Типи задач

з дисципліни « Прикладна криптології »для КБ 31(6 семестр)

Задача 1. Визначте структурну скритність лінійної рекурентної послідовності, якщо база ЛРР m={7, 10, 12, 19, 31, 63, 89, 127, 257, 52}.

Структурна скритність визначається формулою:

$$S_c = \frac{l_0}{T},$$

де $l_0 = 2 \cdot m$ - відстань єдності, $T = 2^m - 1$ - період лінійної рекурентної послідовності.

Визначимо значення структурної скритності для значень m, які задані в умові задачі:

1) $S_c = \frac{2 \cdot m}{2^m - 1} = \frac{2 \cdot 7}{2^7 - 1} = \frac{14}{127} = 0{,}11$
2) $S_c = \frac{2 \cdot m}{2^m - 1} = \frac{2 \cdot 10}{2^{10} - 1} = \frac{20}{1023} = 0{,}02$
3) $S_c = \frac{2 \cdot m}{2^m - 1} = \frac{2 \cdot 12}{2^{12} - 1} = \frac{24}{4095} = 5{,}9 \cdot 10^{-3}$
4) $S_c = \frac{2 \cdot m}{2^m - 1} = \frac{2 \cdot 19}{2^{19} - 1} = \frac{38}{524287} = 72{,}5 \cdot 10^{-6}$
5) $S_c = \frac{2 \cdot m}{2^m - 1} = \frac{2 \cdot 31}{2^{31} - 1} = \frac{62}{2147483647} = 28{,}9 \cdot 10^{-9}$
6) $S_c = \frac{2 \cdot m}{2^m - 1} = \frac{2 \cdot 63}{2^{63} - 1} = \frac{126}{9223372036854775807} = 6{,}7 \cdot 10^{-18}$
7) $S_c = \frac{2 \cdot m}{2^m - 1} = \frac{2 \cdot 89}{2^{89} - 1} = \frac{178}{618970019642690137449562111} = 287{,}6 \cdot 10^{-27}$
8) $S_c = \frac{2 \cdot m}{2^m - 1} = \frac{2 \cdot 127}{2^{127} - 1} = \frac{254}{170141183460469231731687303715884105727} = 1{,}49 \cdot 10^{-36}$

9) $S_c = \frac{2 \cdot m}{2^m - 1} = \frac{2 \cdot 257}{2^{257} - 1} = \frac{514}{231584178474632390847141970017375815706539969331281128078915168015826259279871} = 2{,}2 \cdot 10^{-75}$

10) $S_c = \frac{2 \cdot m}{2^m - 1} = \frac{2 \cdot 52}{2^{52} - 1} = \frac{104}{4503599627370495} = 2{,}3 \cdot 10^{-14}$

Після проведених розрахунків можемо побачити, що при $m \to \infty$ структурна скритність $S_c \to 0$.

Задача.2. Знайдіть довжину відрізка гами шифрування потокового шифру, при якій ймовірність перекриття не перевищує 0,6 , якщо період гами $2^{128 + r}$, r – номер реєстрації.

Решение:

Если мы сгенерируем последовательность равную периоду(T),то у нас не будет перекрытия,но у нас дано что вероятность перекрытия не привышает 0.6 ,то есть длина последовательности может быть больше периода(T) на 0.6*T.

Следовательно общая длина отрезга гаммы шифрования=L

$L=T+0.6*T=2^{128 + 11}+0.6*2^{128 + 11} = 1.6*2^{139}$

Задача 3. Визначте закон формування лінійної рекурентної послідовності, $2 \cdot m$ перехоплених символів A_i якої наведено в таблиці 1.

Таблиця 1 – Значення A_i перехоплених символів

I	A_i	I	A_i
1	11110001	9	111111000001
2	01001101	10	111111011010
3	11110101	11	111111001010
4	11001000	12	1110000010
5	1111100011	13	11111110000111
6	1111100110	14	00110000011011
7	1111101000	15	00000010000011
8	00100010	16	11000001010101

Розв’язок

Візьмемо A_{13} = 11111110000111. Спочатку побудуємо систему рівнянь:

$$\begin{cases} x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 = 0 & (1) \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 = 0 & (2) \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 = 0 & (3) \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0 & (4) \\ x_1 \oplus x_2 \oplus x_3 = 1 & (5) \\ x_1 \oplus x_2 \oplus x_7 = 1 & (6) \\ x_1 \oplus x_6 \oplus x_7 = 1 & (7) \end{cases}$$

Складемо за модулем 2 (сума двоходнаковихелементівдорівнює 0)рівняння (1) та (2):

$$(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7) \oplus (x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6) = 0,$$

$$x_7 = 0.$$

Далі складемо друге та третє рівняння:

$$(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6) \oplus (x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5) = 0,$$

$$x_6 = 0.$$

Складемо (3) та (4) рівняння:

$$(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5) \oplus (x_1 \oplus x_2 \oplus x_3 \oplus x_4) = 0,$$

$$x_5 = 0.$$

Складемо (4) та (5) рівняння:

$$(x_1 \oplus x_2 \oplus x_3 \oplus x_4) \oplus (x_1 \oplus x_2 \oplus x_3) = 1,$$

$$x_4 = 1.$$

Тепер складемо (5) та (6) рівняння:

$(x_1 \oplus x_2 \oplus x_3) \oplus (x_1 \oplus x_2 \oplus x_7) = x_3 \oplus x_7 = 0$, оскільки $x_7 = 0$, то й $x_3 = 0$.

З рівняння (7) маємо:

$$x_1 \oplus 0 \oplus 0 = 1, \text{ тому } x_1 = 1.$$

З рівняння (6) маємо:

$$1 \oplus x_2 \oplus 0 = 1 \text{ а отже } x_2 = 0.$$

Таким чином тільки x_1і x_4 не нульові, тому $f(x) = x^7 + x^4 + 1$.

Зробимоперевірку. Сформуємо послідовність, підставивши в ЛРР початкове значення його стану «1111111»:

1 1 1 1 1 1 1
0 1 1 1 1 1 1
0 0 1 1 1 1 1
0 0 0 1 1 1 1
0 0 0 0 1 1 1
1 0 0 0 0 1 1
1 1 0 0 0 0 1
1 1 1 0 0 0 0
0 1 1 1 0 0 0
1 0 1 1 1 0 0
1 1 0 1 1 1 0
1 1 1 0 1 1 1
1 1 1 1 0 1 1
0 1 1 1 1 0 1

Таким чином вихідною є послідовність «11111110000111» і вона співпадає з A_{13}, тобто розв’язок зроблено правильно.

ЗАДАЧА 4. Визначте умови та розробіть методику реалізації загрози типу «повне розкриття» відносно ЕЦП. Конкретизуйте розв'язок задачі для випадку, коли як ЕЦП використовуються алгоритми визначені в ISO/IEC-15946-2.

Розв'язання задачі

Щоб реалізувати «повне розкриття» необхідне виконання наступних умов:

1) відомий відкритий ключ;
2) перехоплене повідомлення, створене за допомогою даного закритого ключа;
3) робота в групі точок заданої еліптичної кривої.

Реалізація загрози типу «повне розкриття» відносно ЕЦП полягає у розв'язанні рівняння $Y_i = a^{X_i} (mod\, p)$ відносно особистого ключа X_i.

Ця ЗАДАЧА зводиться до вирішення дискретного логарифмічного рівняння

$$X_i = \log_a Y_i \, (mod\, p).$$

ЕЦП згідно з ISO/IEC-15946-2 побудовані на еліптичних кривих. Тому «повне розкриття» полягає у розв'язанні рівняння $Q_i = d_i \cdot G(mod\, q)$відносно d_i. Таким чином необхідно розв'язати дискретне логарифмічне рівняння в групі точок еліптичної кривої. Для вирішення задачі можна застосовувати метод ρ-Поларда або інші методи дискретного логарифмування.

Задача 5. Визначити період повторення двійкової послідовності, що формується за допомогою двох лінійних рекурентних регістрів ЛРР1 та ЛРР2, якщо ЛРР1 та ЛРР2 реалізовані з використанням незвідних поліномів степенів $m_1 = 89$ та $m_2 = 127$ відповідно. В прикладі степені є числами Мерсена (прості).

Рішення

Якщо поліном $h(x)$ – незвідний, то довжина послідовності, яка генерується ЛРР, максимальна і дорівнює

$$T = 2^m - 1$$

$$T_1 = 2^{89} - 1 = 618970019642690137449562111 \approx 6{,}2 \cdot 10^{25}$$

$$T_2 = 2^{127} - 1 \approx 1{,}7 \cdot 10^{38}$$

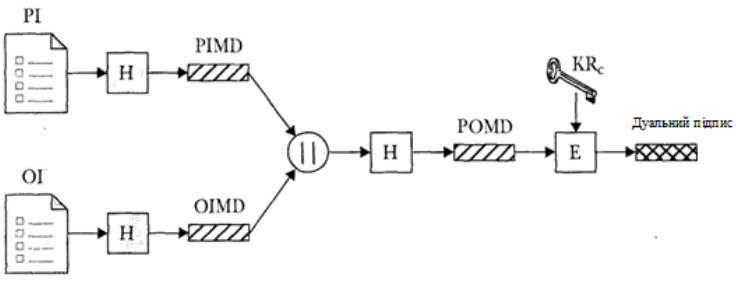
Задача 6. Поясніть вимоги та принципи реалізації ЕЦП дуального типу (наприклад, в протоколі SET).

Розв’язок.

Дуальний підпис (dualsignature) дозволяє зв’язати два повідомлення, призначені двом різним отримувачам. Розглянемо принципи реалізації дуального підпису у протоколі SET.

Покупцю потрібно переслати інформацію про замовлення (Order Information - OI) продавцю і платіжну інформацію (PaymentInformation — PI) банку. Продавцю не потрібно знати номер кредитної картки покупця, а банку не потрібні подробиці замовлення. Покупець же, розділяючи ці відомості, забезпечує тим самим додатковий захист своїх прав з погляду невтручання в його особисте життя. При цьому потрібно поєднати ці відомості так, щоб їх можна було використовувати при виникненні конфлікту.Зв’язокрозділених відомостей потрібендля того, щоб покупець міг довести, що даний платіж призначений для оплати саме цього, а не якогось іншого замовлення.

На рис.6.18.19.1 зображена схема використання дуального підпису для рішення проблеми зв’язування двох підписаних повідомлень.



PI - платіжна інформація
OI - інформація про замовлення
H - функція хешування (SHA-1)
|| - конкатенація

PIMD - профіль повідомлення PI
OIMD - профіль повідомлення
OI POMD - профіль комбінації повідомлень замовлення і платежу
E - шифрування (RSA)
KRc - особистий ключ підпису покупця

Рисунок 6.18.19.1. – Схема дуального підпису

Спочатку покупець, використовуючи алгоритм SHA-1, обчислює хеш- коди для повідомлень PI і OI. Два отриманих хеш-коди зв'язуються операцією конкатенації, і для результату зв'язування теж обчислюється хеш-код. Потім покупець шифрує підсумковий хеш-код з використанням свого особистого ключа цифрового підпису, у результаті отримуючи дуальний підпис. Уся процедура формально може бути записана в такому вигляді:

$$DS = E_{KR_C}[H(H(PI)||H(OI))],$$

де E_{KR_C}— особистий ключ цифрового підпису покупця. Тепер припустимо, що продавець має дуальний підпис (DualSignature- DS), повідомлення OI і профіль повідомлення PI (PIMessageDigest- PIMD). Крім того, у продавця є відкритий ключ покупця, що був витягнутий із сертифіката покупця. У таких умовах продавець може обчислити два таких значення:

$$H(PIMD||H(OI)) \text{ та} D_{KU_C}[DS],$$

де KU_C— відкритий ключ цифрового підпису покупця. Якщо обидва значення виявляються рівними, продавець вважає, що підпис перевірений. Точно так само, маючи DS, PI, профіль повідомлення OI (OIMD) і відкритий ключ покупця, банк може обчислити

$$H(H(PI)||OIMD) \text{ та} D_{KU_C}[DS].$$

І знову, якщо ці значення виявляються рівними, банк вважає, що підпис покупця перевірений. Підводячи підсумок, можна сказати, що:

1) Продавець отримує повідомлення *OI* і виконує перевірку підпису покупця.
2) Банк отримує повідомлення *PI* і виконує перевірку підпису покупця.
3) Повідомлення *OI* і *PI* виявляються зв'язаними, і покупець може довести їх зв'язок.

