot s_1 \oplus \alpha_{2,2} \cdot s_0 = 0 \oplus 0 \cdot 1 \oplus 1 \cdot 0 = 0,\ e_2 = 0;$

$\tau = 1$;
$f_3(\lambda) = f_2(\lambda) = 1 + \lambda^2$, $f_3(\lambda) = 1 + \lambda^2$;
$l_3 = l_2 = 2$.

t	-1	0	1	2	3	4	5	6	7	8
l	-1	0	0	2	2					
$f_t(\lambda)$	1	1	1	$1+\lambda^2$	$1+\lambda^2$					

При $t = 3$ індекс $t - l_t = 1$, коефіцієнти $\alpha_{3,1} = 0$, $\alpha_{3,2} = 1$
$e_3 = s_3 \oplus \alpha_{3,1} \cdot s_2 \oplus \alpha_{3,2} \cdot s_1 = 0 \oplus 0 \cdot 0 \oplus 1 \cdot 1 = 1$, $e_3 = 1$;
$\tau = 1$; $t - \tau = 2$;
$f_4(\lambda) = f_3(\lambda) + f_1(\lambda) \cdot \lambda^2 = 1 + \lambda^2 + 1 \cdot \lambda^2 = 1$, $f_4(\lambda) = 1$;
$l_4 = l_3 = 2$.

t	-1	0	1	2	3	4	5	6	7	8
l	-1	0	0	2	2	2				
$f_t(\lambda)$	1	1	1	$1+\lambda^2$	$1+\lambda^2$	1				

При $t = 4$ індекс $t - l_t = 2$, коефіцієнти $\alpha_{4,1} = 0$, $\alpha_{4,2} = 0$
$e_4 = s_4 \oplus \alpha_{4,1} \cdot s_3 \oplus \alpha_{4,2} \cdot s_2 = 1 \oplus 0 \cdot 0 \oplus 0 \cdot 0 = 1$, $e_4 = 1$;
$\tau = 1$; $t - \tau = 3$;
$f_5(\lambda) = f_4(\lambda) + f_1(\lambda) \cdot \lambda^3 = 1 + 1 \cdot \lambda^3 = 1 + \lambda^3$, $f_5(\lambda) = 1 + \lambda^3$;
$l_5 = t + 1 - l_4 = 5 - 2 = 3$.

t	-1	0	1	2	3	4	5	6	7	8
l	-1	0	0	2	2	2	3			
$f_t(\lambda)$	1	1	1	$1+\lambda^2$	$1+\lambda^2$	1	$1+\lambda^3$			

При $t = 5$ індекс $t - l_t = 2$, коефіцієнти $\alpha_{5,1} = 0$, $\alpha_{5,2} = 0$, $\alpha_{5,3} = 1$
$e_5 = s_5 \oplus \alpha_{5,1} \cdot s_4 \oplus \alpha_{5,2} \cdot s_3 \oplus \alpha_{5,3} \cdot s_2 = 1 \oplus 0 \cdot 1 \oplus 0 \cdot 0 \oplus 1 \cdot 0 = 1$, $e_5 = 1$;
$\tau = 4$; $t - \tau = 1$;
$f_6(\lambda) = f_5(\lambda) + f_4(\lambda) \cdot \lambda = 1 + \lambda^3 + 1 \cdot \lambda = 1 + \lambda + \lambda^3$, $f_6(\lambda) = 1 + \lambda + \lambda^3$;
$l_6 = t + 1 - l_5 = 6 - 3 = 3$.

t	-1	0	1	2	3	4	5	6	7	8
l	-1	0	0	2	2	2	3	3		
$f_t(\lambda)$	1	1	1	$1+\lambda^2$	$1+\lambda^2$	1	$1+\lambda^3$	$1+\lambda+\lambda^3$		

При $t = 6$ індекс $t - l_t = 3$, коефіцієнти $\alpha_{6,1} = 1$, $\alpha_{6,2} = 0$, $\alpha_{6,3} = 1$

$e_6 = s_6 \oplus \alpha_{6,1} \cdot s_5 \oplus \alpha_{6,2} \cdot s_4 \oplus \alpha_{6,3} \cdot s_3 = 1 \oplus 1 \cdot 1 \oplus 0 \cdot 1 \oplus 1 \cdot 0 = 0$, $e_6 = 0$;