Припустимо, що продавець вирішить замінити повідомлення *OI* даної транзакції іншим, у надії витягти з цього вигоду. Для цього йому доведеться знайти інше повідомлення *OI* з точно таким же хеш-кодом*OIMD.*На сьогоднішній день при використанні алгоритму SHA-1 це є практично нерозв'язною задачею. Таким чином, у продавця немає можливості зв'язати з даним повідомленням *PI* інше повідомлення *OI.*

Задача.7. Знайти радіус зірки, у якої число атомів дорівнює порядку базової точки еліптичної кривої, якщо порядок базової точки $n = 2^{160 + k16}$, а радіус атома $k\ 10^{-12}$ метра, k - номер реєстрації.

Розв’язок задачі:

Цю задачу можна легко вирішити за допомогою однієї простої геометричної формули. Оскільки ми маємо радіус атома зіркиr_a, то можемо знайти його об'єм за формулою:

$$V_a = \frac{4}{3}\pi {r_a}^3$$

(1.1)

Щоб знайти приблизне значення об'єму зірки, необхідно отримане значення об'єму атому помножити на кількість атомів у зірці:

$$V_з = V_a * n \qquad (1.2)$$

Перетворимо формулу (1.1) для того, щоб знайти шуканий радіус зірки:

$$\frac{3V_з}{4\pi} = {r_з}^3$$

$$r_з = \sqrt[3]{\frac{3V_з}{4\pi}} \qquad (1.3)$$

Кінцевий результат отримаємо за формулою (1.3). Робимо розрахунки:

$$V_a = \frac{4}{3}\pi * (11 * 10^{-12})^3 = 1774{,}7\pi * 10^{-36}(м^3)$$

$$V_з = 1774{,}7\pi * 10^{-36} * 2^{336} = 2{,}48\pi * 10^{68}(м^3)$$

$$r_з = \sqrt[3]{\frac{3 * 2{,}48\pi * 10^{68}}{4\pi}} = 5{,}7 * 10^{22}(м)$$

Знайдений результат може бути розцінений як реальний, бо він співвідноситься з відомими радіусами реальних зірок.

Задача 8. В криптосистемі NTRU, що ґрунтується на перетвореннях в кільці зрізаних поліномів, використовується параметри , що наведені в таблиці.

Таблиця– Загальні параметри NTRU

Параметри	N	df
NTRU 167:3	167	61
NTRU 251:3	251	50
NTRU 503:3	503	216

Визначити число ключів f , які можна згенерувати, якщо Lf = L (df, df – 1), df визначає число коефіцієнтів, що дорівнюють (1), (df – 1) – число коефіцієнтів, що дорівнюють (-1), а ті що залишились (0) – нулі.

Рішення

Кількість різних вибірок коефіцієнтів, що дорівнюють (1) із загальної кількості коефіцієнтів n=N:

$$C_n^{df} = \frac{n!}{df!\,(n-df)!}$$

Кількість різних вибірок коефіцієнтів, що дорівнюють (-1) після того, як вибрали коефіцієнти (1) буде дорівнювати

$$C_{n-df}^{df-1} = \frac{(n-df)!}{(df-1)!\,(n-2df+1)!}$$

Оскільки всі коефіцієнти які залишаться будуть дорівнювати (0) то кількість їх різних вибірок буде дорівнювати одиниці.

Отже загальна кількість поліномів із заданою кількістю коефіцієнтів, що дорівнюють (1), (-1) та (0) розраховується за формулою:

$$M = C_{n-df}^{df-1} \cdot C_n^{df} \cdot 1 = \frac{n!}{df!\,(n-df)!} \cdot \frac{(n-df)!}{(df-1)!\,(n-2df+1)!} =$$

$$= \frac{n!}{df!\,(df-1)!\,(n-2df+1)!}$$

Параметри	N	df	M
NTRU 167:3	167	61	$6{,}46 \cdot 10^{76}$
NTRU 251:3	251	50	$3{,}34 \cdot 10^{100}$
NTRU 503:3	503	216	$5{,}42 \cdot 10^{216}$

Задача 9. Оцінити складність злому NTRU за методом лобової атаки на решітку для $N = 167, 251, 503$, якщо її можна обчислити за формулою $T = 2^{(0.4N - 3,5)}$. Обґрунтуйте застосування формули.

Задача 10. Нехай ЕЦП здійснюється з використанням ECDSA, причому використовується крива $y^2 \equiv x^3 + x + 1 (\mathrm{mod}\, 23)$.

Як базова використовується точка $G = (13,7)$ з порядком $n = 7$.

Необхідно:

– виробити асиметричну пару - особистий dI та відкритий Qi ключі;

– виробити цифровий підпис згідно з ECDSA, якщо $e = H(M) = 6$;

– перевірити цілісність та справжність повідомлення, у якого хеш-функція $e = H(M) = 6$.

Розв'язок

Спочатку сгенеруємо особистий ключ *d*, який належить інтервалу *[1, n – 1]*. Вибираємо випадково *d = 5*.

Розраховуємо відкритий ключ:

$$Q_i = d_i \cdot G = 5G = 5 \cdot (13,7)$$

Спочатку знайдемо точку $2G = 2 \cdot (13,7)$. Для цього скористаємось формулами для подвоєння точок на еліптичній кривій.

$$\lambda = \frac{3 \cdot x^2 + a}{2y} = \frac{3 \cdot 169 + 1}{2 \cdot 7} = \frac{508}{14} = \frac{254}{7} (mod\ 23) = \frac{1}{7} (mod\ 23) = 10$$

$$x_3 = \lambda^2 - 2 \cdot x = 100 - 26 = 74 (mod\ 23) = 5$$

$$y_3 = -y + \lambda(x - x_3) = -7 + 10(13 - 5) = 73 (mod\ 23) = 4$$

Отже, точка $2G = (5; 4)$. Перевіримо чи належить точка еліптичній кривій $y^2 \equiv x^3 + x + 1 (\mathrm{mod}\, 23)$:

$$4^2 = 5^3 + 5 + 1 (mod\ 23)$$

$$16 = 131 (mod\ 23)$$

$16 = 16 (mod\ 23)$ - точка $2G = (5; 4)$ належить еліптичній кривій.

Розрахуємо значення точки $4G = 2(2G) = 2(5; 4)$:

$$\lambda = \frac{3 \cdot 25 + 1}{2 \cdot 4} = \frac{76}{8} = \frac{19}{2} (mod\ 23) = 21$$

$$x_3 = \lambda^2 - 2 \cdot x = 441 - 10 = 431 (mod\ 23) = 17$$

$$y_3 = -y + \lambda(x - x_3) = -4 + 21(5 - 17) = -256 (mod\ 23) = 20$$

Точка $4G = (17; 20)$. Перевіримо чи належить точка еліптичній кривій $y^2 \equiv x^3 + x + 1 (\mathrm{mod}\, 23)$:

$20^2 = 17^3 + 17 + 1 (mod\ 23)$

$400 = 4931 (mod\ 23)$

$9 = 9 (mod\ 23)$ - точка $4G = (17; 20)$ належить еліптичній кривій.

Розрахуємо значення точки $5G = 4G + G = (17; 20) + (13; 7)$:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{20 - 7}{17 - 13} = \frac{13}{4} (mod\ 23) = 9$$

$x_3 = \lambda^2 - x_1 - x_2 = 81 - 17 - 13 = 51 (mod\ 23) = 5$

$y_3 = -y_1 + \lambda(x_1 - x_3) = -7 + 9(13 - 5) = 65 (mod\ 23) = 19$

Точка $5G = (5; 19)$. Перевіримо чи належить точка еліптичній кривій $y^2 \equiv x^3 + x + 1 (\mathrm{mod}\, 23)$:

$19^2 = 5^3 + 5 + 1 (mod\ 23)$

$361 = 131 (mod\ 23)$

$16 = 16 (mod\ 23)$ - точка $4G = (5; 19)$ належить еліптичній кривій.

Отже, особистий ключ *d* = 5, відкритий $Q = (5; 19)$.

Виробимо цифровий підпис при $e = H(M) = 6$:

1. Випадково генеруємо *k =2* з інтервалу *[1, n – 1]*.
2. Знаходимо $k \cdot G = 2G = (5; 4)$.
3. Виділяємо $x_1 = 5$.
4. Знаходимо $r = x_1 (mod\ n) = 5 (mod\ 7)$.
5. Обчислюємо значення $s = k^{-1}(e + dr) (mod\ n) = 2^{-1}(6 + 5 \cdot 5) (mod\ 7) = 5$.

Цифровий підпис має вигляд (5;5).

Зробимо перевірку підпису при $e = H(M) = 6$:

1. $w = s^{-1} (mod\ n) = 5^{-1} (mod\ 7) = 3$
2. $U_1 = w \cdot e (mod\ n) = 3 \cdot 6 (mod\ 7) = 18 (mod\ 7) = 4$

$U_2 = w \cdot r (mod\ n) = 3 \cdot 5 (mod\ 7) = 15 (mod\ 7) = 1$

3. $(x_1, y_1) = U_1 \cdot G + U_2 \cdot Q = 4G + Q = 4G + 5G = 9G (mod\ 7) = 2G = (5; 4)$.
4. Виділяємо $x_1 = 5$.
5. Знаходимо $v = x_1 (mod\ n) = 5 (mod\ 7)$.
6. Перевіряємо $r = v \quad \rightarrow 5 = 5$.

Отже, підпис справжній.

Задача 11.. Зробіть порівняння ЕЦП згідно ДСТУ 4145- 2002 та ГОСТ Р 34.10 – 2012 по критерію захищеності від атаки повне розкриття та по аналогії: ДСТУ 4145- 2002 та ISO 15946-2 (ECDSA); ДСТУ 4145- 2002 та ISO 15946-2 (EC G DSA); ДСТУ 4145- 2002 та ISO 15946-2 (EC KC DSA).

Погроза повне розкриття (total break) характеризується тим, що крипто аналітик може обчислити особистий ключ, можливо відмінний від *d*, але відповідний *Q*. Це дозволяє криптоаналітику формувати власні підписи будь-яких повідомлень.

Практичну оцінку погрозі повного розкриття дає параметр $t_б$ – безпечний час виконання криптоаналізу, який розраховується за формулою:

$$t_б = \frac{I}{\gamma \cdot K},$$

де I – складність криптоаналізу, γ – потужність крипто аналітичної системи, $k = 3{,}15 \cdot 10^7\, с/рік$ – кількість секунд у році. У свою чергу складність криптоаналізу розраховується за формулою:

$$I = \sqrt{\frac{\pi \cdot n}{4}},$$

де n – порядок базової точки. Розрахуємо $t_б$ для ДСТУ 4145- 2002, ГОСТ Р 34.10 – 2001, ECDSA, EC G DSA та EC KC DSA при мінімально можливих значеннях порядку базової точки,згідно зі стандартами, при потужності крипто аналітичної системи $\gamma = 10^{10}$ оп/с. Результати запишемо у таблицю 6.18.16.1

Таблиця 6.18.16.1 – Результати розрахунків

Назва алгоритму	n	$t_б$,років
ДСТУ 4145- 2002	2^{164}	10^7
ГОСТ Р 34.10 – 2001	2^{255}	$5 \cdot 10^{20}$
ECDSA	2^{161}	$4 \cdot 10^6$
EC G DSA	2^{161}	$4 \cdot 10^6$
EC KC DSA	2^{192}	$5{,}6 \cdot 10^{10}$

Згідно з отриманими результатами, можна зробити висновок, що при мінімальних значеннях порядку базової точки ДСТУ 4145- 2002 має кращу криптостійкість ніж алгоритми ECDSA та EC G DSA, але значення параметру t_6 для ДСТУ 4145- 2002 гірші ніж для EC KC DSA та ГОСТ Р 34.10 – 2001.

Але для алгоритмів EC KC DSA та ГОСТ Р 34.10 – 2001 значення максимального значення порядку базової точки обмежені(2^{256} та 2^{255} відповідно), а для алгоритмів ДСТУ 4145- 2002, ECDSA та EC G DSA існують лише межі мінімуму($n > 2^{163}, n > 2^{160}$).

Тобто ДСТУ 4145- 2002 більш захищений від погрози повного розкриття при великих значеннях порядку базової точки ніж KC DSA та ГОСТ Р 34.10 – 2001.

Задача 12. Знайдіть безпечний час криптосистеми ЕЦП в групах точок ЕК, якщо $\gamma = 10^7, 10^9$ та 10^{10} *операцій.складання/ЕК* , а $n = 2^{192}, 2^{224}, 2^{256}$ *та* 2^{512}.

Розв'язання

В загальному вигляді формула обчислення безпечного часу має вид:

$$t_б = \frac{N_в}{\gamma \cdot K} \cdot P_н,$$

де$N_в$ – кількість варіантів;γ - продуктивність криптоаналітичної системи; $P_н$ – імовірність, з якою необхідно здійснити криптоаналіз; К = 3,15·10^7 с/рік – наближене значення кількості секунд в році.

Якщо вважати, що $P_н$=1, то безпечний час криптосистеми ЕЦП в групах точок ЕК обчислюється за формулою:

$t_б = \frac{I}{\gamma \cdot K}$,деI– складність криптоаналізу.

Вважатимемо, що криптоаналіз здійснюється методом повного розкриття з використанням оптимального методу ρ- Поларда. В цьому випадку складність криптоаналізу визначається за формулою:

$I = \sqrt{\frac{\pi \cdot n}{4}}$, де *n* – порядок базової точки ЕК(період).

Отже, безпечний час обчислюється за такою формулою:

$$t_б = \frac{\sqrt{\pi \cdot n / 4}}{\gamma \cdot K} = \frac{\sqrt{\pi \cdot n}}{2 \cdot \gamma \cdot K}.$$

$n = 2^{192}; \gamma = 10^7 \rightarrow t_б = \frac{\sqrt{3{,}14 \cdot 2^{192}}}{2 \cdot 10^7 \cdot 3{,}15 \cdot 10^7} \approx \frac{1{,}77 \cdot 2^{98}}{6{,}3 \cdot 10^{14}} = \frac{1{,}77 \cdot 10^{29{,}4}}{6{,}3 \cdot 10^{14}} \approx 0{,}7 \cdot 10^{15}$ (років);

$n = 2^{192}; \gamma = 10^9 \rightarrow t_б = \frac{\sqrt{3{,}14 \cdot 2^{192}}}{2 \cdot 10^9 \cdot 3{,}15 \cdot 10^7} \approx \frac{1{,}77 \cdot 2^{98}}{6{,}3 \cdot 10^{16}} = \frac{1{,}77 \cdot 10^{29{,}4}}{6{,}3 \cdot 10^{16}} \approx 0{,}7 \cdot 10^{13}$ (років);

$n = 2^{192}; \gamma = 10^{10} \rightarrow t_б = \frac{\sqrt{3{,}14 \cdot 2^{192}}}{2 \cdot 10^{10} \cdot 3{,}15 \cdot 10^7} \approx \frac{1{,}77 \cdot 2^{98}}{6{,}3 \cdot 10^{17}} = \frac{1{,}77 \cdot 10^{29{,}4}}{6{,}3 \cdot 10^{17}} \approx 0{,}7 \cdot 10^{12}$

(років);

$n = 2^{224}; \gamma = 10^7 \rightarrow t_б = \frac{\sqrt{3{,}14 \cdot 2^{224}}}{2 \cdot 10^7 \cdot 3{,}15 \cdot 10^7} \approx \frac{1{,}77 \cdot 2^{112}}{6{,}3 \cdot 10^{14}} = \frac{1{,}77 \cdot 10^{33{,}6}}{6{,}3 \cdot 10^{14}} \approx 1{,}1 \cdot 10^{19}$ (років);

$n = 2^{224}; \gamma = 10^9 \rightarrow t_б = \frac{\sqrt{3{,}14 \cdot 2^{224}}}{2 \cdot 10^9 \cdot 3{,}15 \cdot 10^7} \approx \frac{1{,}77 \cdot 2^{112}}{6{,}3 \cdot 10^{16}} = \frac{1{,}77 \cdot 10^{33{,}6}}{6{,}3 \cdot 10^{16}} \approx 1{,}1 \cdot 10^{17}$ (років);

$n = 2^{224}; \gamma = 10^{10} \rightarrow t_б = \frac{\sqrt{3{,}14 \cdot 2^{224}}}{2 \cdot 10^{10} \cdot 3{,}15 \cdot 10^7} \approx \frac{1{,}77 \cdot 2^{112}}{6{,}3 \cdot 10^{17}} = \frac{1{,}77 \cdot 10^{33{,}6}}{6{,}3 \cdot 10^{17}} \approx 1{,}1 \cdot 10^{16}$

(років);

$n = 2^{256}; \gamma = 10^7 \rightarrow t_б = \frac{\sqrt{3{,}14 \cdot 2^{256}}}{2 \cdot 10^7 \cdot 3{,}15 \cdot 10^7} \approx \frac{1{,}77 \cdot 2^{128}}{6{,}3 \cdot 10^{14}} = \frac{1{,}77 \cdot 10^{38{,}4}}{6{,}3 \cdot 10^{14}} \approx 0{,}7 \cdot 10^{24}$ (років);

$n = 2^{256}; \gamma = 10^9 \rightarrow t_б = \frac{\sqrt{3{,}14 \cdot 2^{256}}}{2 \cdot 10^9 \cdot 3{,}15 \cdot 10^7} \approx \frac{1{,}77 \cdot 2^{128}}{6{,}3 \cdot 10^{16}} = \frac{1{,}77 \cdot 10^{38{,}4}}{6{,}3 \cdot 10^{16}} \approx 0{,}7 \cdot 10^{22}$ (років);

$n = 2^{256}; \gamma = 10^{10} \rightarrow t_б = \frac{\sqrt{3,14 \cdot 2^{256}}}{2 \cdot 10^{10} \cdot 3,15 \cdot 10^{7}} \approx \frac{1,77 \cdot 2^{128}}{6,3 \cdot 10^{17}} = \frac{1,77 \cdot 10^{38,4}}{6,3 \cdot 10^{17}} \approx 0,7 \cdot 10^{21}$ (років);

$n = 2^{512}; \gamma = 10^{7} \rightarrow t_б = \frac{\sqrt{3,14 \cdot 2^{512}}}{2 \cdot 10^{7} \cdot 3,15 \cdot 10^{7}} \approx \frac{1,77 \cdot 2^{256}}{6,3 \cdot 10^{14}} = \frac{1,77 \cdot 10^{76,9}}{6,3 \cdot 10^{14}} \approx 2,2 \cdot 10^{62}$ (років);

$n = 2^{512}; \gamma = 10^{9} \rightarrow t_б = \frac{\sqrt{3,14 \cdot 2^{512}}}{2 \cdot 10^{9} \cdot 3,15 \cdot 10^{7}} \approx \frac{1,77 \cdot 2^{256}}{6,3 \cdot 10^{16}} = \frac{1,77 \cdot 10^{76,9}}{6,3 \cdot 10^{16}} \approx 2,2 \cdot 10^{60}$ (років);

$n = 2^{512}; \gamma = 10^{10} \rightarrow t_б = \frac{\sqrt{3,14 \cdot 2^{512}}}{2 \cdot 10^{10} \cdot 3,15 \cdot 10^{7}} \approx \frac{1,77 \cdot 2^{256}}{6,3 \cdot 10^{17}} = \frac{1,77 \cdot 10^{76,9}}{6,3 \cdot 10^{17}} \approx 2,2 \cdot 10^{59}$ (років).

Задача 13. При виробці цифрового підпису використовуються однонаправленігеш-функції SHA-1 ГОСТ 34.311-95 та SHA-2. Вони формують геш значення для SHA-1 довжина l =160 бітів, для ГОСТ 34.311-95 l=256 бітів і SHA-2 – 256, 384 чи 512 бітів. Оракул здійснює обчислення геш значень зі швидкістю $V_1 = 1{,}2 \cdot 10^{10}$ Мбіт/с для SHA-1, $V_2 = 1{,}7 \cdot 10^9$ для ГОСТ 34.311-95, $V_3 = 2{,}7 \cdot 10^9$ для SHA-2 (lh=256 бітів) і $V_4 = 1{,}8 \cdot 10^9$ для SHA-2 (lh=512 бітів). Необхідно знайти імовірність екзистенціальної підробки, якщо оракул функціонує протягом одного року.

Розв’язок задачі:

Розв’язок задачі знайдемо, використовуючи загальну теорію колізій, що базується на «парадоксі про день народження».

Справедливе рівняння:

$$P_k = 1 - e^{-\frac{k(k-1)}{2n}}$$

(6.1)

де k – число обчислень, зроблених оракулом за один рік, n – розмір множини допустимих геш-значень, P_k – вірогідність колізії.

Обчислимо значення для n_i та k_i. Значення n_i обчислимо таким чином:

$$n_1 = 2^{160} \approx 10^{48}$$

$$n_2 = n_3 = 2^{256} \approx 10^{77}$$

$$n_4 = 2^{512} \approx 10^{154}$$

Далі обчислюємо число k геш-значень, що можуть бути сформовані оракулом протягом року, якщо довжина повідомлень, що гешуються - $I_m = 1\text{Кбайт} = 8 * 10^3\text{Кбіт}$.

$$k = \frac{V_i * K}{l_M}$$

(6.2)

де $K = 3{,}15 * 10^7$ с/рік.

Підставивши значення в формулу, отримаємо наступне:

$$k_1 = \frac{1{,}2 * 10^{10} * 3{,}15 * 10^7}{8 * 10^3} = 4{,}7 * 10^{13}$$

$$k_2 = \frac{1{,}7 * 10^{9} * 3{,}15 * 10^7}{8 * 10^3} = 6{,}7 * 10^{12}$$

$$k_3 = \frac{2{,}7 * 10^{9} * 3{,}15 * 10^7}{8 * 10^3} = 1{,}1 * 10^{13}$$

$$k_4 = \frac{1{,}8 * 10^{9} * 3{,}15 * 10^7}{8 * 10^3} = 5{,}8 * 10^{12}$$

Так як усі $k_i \ll 0{,}1n_i$, то для обчислення імовірності колізії можна використати формулу:

$$P_k = 1 - e^{-\frac{k(k-1)}{2n}} = 1 - e^{\frac{-k^2}{2n}}$$

(6.3)

Підставивши у формулу (6.3) знайдені значення k_i та n_i, отримаємо:

$$P_1 = 1 - e^{\frac{-(4{,}7*10^{13})^2}{2*10^{48}}} \approx 1 - e^{-21} = 1 - e^{-21} \approx 10^{-10^{21}}$$

$$P_2 = 1 - e^{\frac{-(6{,}7*10^{12})^2}{2*10^{77}}} \approx 1 - e^{-10^{-52}} \approx 10^{-10^{52}}$$

$$P_3 = 1 - e^{\frac{-(1{,}1*10^{13})^2}{2*10^{77}}} \approx 1 - e^{-10^{-50}} \approx 10^{-10^{50}}$$

$$P_2 = 1 - e^{\frac{-(5{,}8*10^{12})^2}{2*10^{154}}} \approx 1 - e^{-10^{-128}} \approx 10^{-10^{128}}$$

Із наведених розрахунків випливає, що усі представлені геш-функції є колізійно стійкими, тому ЕЦП на основі ECDSA є захищенною від загрози типу екзистенціальна підробка.

Задача 14. Зробіть порівняння ЕЦП згідно ДСТУ 4145- 2002 та ГОСТ Р 34.10 – 2001 по критерію захищеності від атаки повне розкриття та по аналогії: ДСТУ 4145- 2002 та ISO 15946-2 (ECDSA); ДСТУ 4145- 2002 та ISO 15946-2 (EC G DSA); ДСТУ 4145- 2002 та ISO 15946-2 (EC KC DSA).
Погроза повне розкриття (total break) характеризується тим, що крипто аналітик може обчислити особистий ключ, можливо відмінний від *d*, але відповідний *Q*. Це дозволяє криптоаналітику формувати власні підписи будь-яких повідомлень.