$\tau = 4$; $t - \tau = 2$;

$f_7(\lambda) = f_6(\lambda) = 1 + \lambda + \lambda^3$, $f_7(\lambda) = 1 + \lambda + \lambda^3$;

$l_7 = l_6 = 3$.

t	-1	0	1	2	3	4	5	6	7	8
l	-1	0	0	2	2	2	3	3	3	
$f_t(\lambda)$	1	1	1	$1+\lambda^2$	$1+\lambda^2$	1	$1+\lambda^3$	$1+\lambda+\lambda^3$	$1+\lambda+\lambda^3$	

При $t = 7$ індекс $t - l_t = 4$, коефіцієнти $\alpha_{7,1} = 1$, $\alpha_{7,2} = 0$, $\alpha_{7,3} = 1$

$e_7 = s_7 \oplus \alpha_{7,1} \cdot s_6 \oplus \alpha_{7,2} \cdot s_5 \oplus \alpha_{7,3} \cdot s_4 = 0 \oplus 1 \cdot 1 \oplus 0 \cdot 1 \oplus 1 \cdot 1 = 0$, $e_7 = 0$;

$\tau = 4$; $t - \tau = 3$;

$f_8(\lambda) = f_7(\lambda) = 1 + \lambda + \lambda^3$, $f_8(\lambda) = 1 + \lambda + \lambda^3$;

$l_8 = l_7 = 3$.

t	-1	0	1	2	3	4	5	6	7	8
l	-1	0	0	2	2	2	3	3	3	3
$f_t(\lambda)$	1	1	1	$1+\lambda^2$	$1+\lambda^2$	1	$1+\lambda^3$	$1+\lambda+\lambda^3$	$1+\lambda+\lambda^3$	$1+\lambda+\lambda^3$

Побудуємо характеристичний многочлен

$f(\lambda) = \lambda^{l_8} \cdot f_8(1/\lambda) = \lambda^3 \cdot (1 + 1/\lambda + 1/\lambda^3) = \lambda^3 + \lambda^2 + 1$,

$f(\lambda) = \lambda^3 + \lambda^2 + 1$,

і рекурентне співвідношення

$s_{k+3} = s_{k+2} \oplus s_k$.

Період знайденої послідовності

0100111 0100111 0100111 0100111 01001…..

дорівнює 7.

Додаток Л
Алгоритм підпису ЕльГамаля

Алгоритм ЕльГамаля є одним зі перших алгоритмів цифрового підпису. Цифровий підпис створюється за допомогою операцій в мультиплікативній групі залишків за модулем великого простого числа. Алгоритм ЕльГамаля не передбачає хешування повідомлення.

Відкритими параметрами алгоритму є випадкове просте число p та число g – генератор мультиплікативної групи залишків за модулем p. Секретним ключем підписувача А є число x, його відкритим ключем є число $y = g^x \bmod p$. Криптостійкість алгоритму підпису ЕльГамаля базується на обчислювальній складності задачі дискретного логарифмування. Для забезпечення криптостійкості цифрового підпису параметри алгоритму мають бути досить великими: 1024 або 2048 значущих бітів.

Цифровий підпис формується абонентом А за допомогою його секретного ключа, перевірка підпису здійснюється абонентом В з використанням відкритого ключа абонента А.

Загальносистемні параметри

p – випадкове просте число; g – генератор мультиплікативної групи залишків за модулем p.

Генерація ключів

Згенеруємо секретний та відкритий ключі абонента А.

Оберемо випадкове число x, $2 \le x \le p-2$.

Обчислимо $y = g^x \bmod p$.

Секретним ключем абонента А є число x.

Відкритим ключем абонента А є число y.

Формування цифрового підпису

Підписувачеві А необхідно підписати повідомлення M.

Він обирає випадкове число k, $2 \le k \le n-2$.

Далі підписувач А обчислює перший

$r = g^k \bmod p$

та другий елементи підпису

$s = \dfrac{M - x \cdot r}{k} \bmod (p-1)$.

(Число s не повинно бути 0.)

Цифровим підписом є пара чисел $\langle r, s \rangle$.

Перевірка цифрового підпису

Для перевірки підписаного абонентом А повідомлення $\{M, \langle r, s \rangle\}$ отримувач – абонент В – використовує відкриті загальносистемні параметри алгоритму ЕльГамаля – p, g – та відкритий ключ y підписувача А.