Практичну оцінку погрозі повного розкриття дає параметр $t_б$ – безпечний час виконання криптоаналізу, який розраховується за формулою:

$$t_б = \frac{I}{\gamma \cdot K},$$

де I – складність криптоаналізу, γ – потужність крипто аналітичної системи, $k = 3{,}15 \cdot \cdot 10^7 с/рік$ – кількість секунд у році. У свою чергу складність криптоаналізу розраховується за формулою:

$$I = \sqrt{\frac{\pi \cdot n}{4}},$$

де n – порядок базової точки. Розрахуємо $t_б$ для ДСТУ 4145- 2002, ГОСТ Р 34.10 – 2001, ECDSA, EC G DSA та EC KC DSA при мінімально можливих значеннях порядку базової точки,згідно зі стандартами, при потужності крипто аналітичної системи $\gamma = 10^{10}$ оп/с. Результати запишемо у таблицю 6.18.16.1

Таблиця 6.18.16.1 – Результати розрахунків

Назва алгоритму	n	$t_б$,років
ДСТУ 4145- 2002	2^{164}	10^7
ГОСТ Р 34.10 – 2001	2^{255}	$5 \cdot 10^{20}$
ECDSA	2^{161}	$4 \cdot 10^6$
EC G DSA	2^{161}	$4 \cdot 10^6$
EC KC DSA	2^{192}	$5{,}6 \cdot 10^{10}$

Згідно з отриманими результатами, можна зробити висновок, що при мінімальних значеннях порядку базової точки ДСТУ 4145- 2002 має кращу криптостійкість ніж алгоритми ECDSA та EC G DSA, але значення параметру t_6 для ДСТУ 4145- 2002 гірші ніж для EC KC DSA та ГОСТ Р 34.10 – 2001.

Але для алгоритмів EC KC DSA та ГОСТ Р 34.10 – 2001 значення максимального значення порядку базової точки обмежені(2^{256} та 2^{255} відповідно), а для алгоритмів ДСТУ 4145- 2002, ECDSA та EC G DSA існують лише межі мінімуму($n > 2^{163}, n > 2^{160}$).

Тобто ДСТУ 4145- 2002 більш захищений від погрози повного розкриття при великих значеннях порядку базової точки ніж KC DSA та ГОСТ Р 34.10 – 2001.

Задача 15. Нехай ЕЦП здійснюється з використанням ECDSA, причому використовується крива $y^2 \equiv x^3 + x + 1 \bmod 23$.

Як базова використовується точка *G=(13,7)* з порядком *n=7*.

Необхідно:

– виробити асиметричну пару - особистий d_i та відкритий Q_i ключі;

– виробити цифровий підпис згідно з ECDSA, якщо *e=H(M)=6*.

Розв'язок

Спочатку сгенеруємо особистий ключ *d*, який належить інтервалу *[1, n – 1]*. Вибираємо випадково *d = 5*.

Розраховуємо відкритий ключ:

$$Q_i = d_i \cdot G = 5G = 5 \cdot (13,7)$$

Спочатку знайдемо точку $2G = 2 \cdot (13,7)$. Для цього скористаємось формулами для подвоєння точок на еліптичній кривій.

$$\lambda = \frac{3 \cdot x^2 + a}{2y} = \frac{3 \cdot 169 + 1}{2 \cdot 7} = \frac{508}{14} = \frac{254}{7} (mod\ 23) = \frac{1}{7} (mod\ 23) = 10$$

$$x_3 = \lambda^2 - 2 \cdot x = 100 - 26 = 74 (mod\ 23) = 5$$

$$y_3 = -y + \lambda(x - x_3) = -7 + 10(13 - 5) = 73 (mod\ 23) = 4$$

Отже, точка $2G = (5; 4)$. Перевіримо чи належить точка еліптичній кривій $y^2 \equiv x^3 + x + 1 (\bmod 23)$:

$$4^2 = 5^3 + 5 + 1 (mod\ 23)$$

$$16 = 131 (mod\ 23)$$

$16 = 16 (mod\ 23)$ - точка $2G = (5; 4)$ належить еліптичній кривій.

Розрахуємо значення точки $4G = 2(2G) = 2(5; 4)$:

$$\lambda = \frac{3 \cdot 25 + 1}{2 \cdot 4} = \frac{76}{8} = \frac{19}{2} (mod\ 23) = 21$$

$$x_3 = \lambda^2 - 2 \cdot x = 441 - 10 = 431 (mod\ 23) = 17$$

$$y_3 = -y + \lambda(x - x_3) = -4 + 21(5 - 17) = -256 (mod\ 23) = 20$$

Точка $4G = (17; 20)$. Перевіримо чи належить точка еліптичній кривій $y^2 \equiv x^3 + x + 1 (\bmod 23)$:

$$20^2 = 17^3 + 17 + 1 (mod\ 23)$$

$$400 = 4931 (mod\ 23)$$

$9 = 9(mod\ 23)$ - точка $4G = (17; 20)$ належить еліптичній кривій.

Розрахуємо значення точки $5G = 4G + G = (17; 20) + (13; 7)$:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{20 - 7}{17 - 13} = \frac{13}{4}(mod\ 23) = 9$$

$$x_3 = \lambda^2 - x_1 - x_2 = 81 - 17 - 13 = 51(mod\ 23) = 5$$

$$y_3 = -y_1 + \lambda(x_1 - x_3) = -7 + 9(13 - 5) = 65(mod\ 23) = 19$$

Точка $5G = (5; 19)$. Перевіримо чи належить точка еліптичній кривій $y^2 \equiv x^3 + x + 1 (\mathrm{mod}\, 23)$:

$$19^2 = 5^3 + 5 + 1(mod\ 23)$$

$$361 = 131(mod\ 23)$$

$16 = 16(mod\ 23)$ - точка $4G = (5; 19)$ належить еліптичній кривій.

Отже, особистий ключ *d = 5*, відкритий $Q = (5; 19)$.

Виробимо цифровий підпис при $e = H(M) = 6$:

1. Випадково генеруємо *k =2* з інтервалу *[1, n – 1]*.
2. Знаходимо $k \cdot G = 2G = (5; 4)$.
3. Виділяємо $x_1 = 5$.
4. Знаходимо $r = x_1(mod\ n) = 5(mod\ 7)$.
5. Обчислюємо значення $s = k^{-1}(e + dr)(mod\ n) = 2^{-1}(6 + 5 \cdot 5)(mod\ 7) = 5$.

Цифровий підпис має вигляд (5;5).

Задача 16. Зробіть порівняння ЕЦП згідно ДСТУ 4145- 2002 та ГОСТ Р 34.10 – 2001 по критерію захищеності від атаки повне розкриття та по аналогії: ДСТУ 4145- 2002 та ISO 15946-2 (ECDSA); ДСТУ 4145- 2002 та ISO 15946-2 (EC G DSA); ДСТУ 4145- 2002 та ISO 15946-2 (EC KC DSA).

Погроза повне розкриття (total break) характеризується тим, що крипто аналітик може обчислити особистий ключ, можливо відмінний від *d*, але відповідний *Q*. Це дозволяє криптоаналітику формувати власні підписи будь-яких повідомлень.

Практичну оцінку погрозі повного розкриття дає параметр $t_б$ – безпечний час виконання криптоаналізу, який розраховується за формулою:

$$t_б = \frac{I}{\gamma \cdot K},$$

де I – складність криптоаналізу, γ – потужність крипто аналітичної системи, $k = 3{,}15 \cdot 10^7\, с/рік$ – кількість секунд у році. У свою чергу складність криптоаналізу розраховується за формулою:

$$I = \sqrt{\frac{\pi \cdot n}{4}},$$

де n – порядок базової точки. Розрахуємо $t_б$ для ДСТУ 4145- 2002, ГОСТ Р 34.10 – 2001, ECDSA, EC G DSA та EC KC DSA при мінімально можливих значеннях порядку базової точки,згідно зі стандартами, при потужності крипто аналітичної системи $\gamma = 10^{10}$ оп/с. Результати запишемо у таблицю 6.18.16.1

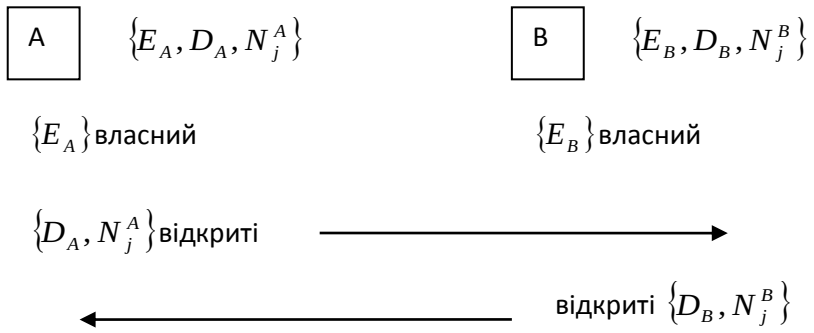
Таблиця 6.18.16.1 – Результати розрахунків

Назва алгоритму	n	$t_б$,років
ДСТУ 4145- 2002	2^{164}	10^7
ГОСТ Р 34.10 – 2001	2^{255}	$5 \cdot 10^{20}$
ECDSA	2^{161}	$4 \cdot 10^6$
EC G DSA	2^{161}	$4 \cdot 10^6$
EC KC DSA	2^{192}	$5{,}6 \cdot 10^{10}$

Згідно з отриманими результатами, можна зробити висновок, що при мінімальних значеннях порядку базової точки ДСТУ 4145- 2002 має кращу криптостійкість ніж алгоритми ECDSA та EC G DSA, але значення параметру t_6 для ДСТУ 4145- 2002 гірші ніж для EC KC DSA та ГОСТ Р 34.10 – 2001.

Але для алгоритмів EC KC DSA та ГОСТ Р 34.10 – 2001 значення максимального значення порядку базової точки обмежені(2^{256} та 2^{255} відповідно), а для алгоритмів ДСТУ 4145- 2002, ECDSA та EC G DSA існують лише межі мінімуму($n > 2^{163}, n > 2^{160}$).

Тобто ДСТУ 4145- 2002 більш захищений від погрози повного розкриття при великих значеннях порядку базової точки ніж KC DSA та ГОСТ Р 34.10 – 2001.



Задача 17. Реалізуйте протокол, що наведений на рис. використовуючи RSA криптосистему**.**

Розв’язок задачі

Протокол заключається в наступному: абонент А звертається до В з запитом виду I_A (ідентифікатор А). За допомогою D_B А шифрує деяку функцію:

$$\{I_A, CR_A, ?\,запит\ ресурсів\} \tag{7.1}$$

і передає її користувачу В. Користувач В своїм секретним ключем розшифровує це повідомлення і порівнює I_A відкрите з I_A після розшифрування. CR_A – випадкове число для контролю цілісності сеансу. В відповідає А: на відкритому ключі D_A створює криптограму:

$$\{I_A, I_B, CR_A, CR_B, K_{AB}\}, \tag{7.2}$$

де K_{AB} – ключ з’єднання, I_B – ідентифікатор В, CR_B – випадкове число, що формує та передає В. Після цього А на своєму секретному ключі E_A розшифровує криптограму від В та виділяє ключ K_{AB}. На третьому кроці передає В контрольне повідомлення

$$\{I_A, K_{AB,}(CR_B, I_B)\}. \tag{7.3}$$

В, отримавши це повідомлення, бачить, що А правильно прийняв ключ K_{AB} з'єднання і, що саме з'єднання – цілісне. Далі А та В обмінюються між собою інформацією, шифруючи її ключем K_{AB}.

Протокол виробки загального секрету:

Нехай користувачам А та В необхідно виробити загальний секрет K_{AB}. Використаємо для цього протокол Діффі-Хеллману в полі GF(P). Нехай А та В знають загальносистемні параметри $\{P, \theta_V\}$, що породжені випадковим процесом. Тоді за допомогою схеми Діффі-Хеллмана можна забезпечити слушний протокол. Протокол наведено на рис. 7.2.

Нехай А та В використовують такі параметри та ключі:

$N_A = P \cdot Q = 7 \cdot 11 = 77,\ E_A = 13,\ D_A = 37$;

$N_B = P \cdot Q = 11 \cdot 19 = 209,\ E_B = 7,\ D_A = 103$.

Переконайтесь, що ці параметри та ключі задовольняють вимоги RSA криптосистеми. Для спрощення приймемо, що абонент А передає повідомлення (2.129) $M_A = 2$, а В у відповідь $M_B = 4 = 2^2$. Тоді:

$$C_A = M_A^{D_B} (\mathrm{mod}\, N_B) = 2^{103} (\mathrm{mod}\, 209) = 41.$$

Криптограма C_A розшифровується В з використанням особистого ключа E_B:

$$M_A = C_A^{E_B} (\mathrm{mod}\, N_B) = 41^7 (\mathrm{mod}\, 209) = 2 (\mathrm{mod}\, 209).$$

Далі абонент В, використовуючи відкритий ключ D_A, зашифровує повідомлення M_B:

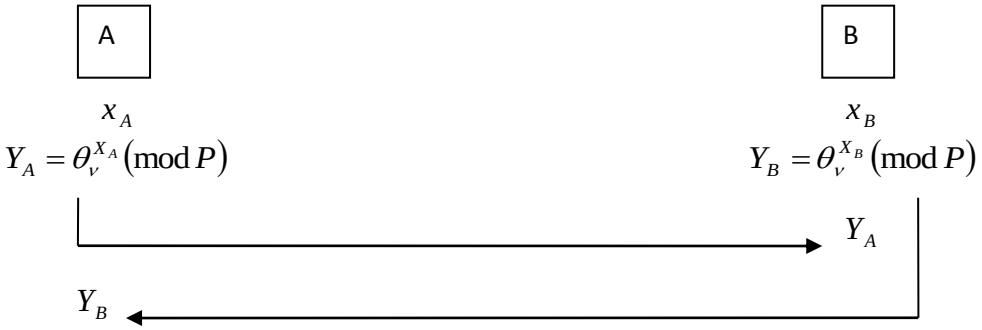
$$C_B = M_B^{D_A} (\mathrm{mod}\, N_A) = 4^{37} (\mathrm{mod}\, 77) = 2^{2 \cdot 37} (\mathrm{mod}\, 77) = 60 (\mathrm{mod}\, 77).$$

Криптограма C_B розшифровується А з використанням особистого ключа E_A:

$$M_B = C_B^{E_A} (\mathrm{mod}\, N_A) = 60^{13} (\mathrm{mod}\, 77) = 4 (\mathrm{mod}\, 77).$$

Виділивши із M_B випадкове число CR_A, абонент А установлює цілісність сеансу. Нехай $M_B = K_{AB}$ є отриманий від В сеансів ключ. Тоді на третьому кроці повідомлення (7.3), що має, наприклад, вид 11101100 10010001 11110000 10100011, зашифровується ключем CR_A.

Виділивши із отриманої криптограми своє випадкове число CR_B із (7.2) В установлює цілісне з'єднання чи ні. Крім того, при правильному розшифруванні, В установлює, що А отримав ключ K_{AB} і може його використовувати в подальшому.



$$K_{AB} = K_{BA} = Y_B^{X_A} (\mathrm{mod}\, P) = Y_A^{X_B} (\mathrm{mod}\, P) = \theta_v^{X_A X_B} (\mathrm{mod}\, P)$$

Рисунок 7.19.1.2 – Протокол Діфі-Хелмана

Пояснення до рис. 7.19.1.2: А та В генерують свої власні ключі X_A та X_B довжиною $I_{X_B} = I_{X_A}$ відповідно. Потім кожний з них розраховує свої відкриті ключі, використовуючи формули:

$Y_A = \theta_V^{X_A} (\mathrm{mod}\, P)$;

$Y_B = \theta_V^{X_B} (\mathrm{mod}\, P)$.

Розрахувавши відкриті ключі, А та В обмінюються ними по закритому автентичному каналу, тобто з забезпеченням цілісності та справжності. Далі А виробляє загальний секрет K_{AB} з використанням відкритого ключа $Y_B : K_{AB} = Y_B^{X_A} (\mathrm{mod}\, P) = \theta_V^{X_B X_A} (\mathrm{mod}\, P)$. В виробляє $K_{BA} : K_{BA} = Y_A^{X_B} (\mathrm{mod}\, P) = = \theta_V^{X_A X_B} (\mathrm{mod}\, P)$. Алгоритм гарантує, що числа K_{AB} та

K_{BA} однакові (тобто $K_{AB} = K_{BA}$) і можуть бути використані як загальний секрет для подальшого використання, наприклад, виробки з нього конфіденційного ключа.

Задача 18. В системі використовується схема вироблення загального секрету по протоколу Діффі-Геллмана. Довжина модуля P=37.

Необхідно знайти:

- знайти первісний елемент поля GF(P);
- визначити величину множини первісних елементів;
- сформувати особистий ключ та визначити відкритий ключ;
- виробити загальний секрет.

Розв'язок

Перевіримо чи буде первісним коренем 2. $\varphi(P) = 36 = 2^2 \cdot 3^2$

$2^{37-1} \equiv 1 mod 37$

$2^{\frac{37-1}{2}} \equiv -1 mod 37$

$2^{\frac{37-1}{3}} \equiv 26 mod 37$

Отже 2 можна прийняти за первісний корінь.

Кількість первісних коренів дорівнює $\varphi\big(\varphi(P)\big) = \varphi(36) = \varphi(2)^2 \cdot \varphi(3)^2 = 1 \cdot 4 = 4$

Нехай закриті ключі $E_A = 13, E_B = 7$ тоді відкриті ключі дорівнюють $D_A = 2^{13} mod 37 = 15, D_B = 2^7 mod 37 = 17.$ Загальний секрет$K = {D_A}^{E_B} mod 37 = {D_B}^{E_A} mod 37 = 35 mod 37.$

Задача 19. Розробіть повний протокол Діффі-Хеллмана виробки загального секрету, орієнтуючись на двохсторонній канал, в якому використовуються параметри $\{P_i, \theta_V\}$, а також довгострокові ключі X , Y та сеансові ключі X_S, Y_S .

Розв'язок

Повний протокол узгодження ключів Діффі-Геллмана у полі

При відомих загальносистемних параметрах (модуль перетворень P та породжуючий елемент θ_V), виробка загального секрету для A та B абонентів протокол виробки ключів на основі довгострокових та ключів сеансу. здійснюється таким чином:

A **B**

Кореспонденти A та B виробляють випадково особисті ключі:

$1 < X_A < P$ $1 < X_B < P$

Потім кожен із них обчислює відкриті ключі асиметричної пари. Відкриті ключі пересилаються між абонентами із забезпеченням їх цілісності й справжності, наприклад, через центр довіри (сертифікації ключів) або із застосуванням іншого дозволеного механізму. Далі кожен із абонентів обчислює спільну таємницю Z_{AB}та відповідно Z_{BA}:

$$Y_A = \theta_\nu^{X_A} (\mathrm{mod}\, P) \qquad Y_B = \theta_\nu^{X_B} (\mathrm{mod}\, P)$$

$$Z_{AB} = Y_B^{X_A} (\mathrm{mod}\, P) \qquad Z_{BA} = Y_A^{X_B} (\mathrm{mod}\, P)$$

Можна легко перевірити, що:

$$Z_{AB} = Z_{BA} = \theta_\nu^{X_A X_B}$$

Ключі сеансу формуються при кожному сеансі зв'язку. Спочатку формуються особисті ключі сеансу:

$1 < X_{AS} < P$ $1 < X_{BS} < P$

Потім формуються відкриті ключі сеансу у вигляді елементів скінченного поля Галуа. Відкриті ключі сеансу пересилаються перед кожним сеансом або поміщаються в першому блоці інформації, що пересилається. Далі кожен із абонентів спочатку обчислює спільну таємницю сеансу, відповідно:

$$Y_{AS} = \theta_v^{X_{AS}} (\mathrm{mod}\, P) \qquad Y_{BS} = \theta_v^{X_{BS}} (\mathrm{mod}\, P)$$

$$Z_{AS} = Y_{BS}^{X_{AS}} (\mathrm{mod}\, P) \qquad Z_{BS} = Y_{AS}^{X_{BS}} (\mathrm{mod}\, P)$$

Можна побачити, що:

$$Z_{AS} = Z_{BS} = \theta_v^{X_{BS} X_{AS}}$$

Формування ключа сеансу відбувається відповідно до правила:

$$K_s = kdf(Z_{AB} \| Z_{AS}, P_r) = kdf(Z_{BA} \| Z_{BS}, P_r)$$

Найбільшу загрозу для криптоперетворень у простих полях складають атаки типу універсальне розкриття та повне розкриття. Сутність атаки типу універсальне розкриття в знаходженні деякого математичного алгоритму, що дозволяє, в загальному випадку, обчислити X_A та X_{AS} і X_B та X_{BS}. Атака типу повне розкриття зводиться до розв'язку двох дискретних логарифмічних рівнянь, відповідно:

$$Y_A = \theta_v^{X_A} (\mathrm{mod}\, P) \qquad Y_B = \theta_v^{X_B} (\mathrm{mod}\, P)$$

$$Y_{AS} = \theta_v^{X_{AS}} (\mathrm{mod}\, P) \quad \text{або} \quad Y_{BS} = \theta_v^{X_{BS}} (\mathrm{mod}\, P)$$

Таким чином, даний протокол захищений від атак типу універсальне та повне розкриття, але для забезпечення захисту від атаки типу «по-середині» необхідне надання абонентам послуг автентичності, цілісності, а при деяких умовах і послуги неспростовності. Тобто необхідно користуватися послугами третьої довірчої сторони, наприклад з виготовлення та обслуговування сертифікатів відкритих ключів.

Задача 20. Побудуйте та доведіть слушність трьохетапного протоколу виробки сеансового ключа, використовуючи направлене RSA шифрування та RSA ЕЦП.Зробіть рекомендації щодо застосування протоколу.

Решение:

Протокол выработки сеансового ключа – это алгоритм совместного действия двух субъектов с использованием передачи данных по открытому каналу связи с целью выработки последовательности символов (ключа), которые известны только субъектам, которые исполняли протокол.

Для отправки сообщений используется направленное шифрование RSA, а для подписывания сообщений используется алгоритм электронной цифровой подписи RSA.

В условиях данной задачи можно использовать протокол Деннинга – Сакко.

Протокол состоит в следующем.

1. Абонент *A* отправляет третьей стороне сообщение, включающее имя свое имя *A* и имя *B*

$$(A, B).$$

2. Третья сторона отправляет *A* открытый ключ *B* (K_b), подписанный с помощью секретного ключа третьей стороны (*T*). Кроме того, третья сторона посылает абоненту *A* его собственный открытый ключ K_a , подписанный закрытым ключом третьей стороны

$$S_t (B, K_b), S_t (B, K_a).$$

3. Абонент *A* отправляет абоненту *B* случайный сеансовый ключ и метку времени, а *также включает в зашифрованные сообщения имена, чтобы абонент B после завершения протокола не мог выдавать себя за абонента A.*

$$E_b (S_a (A,B,K,T_a)), S_t (A,K_a), S_t (B,K_b).$$

4. В расшифровывает сообщение *A* своим закрытым ключом и проверяет подпись *A* с помощью открытого ключа *A*. Кроме того проверяется достоверность метки времени.

Задача 21. Нехай виробка загального секрету здійснюється за схемою Діфі-Хеллмана в полі GF(97) причому твірний елемент θ=5 для користувачів А та В. Необхідно виробити загальний секрет.

Розв'язок.

Нехай користувачам А та В необхідно виробити загальний секрет.

A	B
(x_a, Y_a)	(x_b, Y_b)
$1 < x_a < 97$	$1 < x_b < 97$
$x_a = 4x_b$ =12	
$Y_a = \theta^{x_a} \bmod 97$=	$Y_b = \theta^{x_b} \bmod 97$=
$= Y_a = 5^4 \bmod 97 = = Y_b = 5^{12} \bmod 97 =$	
= 625 *mod* 97 = 43.	= 244140625 *mod* 97 = 64.

Y_b ← → Y_a

$K_{AB} = Y_b{}^{x_a} \bmod 97 =$	$K_{BA} = Y_a{}^{x_b} \bmod 97 =$
$= 64^4 \bmod 97 = 96.$	$= 43^{12} \bmod 97 =$
	$= 43^6 \cdot 43^6 \bmod 97 =$
	= 484 *mod* 97 = 96.

$K_{AB} = K_{BA}$.

Таким чином користувачі А та В виробили загальний секрет, який дорівнює 96.

Задача 22. . Визначте безпечний час $t_б$ основних БСШ, що знайшли визнання, застосовувались або мають перспективи застосування (наприклад за вибором, DES, TDES, ГОСТ 28147 – 89, IDEA, FIPS 197, Rijndael, Camellia, Калина тощо), за умови здійснення атаки типу «брутальна сила». При оцінці обгрутуйте та виберіть потужність крипто аналітичної системи (наприклад в межах10^8- 10^{12} групових операцій в секунду). Визначте також інші показники якості вказаних БСШ – ентропію джерела ключів H(K) та відстань єдності l_0.