Якщо виконуються умови:

$r < p$,

$y^r \cdot r^s = g^M \bmod p$,

підпис $\{M, \langle r, s \rangle\}$ признається справжнім.

Приклад.

Нехай відкритими параметрами алгоритму ЕльГамаля є $p = 23$, $g = 5$.

Для генерування асиметричної пари ключів абонента А виберемо випадкове число $x = 12$ та обчислимо число

$y = g^x \bmod p = 5^{12} \bmod 23 = 18$.

Відкритим ключем абонента А є $x = 12$.

Секретним ключем абонента А є $y = 18$.

Нехай абоненту А необхідне підписати повідомлення $M = 17$.

Абонент А обирає випадкове число $k = 19$ та обчислює перший

$r = g^k \bmod p = 5^{19} \bmod 23 = 7$

та другий елементи підпису

$$s = \frac{M - x \cdot r}{k} \bmod (p-1) = \frac{17 - 12 \cdot 7}{19} \bmod 52 = 15.$$

з використанням секретного ключа $x = 12$.

Цифровим підписом є пара чисел $\langle r = 7, s = 15 \rangle$.

Для перевірки підписаного абонентом А повідомлення $\{M = 17, \langle r = 7, s = 15 \rangle\}$ використовуються відкриті загальносистемні параметри алгоритму ЕльГамаля $p = 23$, $g = 5$ та відкритий ключ $y = 18$ абонента А.

Оскільки виконуються умови:

$r < p$, тобто $7 < 23$,

$y^r \cdot r^s = g^M \bmod p$,

тобто $y^r \cdot r^s = 18^7 \cdot 7^{15} \bmod 23 = 15$ і $g^M = 5^{17} \bmod 23 = 15$;

підпис $\{M = 17, \langle r = 7, s = 15 \rangle\}$ признається справжнім.

Додаток М
Атака на алгоритм підпису ЕльГамаля

Атака була запропонована на конференції Eurocrypt'96 швейцарським криптографом Даниелем Блайхенбахером (Daniel Bleichenbacher, 1964 р.н.).

Атакуючий обирає спеціальним чином загальносистемні параметри – просте число p і твірний елемент g мультиплікативної групи залишків за модулем p – та надає їх підписувачу А для реалізації алгоритму ЕльГамаля. Це в подальшому дозволить атакуючому легко розв'язати задачу дискретного логарифмування для формування підпису по відкритому ключу y абонента А без знання його секретного ключа.

Атака на алгоритм підпису ЕльГамаля

Атакуючий обирає загальносистемний параметр p за умовою

$$p-1=q\cdot u,$$

де q – велике просте число, а число u має невеликі прості дільники.

Далі атакуючий обирає числа $\alpha < p$, $c < u$ таким чином, щоб елемент g, обчислений за формулою

$$g=\beta^{\alpha} \bmod p,$$

де $\beta = c\cdot q$,

був генератором мультиплікативної групи залишків за модулем p.

Загальносистемні параметри – p і g – атакуючий надає підписувачу А.

Зауважимо, що елемент $g^q \bmod p$ мультиплікативної групи залишків за модулем p має порядок, менший або рівний u:

$$\left(g^q\right)^u = g^{q\cdot u} = g^{p-1} = 1 \bmod p.$$

Тоді легко розв'язується задача дискретного логарифмування відносно z

$$\left(g^q\right)^z = y^q \bmod p,$$

де y – відомий атакуючому відкритий ключ абонента А.

За допомогою параметра z атакуючий може сформувати справжній підпис будь-якого повідомлення M без знання секретного ключа абонента А:

$$r = \beta,$$
$$s = \alpha(M - \beta \cdot z) \bmod (p-1).$$

Покажемо, що сформований підпис пройде перевірку підпису за алгоритмом ЕльГамаля:

$$y^r \cdot r^s = y^{c \cdot q} \cdot \beta^{\alpha \cdot (M - c \cdot q \cdot z)} = g^{c \cdot q \cdot z} \cdot g^{M - c \cdot q \cdot z} = g^M \bmod p.$$

Таким чином, атакуючий має можливість підробляти підпис абонента А для будь-якого документа за допомогою його відкритого ключа.

Приклад.