Розв'язок задачі

У криптоалгоритмі, що розглядається, довжина ключів та число ключів мають такі значення:

DES $l_k = 56$ біт $n_k = 2^{56}$

Основними показниками, за якими може бути оцінена стійкість криптоалгоритмів є такі: $t_б$(безпечний час), $N_{кл}$(кількість ключів), $H(K)$ (ентропія джерела ключів), l_0 (відстань єдності):

$N_{кл}$(D) = 2^{56} ключів.

Вважатимемо, що ключіз'являютьсярівноймовірно і незалежно, визначимо ентропію джерела ключів$H(K)$:

$$H(K) = -\sum_{i=1}^{N_k} P(K_i)\log P(K_i) = -\sum_{i=1}^{N_k} \frac{1}{N_{кл}} \log N_{кл}^{-1};$$

$H(K)$ = 56 біт.

Якщо $P(K_i) = \frac{1}{N_{кл}} = N_{кл}^{-1}$,тоді:

$$t_б^{DES} = \frac{N_{кл}^{DES}}{\gamma * K} * 1 = \frac{2^{56}}{10^9 \, операцій/с * 3*10^7} = \frac{10^{16,8}}{3*10^{16}} \approx 2,1 \text{ (роки)},$$

де γ – продуктивність криптоаналітичної системи, K – кількість секунд в році.

Таким чином, для здійснення криптоаналізу методом грубої сили необхідно ≈ 2 роки.

Знайдемо $t_б$ для випадку диференціального або лінійного криптоаналізу, для яких $N_{вар} = 2^{47}$. В результаті маємо, що:

$$t_б = \frac{2^{47}}{\gamma * K} = \frac{10^{14,1}}{3*10^{16}} = 3*10^{-3} \text{ (років)} \approx 1,2 \text{ дні}.$$

Вважатимемо, що в системі передаються повідомлення англійським текстом, надмірність якого 0,45.

Відстань єдності:

$$l_0^{DES} = \frac{H(K)}{d*\log m} = \frac{H(K)}{d*\log 2} = \frac{56}{0,45*1} = 124 \text{ (біт)}.$$

Зі значення l_0 робимо висновок, що для того, щоб успішно здійснити криптоаналіз, треба перехопити не менш ніж 124 біт символів криптограми, тоді, затративши $t_б$, ми можемо успішно вирішити задачу криптоаналізу.

Задача 23. Визначте безпечний час *tб*основних БСШ, що знайшли визнання, застосовувались або мають перспективи застосування (наприклад за вибором, (DES, TDES, ГОСТ 28147 – 89, IDEA, FIPS 197, Rijndael, Camellia, Калина тощо), за умови застосування «табличної атаки». При оцінці обгрутуйте та виберіть потужність крипто аналітичної системи (наприклад в межах10^9 - 10^{13} групових операцій в секунду)

Розв'язок

«Таблична атака» заснована на принципі формування таблиць великих розмірів з парами відкритого та шифрованого тексту за допомогою різних ключів. Для шифру AES-128 для використовуючи 2^{32} ключів складніть передобчислення складає 2^{96}, після чого ключ може бути знайдений зі складністю 2^{80} (наприклад атака на зв'язаних ключах має складність $2^{99.5}$). При 10^{13} операціях в секунду потрібно буде $\frac{2^{80}}{10^{13}} \approx 10^{11} c,$ що приблизно 4000 років. Отже при табличній атаці на AES-128 при 10^{13} операціях в секунду $t_б \approx 4000\, років$.

Отже $O = 3584^{\frac{1}{4}} \approx 7{,}74$.

ЗАДАЧА 24. Порівняйте по критерію мінімума безпечного часу $тб_{min}$ криптографічну стійкість БСШ проти атак типу: «брутальна сила», «табличної атаки» та атаки «зі словником» (наприклад за вибором чи згідно вказівки викладача, DES, TDES, ГОСТ 28147 – 89, IDEA, FIPS 197, Rijndael, Camellia, Калина тощо) . При оцінці обгрутуйте та виберіть потужність крипто аналітичної системи (наприклад в межах10^8 - 10^{13} групових операцій в секунду).

Розв’язок задачі

Для порівняння були обрані шифри DES та Rijndael.

Для порівняння по критерію мінімума безпечного часу необхідно взяти найкращі показники потужності крипто аналітичної системи та найменші довжини блока/ключа шифрування.

Таким чином, для DES довжина ключа l_k = 56 біт, а довжина блока l_b = 64 біт. А для Rijndael довжина ключа l_k = 192 біт, а довжина блока l_b = 128 біт.

Для обчислення безпечного часу використовуємо формулу

$$t_b = \frac{N}{\gamma k} P_k$$

обравши при цьому потужність крипто аналітичної системи γ = 10^{13} групових операцій в секунду.

Для атаки повного перебору необхідно перебрати усі можливі варіанти ключа, об’єм яких складає 2^k.

Для табличної атаки необхідна таблиця 2^n блоків, для побудови якої необхідно 2^n шифрувань, де n — бітова довжина блоку.

Складність атаки зі словнико також визначається довжиною блока, але ще й режимом роботи алгоритму.

Таким чином можна зробити порівняльну таблицю складності атак на БСШ.

Таблиця 8.1 — складніть атак

Назва методу	DES	Rijndael
Перебір ключів	7 годин	$2*10^{37}$ років
Атака зі словником	3,5 місяці (в режимі простої заміни)	10^{18} років (в режимі простої заміни)
Таблична атака	3,5 місяці	10^{18} років

Задача 25. Лінійний криптоаналізуважається одним з найбільш ефективних для сучасних блокових симетричних шифрів. Критерій стійкості *r*-циклового SPN-шифру до лінійного криптоаналізу може бути представлений у вигляді наступної нерівності:

$$P_{ЛХ}(r) \leq 2^{-\frac{n}{2}},$$

де *r* – число циклів шифру, *n* – розмір блоку в бітах, $P_{ЛХ}^{(r-1)}$ – верхня границя ймовірності *r*-циклової лінійної характеристики.

Для обчислення верхньої границі ймовірності лінійної характеристики максимальну ймовірність лінійної апроксимації окремої підстановки підносять до степеня числа активних підстановок, тобто:

$$P_{ЛХ}(r) = \left(P_{L_{max}}\right)^{a(r)},$$

де *a*(*r*) – мінімальна кількість активних підстановок в *r*-циклах шифру.

Отримайте верхні границі ймовірності для багатоциклових лінійних характеристик для спрощеного шифру $P_{L_{max}} = 2^{-2}$, обґрунтувавши *a*(*r*).

Зробіть висновок про стійкість до лінійного криптоаналізу шифру «Калина» з 128-бітним блоком, що містить 7 і більше циклів; шифру «Калина» з 256-бітним блоком, що містить 9 і більше циклів; і шифру «Калина» з 512-бітним блоком, що містить 9 і більше циклів.

Розв’язання задачі

Обчислимо критерій стійкості до лінійного крипто аналізу та знаходимо мінімальну кількість активних підстановок для різної довжини блоку шифру «Калина».

Для шифру «Калина» з 128-бітним блоком, що містить від 7 циклів:

$$P_{ЛХ}(7) \leq 2^{-\frac{128}{2}} = 5{,}42 \cdot 10^{-20};$$

$$a(r) = \log_{P_{L_{max}}} P_{ЛХ}(7) = 32.$$

Для шифру «Калина» з 256-бітним блоком, що містить від 9 циклів:

$$P_{ЛХ}(9) \leq 2^{-\frac{256}{2}} = 2{,}94 \cdot 10^{-39};$$

$$a(r) = \log_{P_{L_{max}}} P_{\text{ЛХ}}(9) = 64.$$

Для шифру «Калина» з 128-бітним блоком, що містить від 7 циклів:

$$P_{\text{ЛХ}}(9) \leq 2^{-\frac{512}{2}} = 8{,}64 \cdot 10^{-78};$$

$$a(r) = \log_{P_{L_{max}}} P_{\text{ЛХ}}(7) = 128.$$

Отже, чим більша довжина блоку, тим вища стійкість до лінійного крипто аналізу і більша кількість мінімальних підстановок.

Задача 26. Факторизувати модуль N RSA перетворення методом ρ - Полларда, для значень модуля, що наведені в таблиці 7.9.8..1.1

Таблиця 7.9.8..1.1 – Значення модуля RSA перетворення

i	1	2	3	4	5	6	7	8	9	10	11
Ni	377	221	299	209	247	323	403	351	391	161	437

Розв'язок задачі

Дано, що $N = 221$, $a = 11$, $x_0 = 127$, $C = 1$.

$x_1 = (127 \cdot 11 + 1)(\mathrm{mod} 2^8)$;

$x_1 = 118$;

НСД(127-118, 221) = (9, 221)=1, тобто спільних дільників немає.

$x_2 = (118 \cdot 11 + 1)(\mathrm{mod} 2^8)$;

$x_2 = 19$;

НСД (118-19,221) = НСД (99,221) = 1.

Таким чином НСД ($x_1 - x_2$, N) знову не має сильного дільника.

$x_3 = (19 \cdot 11 + 1)(\mathrm{mod} 2^8)$.

Розрахуємо послідовно x_i поки, НСД ($x_1 - x_2$, N) різнитиметься від 1 або N.

$x_3 = 210$; НСД (191,221) = 1;

$x_4 = (210 \cdot 11 + 1)(\mathrm{mod} 2^8)$;

$x_4 = 7$; НСД (203 , 221) =1;

$x_5 = (7 \cdot 11 + 1)(\mathrm{mod} 2^8)$;

$x_5 = 78$; НСД (71,221) = 1;

$x_6 = (78 \cdot 11 + 1)(\mathrm{mod} 2^8)$;

$x_6 = 91$.

При x_6 маємо НСД ($x_6 - x_5$, N) = НСД (91 – 78, 221) = НСД (13, 221) = 13.

Таким чином один із співмножників модуля N є 13, наприклад, P=13. Тоді $Q=N/P$=221/13=17.

Задача 27. Нехай відомо, що в RSA системі використовується відкритий ключ Dk = 103, а модуль перетворення N = 209. Необхідно знайти особистий (секретний) ключ Ek та оцінити складність криптоаналізу для $N = 2^{1024+k\,256}$, k – номер реєстрації.

Факторизацію виконуємо, використовуючи метод двійкового решета.Спочатку визначаємо базу розкладу – прості невеликі числа $p_1, p_2, \ldots p_r$, добуток яких P є близьким до N= 209.

P =2·3·5·7=210, N≈P.

Знаходимо ⌊√N⌋=⌊√209⌋=14. Будуємо таблицю розрахунків. Шукаємо строку, що задовольняє умові:

$$X^2 \equiv Y^2 mod N. \ (1)$$

Таблиця 7.9.8.3.1 – Розрахунки

N/p	*X*	$Z = \lfloor x + \sqrt{N} \rfloor$	$Z^2 mod\ N$	2	3	5	7	Залишок
1	1	15	16	4	-	-	-	+
2	2	16	47	-	-	-	-	-47
3	3	17	80	4		1	-	+
4	4	18	115	-	-	1	-	-23
5	5	19	152	3	-	-	-	-

Можна не продовжувати таблицю, бо строка, що задовільняєумові (1) знайдена:

$$15^2 \equiv 2^4 (\text{mod } 209) \text{ ->x} = 15, \text{y} = 4.$$

НСД(15-4, 209) = 11. Тепер можемо знайти розклад числа N:

P=11;

$Q=N/P$=209/11=19.

Ми факторизували модуль N = 209=11·19.

Знайдемоособистий ключ $E_к$. Спочатку визначимофункцію Ойлера від модуля N:

$$\varphi(N) = \varphi(P) \cdot \varphi(Q) = (P-1)(Q-1); \ (2)$$

$$\varphi(N) = 180.$$

Визначимо ключову пару $E_к$, $D_к$з наступного рівняння:

$$E_к D_к \equiv 1 \; mod\varphi(N); \; (3)$$

$$103 \cdot E_k \equiv 1 \; (mod \; 180).$$

За алгоритмом ланцюгових дробів визначимо $E_к$, $D_к$:

$$180x + 103y = 1;$$

$$\frac{180}{103} = 1 + \frac{77}{103}; \frac{103}{77} = 1 + \frac{26}{77};$$

$$\frac{77}{26} = 2 + \frac{25}{26}; \frac{26}{25} = 1 + \frac{1}{25}; \frac{25}{1} = 25 + 0;$$

Цілі частини $r_0 = 1$, $r_1 = 1$, $r_2 = 2$, $r_3 = 1$, $r_4 = 25$.Побудуємо таблицю для виконання обчислень $E_к$:

Таблиця 7.9.8.3.2 - Розрахунки

i	-1	0	1	2	3	4
r	-	1	1	2	1	25
A	1	1	2	5	7	180

$$E_j = (-1)^i \cdot A_{i-1} \; ; \; (4)$$

$$E_j = 7 \; mod \; \varphi(N).$$

Виконаємо перевірку отриманого результату за формулою (3):

$$103 \cdot 7 \; (mod \; 180) = 721 \; (mod \; 180) = 1 \; (mod \; 180).$$

Оцінимо складність криптоаналізу для $N=2^{(1024+k\cdot 256)}$, де K– номер за журналом (у нашому випадку 3).

Завдання факторизації великого цілого числа N на множники належить до класу субекспоненціальних алгоритмів, складність яких становить:

$$L_N(\alpha, \beta) = \exp(\beta(lnN)^\alpha \cdot (lnlnN)^{1-\alpha}), \; (5)$$

Де α, β– параметри метода. Відомо, що для квадратичного решета числового поля параметриα, βвідповідно дорівнюють 1/3 та $\sqrt[3]{64/9} \approx 1{,}92$.

$$L_N(1/3; 1{,}92) = \exp\left(1{,}92(ln2^{1792})^{\frac{1}{3}} \cdot (lnln2^{1792})^{1-\frac{1}{3}}\right) = \exp(1.92 \cdot 10.74 \cdot 3.7) = \exp(76.29) \approx 1.366 \cdot 10^{33}$$

Задача 28. Розв'язати задачу дискретного логарифмування для порівняння $15^x \equiv n \pmod{23}$ методом ρ - Полларда, с =6. Перевірте правильність розв'язку порівняння. Причому n = (k+17)mod 23, де k-номер реєстрації. Якщо n=0, то n=21.

Розв'язання

В загальному вигляді для розв'язку порівняння $a^x \equiv b(\mathrm{modP})$методом ρ-Поллардапотрібно знайти такі дві пари чисел (U_i, V_i)та (U_j, V_j), що задовільняють умові:

$$a^{U_i} \cdot b^{V_i} \equiv a^{U_j} \cdot b^{V_j}(\mathrm{modP}).$$

За допомогою певних математичних перетворень отримуємо кінцеву формулу:

$$X = \frac{U_j - U_i}{V_i - V_j}\mathrm{mod}(\mathrm{P}-1) = (U_j - U_i)\cdot(V_i - V_j)^{-1}\mathrm{mod}(\mathrm{P}-1).$$

Формувати випадкову пару чисел (U_i, V_i) будемо за правилом:

$$r_i = \begin{cases} r_{i-1}\cdot b(\mathrm{modP}), & r_{i-1} \le C; \\ r_{i-1}\cdot a(\mathrm{modP}), & r_{i-1} > C. \end{cases}$$

Постійну С вибирають таким чином, щоб вона перебувала між *a* та *b* приблизно на однаковій відстані. Але в більшості випадків її підбирають.

Послідовність r_i називають послідовністю ρ-Полларда. Для успішного розв'язання дискретного логарифмічного рівняння необхідно знайти два значення r_i та r_j $(i \neq j)$ – таких, що$r_i = r_j$. Після цього знаходяться пари (U_i, V_i)та (U_j, V_j) та обчислюється особистий ключ X.

k=5; n=(5+17)mod23=22;

$15^x \equiv 22(\mathrm{mod}23)$.

Обчислимо значенняr_i з урахуванням того, що a=15, b=22, P=23за формулами:

$$r_i = \begin{cases} r_{i-1}\cdot b(\mathrm{modP}), & r_{i-1} \le C; \\ r_{i-1}\cdot a(\mathrm{modP}), & r_{i-1} > C. \end{cases}$$

За умовою задачі С=6. Розрахуємо значення r_i:

$r_0 = b^1 \cdot a^0(\mathrm{modP}) = 22^1 \cdot 15^0(\mathrm{mod}23) = 22$;

$r_1 = r_0 \cdot a(\mathrm{modP}) = 22 \cdot 15(\mathrm{mod}23) = 8$;

$r_1 = b^1 \cdot a^1 = 22^1 \cdot 15^1$;

$r_2 = r_1 \cdot a(\mathrm{modP}) = 8 \cdot 15(\mathrm{mod}23) = 5$;

$r_2 = b^1 \cdot a^2 = 22^1 \cdot 15^2$;

$r_3 = r_2 \cdot b(\mathrm{modP}) = 5 \cdot 22(\mathrm{mod}23) = 18$;

$r_3 = b^2 \cdot a^2 = 22^2 \cdot 15^2$;

$r_4 = r_3 \cdot a(\mathrm{modP}) = 18 \cdot 15(\mathrm{mod}23) = 17$;

$r_4 = b^2 \cdot a^3 = 22^2 \cdot 15^3$;

$r_5 = r_4 \cdot a(\mathrm{modP}) = 17 \cdot 15(\mathrm{mod}23) = 2$;

$r_5 = b^2 \cdot a^4 = 22^2 \cdot 15^4$;

$r_6 = r_5 \cdot b(\mathrm{modP}) = 2 \cdot 22(\mathrm{mod}23) = 21$;

$r_6 = b^3 \cdot a^4 = 22^3 \cdot 15^4$;

$r_7 = r_6 \cdot a(\mathrm{modP}) = 21 \cdot 15(\mathrm{mod}23) = 16$;

$r_7 = b^3 \cdot a^5 = 22^3 \cdot 15^5$;

$r_8 = r_7 \cdot a(\text{mod}P) = 16 \cdot 15(\text{mod}23) = 10;$

$r_8 = b^3 \cdot a^6 = 22^3 \cdot 15^6;$

$r_9 = r_8 \cdot a(\text{mod}P) = 10 \cdot 15(\text{mod}23) = 12;$

$r_9 = b^3 \cdot a^7 = 22^3 \cdot 15^7;$

$r_{10} = r_9 \cdot a(\text{mod}P) = 12 \cdot 15(\text{mod}23) = 19;$

$r_{10} = b^3 \cdot a^8 = 22^3 \cdot 15^8;$

$r_{11} = r_{10} \cdot a(\text{mod}P) = 19 \cdot 15(\text{mod}23) = 9;$

$r_{11} = b^3 \cdot a^9 = 22^3 \cdot 15^9;$

$r_{12} = r_{11} \cdot a(\text{mod}P) = 9 \cdot 15(\text{mod}23) = 20;$

$r_{12} = b^3 \cdot a^{10} = 22^3 \cdot 15^{10};$

$r_{13} = r_{12} \cdot a(\text{mod}P) = 20 \cdot 15(\text{mod}23) = 1;$

$r_{13} = b^3 \cdot a^{11} = 22^3 \cdot 15^{11};$

$r_{14} = r_{13} \cdot b(\text{mod}P) = 1 \cdot 22(\text{mod}23) = 22;$

$r_{14} = b^4 \cdot a^{11} = 22^4 \cdot 15^{11};$

Таким чином, $r_0 = r_{14}$. Звідси знаходимо:

$U_i = 0; \quad V_i = 1.$

$U_j = 11; \quad V_j = 4.$

Обчислюємо секретний ключ за формулою:

$X = (U_j - U_i) \cdot (V_i - V_j)^{-1} \text{mod}(P-1) = (11-0) \cdot (1-4)^{-1} \text{mod}22 = 11 \cdot 19^{-1} \text{mod}22.$

Знайдемо зворотній елемент *у*для числа 19 у кільці за модулем 22.

Маємо порівняння:

$19^{-1} \cdot y \equiv 1(\text{mod}22).$

Використовуючи алгоритм Евкліда маємо:

0) $\frac{22}{19} = 1 + \frac{3}{19};$

1) $\frac{19}{3} = 6 + \frac{1}{3};$

2) $\frac{3}{1} = 3 + 0.$

Отже, $\mu = 2$.Обчислюємо коефіцієнти:

$a_0 = r_0 = 1,$

$a_1 = r_0 \cdot r_1 + 1 = 1 \cdot 6 + 1 = 7.$

Для обчислення *у*маємо формулу:

$y = (-1)^{\mu} \cdot a_{\mu-1} = (-1)^2 \cdot a_1 = 7(\text{mod}22).$

За отриманими результатами обчислюємо X:

$X = 11 \cdot 19^{-1} \text{mod}22 = 11 \cdot 7(\text{mod}22) = 11.$

Таким чином, $15^{11} \equiv 22(\text{mod}23)$. Прямим обчисленням переконуємось у правильності розв’язку.

Відповідь: X=11.

Задача 29. Відомо, що відкритий ключ користувача $Q=(17,20)$, $G=(13,7)$ - базова точка, що належить еліптичній кривій $y^2=x^3+x+1(\text{mod}\,23)$. Порядок точки $n=7$, порядок ЕК $u=n\cdot k=4\cdot 7=28$, де $k-$ кофактор. Необхідно знайти відкритий ключ d із порівняння

$$Q=dG(\text{mod}\,p), d\in[1,n-1],$$

тобто в нашому випадку порівняння

$$(17,20)=d\cdot(13,7)(\text{mod}\,p), d\in[1,6].$$

Решение:

Составляем промежутки:

$$f(Z_{i+1})=\begin{cases}2Z_i, 0<|Z_i|\le\left\lceil p/3\right\rceil;\\ Z_i+G, \left\lceil p/3\right\rceil<|Z_i|\le\left\lceil 2p/3\right\rceil;\\ Z_i+Q, \left\lceil 2p/3\right\rceil<|Z_i|\le p-1.\end{cases}$$

$$\left\lceil p/3\right\rceil=7; S_1\in[1,7],$$

$$\left\lceil 2p/3\right\rceil=15; S_2\in[8,15],$$

$$p=23; S_3\in[6,22].$$

Выберем $Z_0=G,\ |Z_0|_X=13$ **принадлежит** S_2**, поэтому**

$$Z_1=Z_0+G=(13,7)+(13,7)=2\cdot(13,7)=(x_3,y_3).$$

$$\lambda=\frac{3\cdot x_1^2+a}{2\cdot y_1}(\text{mod}\,p)=\frac{3\cdot 13^2+1}{2\cdot 7}(\text{mod}\,23)=\frac{24}{7}(\text{mod}\,23)=\frac{1}{7}(\text{mod}\,23)$$

$$\lambda=10;$$

$$x_3=\lambda^2-x_1-x_2(\text{mod}\,P)=100-2\cdot 13(\text{mod}\,23)=74(\text{mod}\,23)=5;$$

$$y_3=\lambda(x_1-x_3)-y_1(\text{mod}\,P)=10\cdot(13-5)-7(\text{mod}\,23)=73(\text{mod}\,23)=4;$$

Получили $Z_1=Z_0+G=2\cdot(13,7)=(5,4).$

$Z_1\in S_1$. **Найдём** $2\cdot Z_1=2\cdot(5,4).$

$$\lambda = \frac{3 \cdot x_1^2 + a}{2 \cdot y_1} (\text{mod}\, p) = \frac{3 \cdot 5^2 + 1}{2 \cdot 4} (\text{mod}\, 23) = \frac{19}{2} (\text{mod}\, 23).$$

$$\lambda = 21;$$
$$x_3 = \lambda^2 - x_1 - x_2 (\text{mod}\, p) = 21^2 - 10 (\text{mod}\, 23) = 17;$$
$$y_3 = \lambda (x_1 - x_3) - y_1 (\text{mod}\, p) = 21 \cdot (5 - 17) - 4 (\text{mod}\, 23) = 20.$$

$$Z_3 = Z_2 + Q = (17,20) + (17,20) = 2 \cdot (17,20).$$

Находим $2 \cdot Z_2 = 2 \cdot (17,20)$

$$\lambda = \frac{3 \cdot x_1^2 + a}{2 \cdot y_1} (\text{mod}\, p) = \frac{3 \cdot 17^2 + 1}{2 \cdot 20} (\text{mod}\, 23) = \frac{217}{10} (\text{mod}\, 23) = 1;$$

$$x_3 = \lambda^2 - 2x_1 (\text{mod}\, p) = 1^2 - 34 (\text{mod}\, 23) = -33 (\text{mod}\, 23) = 13;$$

$$y_3 = \lambda (x_1 - x_3) - y_1 (\text{mod}\, p) = 1 \cdot (17 - 13) - 20 (\text{mod}\, 23) = -16 (\text{mod}\, 23) = 7.$$

Z_i	a_i	b_i	
$Z_0 = (13,7)$	**1**	**0**	$+G$
$Z_1 = (5,4)$	**2**	**0**	$x \cdot 2$
$Z_2 = (17,20)$	**3**	**0**	$+Q$
$Z_3 = (13,7)$	**4**	**1**	

$$Z_3 = Z_0 (\text{mod}\, p);$$
$$a_3 = 4; b_3 = 1; \quad i = 0; \quad j = 3;$$
$$a_0 = 1; b_0 = 0.$$

Находим

$$d = \frac{a_i - a_j}{b_j - b_i} (\text{mod}\, n) = \frac{1 - 4}{1 - 0} (\text{mod}\, 7) = -3 (\text{mod}\, 7) = 4.$$

Проверим

$$Q' = dG = 4 \cdot (13,7).$$
$$2 \cdot (13,7) = (5,4);$$
$$2 \cdot (5,4) = (17,20).$$

Получили
$$Q' = Q;$$
$$(17,20) = (17,20).$$

Задача 30. Крипто аналітиком перехоплено криптограму C_i і відомо що вона зашифрована з використанням RSAалгоритму. Розшифруйте криптограму, використовуючи дані, що наведені в таблиці 3.20.