Нехай атакуючий обрав загальносистемний параметр $p = 53$.

Тоді $p - 1 = 52 = 13 \cdot 4$ і $q = 13$, $u = 4$.

Далі атакуючий обирає числа $\alpha < p$, $c < u$ таким чином, щоб елемент g, обчислений за формулою

$$g = \beta^\alpha \bmod p,$$

де $\beta = c \cdot q$,

був генератором мультиплікативної групи залишків за модулем p.

Загальносистемні параметри – p і g – атакуючий надає підписувачу А.

Нехай атакуючий обрав $\alpha = 7$, $c = 3$ та обчислив $\beta = c \cdot q = 3 \cdot 13 = 39$ і $g = \beta^\alpha \bmod p = 39^7 \bmod 53 = 51$.

Перевіримо, що $g = 51$ є генератором мультиплікативної групи залишків за модулем $p = 53$.

Число $p - 1 = 52$ має прості дільники 13 і 2.

Оскільки

$51^{\frac{52}{13}} = 51^4 \bmod 53 = 16 \neq 1,$

$51^{\frac{52}{2}} = 51^{26} \bmod 53 = 52 \neq 1,$

то $g = 51$ є генератором мультиплікативної групи залишків за модулем $p = 53$

Загальносистемні параметри – $p = 53$ і $g = 51$ – атакуючий надає підписувачу А.

Нехай атакуючому відомий відкритий ключ $y = 37$ абонента А.

Зауважимо, що елемент $g^q \bmod p = 51^{13} \bmod 53 = 23$ мультиплікативної групи залишків за модулем $p = 53$ має порядок, менший або рівний $u = 4$.

Тоді легко розв'язується задача дискретного логарифмування відносно z

$23^z = 52 \bmod 53,$

де $y^q \bmod p = 37^{13} \bmod 53 = 52.$

Обчислимо $23^2 \bmod 53 = 52$, $23^3 \bmod 53 = 30$, $23^4 \bmod 53 = 1.$

Звідси $z = 2$.

За допомогою параметра $z = 2$ атакуючий може сформувати справжній підпис будь-якого повідомлення M, наприклад, $M = 40$, без знання секретного ключа абонента А:

$r = \beta = 39,$

$s = \alpha(M - \beta \cdot z) \bmod(p-1) = 7(40 - 39 \cdot 2) \bmod 52 = 46.$

$\langle r = 39, s = 46 \rangle.$

Покажемо, що сформований підпис $\langle r = 39, s = 46 \rangle$ пройде перевірку підпису за алгоритмом ЕльГамаля:

$y^r \cdot r^s = 37^{39} \cdot 39^{46} \bmod 53 = 46,$

$g^M \bmod p = 51^{40} \bmod 53 = 46.$

Таким чином, атакуючий має можливість підробляти підпис абонента А для будь-якого документа M за допомогою його відкритого ключа.

Допоміжні функції пакету MAPLE

Приклад процедури, що реалізує алгоритм зведення в степінь за модулем – $x^k \bmod p$:

```
xkp:=proc(x,k,p) local i, mk, kb,lkb,bkb,a,b,bb;
if (k=0) then return(1) end if;
mk:=`if`(k>0,k,-k); kb:=convert(mk, binary):
lkb:=length(kb): bkb:=convert(mk,base,2):
a:=x; b:=1;
if (bkb[1] = 1) then b:=x mod p: end if:
for i from 2 to lkb do
  a:=a*a mod p:
  if (bkb[i] = 1) then b:=b*a mod p: end if:
end do:
bb:=`if`(k>0,b,1/b mod p);
return(bb):
end proc;
```

Приклад процедури, що реалізує алгоритм Шенкса розв'язання задачі дискретного логарифмування відносно змінної z

$$a^z = b \bmod p,$$

де елемент a мультиплікативної групи залишків за модулем p має порядок n:

```
Shanks:=proc(a,b,p,n) local i,j,m,A,t,gamma;
m:=ceil(sqrt(n));
A[0]:=1:
for j from 1 to m do A[j]:=A[j-1]*a mod p; end do;
t:=1/A[m] mod p; gamma:=b;
for i from 0 to m-1  do
for j from 0 to m do if (A[j]=gamma) then return(m*i+j)
end if end do; gamma:=gamma*t mod p end do;
end proc;
```