Таблиця 7.3.11.5.1 – Параметри та ключі до задачі 7.3.11.5

C_i	3	4	5	6	7	8	9	10	9	12
P_n	3	11	11	11	23	7	29	17	19	19
Q_n	11	17	23	13	17	23	7	7	7	11
E_j/D_j	-/7	-/11	-/3	-/5	-/3	7/-	11/-	13/-	5/-	3/-

Розв'язання

C_i=7;P= 23;Q= 17;D_j= 3.

У RSA системі формули зашифрування та розшифрування мають вид:

$$C_i = M_i^{E_j} (\text{mod} N),$$

$$M_i = C_i^{D_j} (\text{mod} N),$$

де M_i – блок повідомлення; C_i – блок криптограма;E_j– відкритий ключ прямого перетворення; D_j – ключ зворотного перетворення; N – модуль перетворень.

Обчислимо ключову пару (E_j, D_j) методом ланцюгових дробів.

Модуль перетворення обчислюється за формулою:

$$N=P\cdot Q=23\cdot 17=391,$$

де P,Q– прості числа.

Розрахуємо значення функції Ойлера за формулою:

$$\varphi(N)=\varphi(P\cdot Q)= \varphi(P)\cdot\varphi(Q)=(P-1)\cdot(Q-1)=22\cdot 16=352;$$

$$(\varphi(N),D_j)=(352,3)=1.$$

Ключова пара (E_j, D_j) пов'язана між собою порівнянням:

$$E_j \cdot D_j \equiv 1(\text{mod}\varphi(N)).$$

Для знаходження E_j ключа запишемо це порівняння у вигляді Діафантового рівняння:

$$\varphi(N)\cdot x + D_j \cdot y = 1.$$

Підставивши відповідні значення маємо:

$$352\cdot x + 3\cdot y = 1$$

Подамоа/by вигляді ланцюгового дробу:

$$\frac{a}{b} = \frac{\varphi(N)}{D_j} = \frac{352}{3}.$$

0) $\frac{352}{3} = 117\cdot 3 + \frac{1}{3}$;

1) $\frac{3}{1} = 3 + 0$;

Це означає, щоμ=1.

Тоді значення y=E_jможна знайти з виразу:

$$y = (-1)^{\mu}\cdot a_{\mu-1} = -a_0.$$

Коефіцієнт $a_0 = r_0 = 117.$

$$y = E_j = -a_0(\text{mod}\varphi(N)) = -117(\text{mod}352) = 235.$$

Зробимо перевірку, підставивши значення E_j та D_j в основне порівняння:

$$235 \cdot 3 \equiv 1(\text{mod}352).$$

Ліва та права частини порівнюються, тому $(E_j, D_j) = (235,3)$ є ключовою парою RSA-перетворень.

Використовуючи формулу для розшифрування знайдемо M_i:

$$M_i = {C_i}^{D_j}(\text{modN}) = 7^3(\text{mod}391) = 343.$$

Зробимо перевірку використовуючи знайдений відкритий ключ E_j :

$$C_i = {M_i}^{E_j}(\text{modN}) = 343^{235}(\text{mod}391) = 7.$$

Значення криптограми співпадає з початковим значення, отже повідомлення розшифровано вірно.

Відповідь: $M_i = 343$.

Задача 31. Розрахуйте складність криптоаналізу дискретного логарифму в групі точок еліптичної кривої, якщо $n = 2^{192}$, 2^{224}, 2^{256} та 2^{512}.

Розв’язок задачі

Успішне розв’язання задачі дискретного логарифму в групі точок еліптичної кривої вимагає

$$I = \sqrt{\frac{\pi n}{2}}$$

операцій на еліптичній кривій. Але є можливість розпаралелити процес і тоді буде необхідно

$$I = \sqrt{\frac{\pi n}{4}}$$

операцій на еліптичній кривій.

Отже, наприклад, для $n = 2^{192}$ складність буде дорівнювати

$$I = \sqrt{\frac{3.14 \cdot 2^{192}}{4}} = \sqrt{3.14 \cdot 2^{190}} \approx 7 \cdot 10^{28} \text{ операцій}$$

Таким самим чином розрахуємо складність криптоаналізу і для усіх інших n:

Таблиця 7.6.18.4.1 — складність криптоаналізу дискретного логарифма на ЕК

n	2^{192}	2^{224}	2^{256}	2^{512}
I	$7*10^{28}$	$4*10^{33}$	$6*10^{38}$	$2*10^{77}$

Задача 32. Зробіть порівняльний аналіз стійкості направленого RSA шифрування та Ель-Гамаля направленого шифрування в групі точок еліптичних кривих, якщо довжина модуля N=2^{2048}, а порядок базової точки n=2^{256}.

Нехай криптоаналіз RSA-алгоритму базується на факторизації модуля N. Нехай факторизація здійснюється за допомогою загального решета числового поля. Тоді складність факторизації RSA-алгоритму можна оцінити за формулою:

$$I_N = \exp(1.96 * (\ln N)^{\frac{1}{3}} (\ln \ln N)^{\frac{2}{3}})$$

(3.1)

Складність розв'язку дискретного логарифмічного рівняння в группі точок еліптичних кривих при використанні методу ρ-Поларда можна оцінити за формулою:

$$I_\rho = \sqrt{\frac{\pi * n}{4}}$$

(3.2)

Використовуючи наведені вище формули, знайдемо оцінку складності:

$I_N = \exp(1{,}96 * 11{,}24 * 3{,}75) = \exp(82{,}58) \approx 7{,}29 * 10^{35}$групових операцій

$I_\rho = \sqrt{\frac{\pi * 2^{256}}{4}} \approx 1{,}77 * 2^{127} \approx 3{,}01 * 10^{38}$ операцій складання на ЕК

Задача 33. Визначте умови та сформулюйте пропозиції із реалізації в системі КЗІ загрози типу селективна підробка ЕЦП. Обґрунтуйте та сформулюйте пропозиції із захисту загроз типу селективна підробка.

Розв'язок задачі

Сутність такої підробки полягає в тому, що при невідомому особистому ключі *d* для заздалегідь обраних даних (повідомлень) m необхідно сформувати підпис (*r*,*s*), щоб перевірка на цілісність і справжність підписаних даних дала позитивний результат.

Розглянемо умови підробки підпису для ECDSA.

1) Формуємо чи вибираємо ключ сеансу $k_x \in (1,\dots, n\text{-}1)$.

2) Обчислюємо відкритий ключ сеансу $r_x = \pi(k_x * G)$.

3) Вибираємо чи підбираємо підпис повідомлення M_x, $s_x \in \{1, \dots, n\text{-}1\}$, але за умови, що $s_x = (k_x)^{-1}(dr_x+e') \bmod n$.

4) Посилаємо чи записуємо в базу даних хибне повідомлення M_x з підписом (r_x,s_x).

5) Одержувач при прийомі перевіряє цілісність і справжність повідомлення $(m_x, (r_x, s_x))$. Для цього він виконує такі кроки:

1. Обчислює значення геш-функції від повідомлення: $e' = h(m_x)$

2. Обчислює значення параметрів $w = (s_x)^{-1} \pmod n$, $u_1=e'w \pmod n$ та $u_2=r_xw \pmod n$.

3. Визначає точку еліптичної кривої $(x,y) = u_1G+u_2Q$.

4. Перетворює точку еліптичної кривої $v = \pi(x,y)$

5. Порівнює $r_x = v$

Перевірка на 5-му кроці буде виконана тільки в тому випадку, якщо $s_x=(k_x)^{-1}(dr_x+e') \pmod n$. Аналіз цього виразу показує, що ймовірність правильного вибору s_x у ході підробки однозначно визначається ймовірністю підбору чи вгадування ключа *d* і складає досить малу величину, порядку 2^{-Ld}, де L_d — довжина особистого ключа.

Отже, для захисту від атаки типу «селективна підробка» достатньо встановити досить великий розмір особистого ключа, щоб практично не можливо було реалізувати перебір ключів.

ЗАДАЧА 34. Лінійний криптоаналізуважається одним з найбільш ефективних для сучасних блокових симетричних шифрів. Критерій стійкості *r*-циклового SPN-шифру до лінійного криптоаналізу може бути представлений у вигляді наступної нерівності:

$$P_{ЛХ}(r) \leq 2^{-\frac{n}{2}},$$

де *r* – число циклів шифру, *n* – розмір блоку в бітах, $P_{ЛХ}^{(r-1)}$ – верхня границя ймовірності *r*-циклової лінійної характеристики.

Для обчислення верхньої границі ймовірності лінійної характеристики максимальну ймовірність лінійної апроксимації окремої підстановки підносять до степеня числа активних підстановок, тобто:

$$P_{ЛХ}(r) = \left(P_{L_{max}}\right)^{a(r)},$$

де *a*(*r*) – мінімальна кількість активних підстановок в *r*-циклах шифру.

Отримайте верхні границі ймовірності для багатоциклових лінійних характеристик для спрощеного шифру $P_{L_{max}} = 2^{-2}$, обґрунтувавши *a*(*r*).

Зробіть висновок про стійкість до лінійного криптоаналізу шифру «Калина» з 128-бітним блоком, що містить 7 і більше циклів; шифру «Калина» з 256-бітним блоком, що містить 9 і більше циклів; і шифру «Калина» з 512-бітним блоком, що містить 9 і більше циклів.

Розв’язання задачі

Обчислимо критерій стійкості до лінійного крипто аналізу та знаходимо мінімальну кількість активних підстановок для різної довжини блоку шифру «Калина».

Для шифру «Калина» з 128-бітним блоком, що містить від 7 циклів:

$$P_{ЛХ}(7) \leq 2^{-\frac{128}{2}} = 5{,}42 \cdot 10^{-20};$$

$$a(r) = \log_{P_{L_{max}}} P_{ЛХ}(7) = 32.$$

Для шифру «Калина» з 256-бітним блоком, що містить від 9 циклів:

$$P_{ЛХ}(9) \leq 2^{-\frac{256}{2}} = 2{,}94 \cdot 10^{-39};$$

$$a(r) = \log_{P_{L_{max}}} P_{\text{ЛХ}}(9) = 64.$$

Для шифру «Калина» з 128-бітним блоком, що містить від 7 циклів:

$$P_{\text{ЛХ}}(9) \leq 2^{-\frac{512}{2}} = 8{,}64 \cdot 10^{-78};$$

$$a(r) = \log_{P_{L_{max}}} P_{\text{ЛХ}}(7) = 128.$$

Отже, чим більша довжина блоку, тим вища стійкість до лінійного крипто аналізу і більша кількість мінімальних підстановок.