ПРОГРЕСИВНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

ПРОГРЕССИВНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

PROGRESSIVE INFORMATION TECHNOLOGIES

УДК 004.056.55

Гальченко А. В.[1], Козіна Г. Л.[2]

[1]Ст. гр. РТ – 710М, магістр кафедри Захисту інформації Запорізького національного технічного університету, Запоріжжя, Україна

[2]Канд. фіз.-мат. наук, доцент кафедри Захисту інформації Запорізького національного технічного університету, Запоріжжя, Україна

МОДИФІКАЦІЯ АЛГОРИТМУ ЗАПЕРЕЧУВАНОГО ШИФРУВАННЯ МЕНГА

В статті обговорюється проблема стійкості сучасних криптографічних систем до атак на основі примушування стосовно абонентів криптографічних систем. У зв'язку зі стрімким розвитком галузі інформаційних технологій ця проблема є актуальною в сфері інформаційної безпеки. Для вирішення проблеми стійкості сучасних криптографічних систем авторами запропоновано використання алгоритмів заперечуваного шифрування, які гарантують, що зловмисник не має змоги отримати будь-яку цінну інформацію від абонентів. Вирішення проблеми полягає у використанні алгоритму заперечуваного шифрування Менга, який гарантує захист не лише інформації, а й самих учасників обміну.

Основна мета статті полягає у виконанні модифікації первісного алгоритму заперечуваного шифрування Менга [1] шляхом використання протоколу «непомітної» передачі OT_n^1, використання якого запропоновано Моні Наором [2]. Застосування протоколу «непомітної» передачі OT_n^1 дозволяє суттєво скоротити час, необхідний для виконання алгоритму заперечуваного шифрування Менга, та спрощує його реалізацію для вирішення прикладних завдань в сфері інформаційної безпеки.

За результатами експериментів авторами статті було підтверджено, що використання протоколу «непомітної» передачі OT_n^1 є ефективним вирішенням проблеми генерації і розподілу ключів в алгоритмі заперечуваного шифрування Менга.

Ключові слова: протокол, заперечуване шифрування, неоднозначність, розподіл ключів, фіктивне повідомлення, зловмисник, розширена схема Рабіна, непомітна передача, факторизація, дискретне логарифмування.

НОМЕНКЛАТУРА

AMD – марка виробника центральних процесорів;

BCP – протокол шифрування розроблений E. Bresson, D. Catalano і D. Pointcheval;

RD – PKE – Receiver – Deniable Public Key Encryption Protocol;

RSA – протокол шифрування розроблений Rivest, Shamir і Adleman;

Гб – одиниця вимірювання об'єму пам'яті;

ГГц – одиниця вимірювання частоти (10^{-9} секунди);

КЗІ – криптографічний захист інформації;

мс – одиниця вимірювання часу ($0,001$ секунди);

ОЗУ – оперативний запам'ятовуючий пристрій (внутрішня пам'ять);

ОС – операційна система;

ПЗ – програмне забезпечення;

ЦП – центральний процесор.

$\left(A_1, A_2\right)$ – пара числових значень A_1 і A_2;

a – секретний ключ відправника;

α – елемент мультиплікативної групи;

$C\left(r_2, m\right)$ – контрольна функція від числових значень r_2 і m;

D – проміжне числове значення;

$\left\langle\left(\partial, \wp\right), B\right\rangle$ – криптограма в алгоритмі заперечуваного шифрування Менга;

$\left(e; n\right)$ і $\left(d; n\right)$ – публічний та секретний ключ в алгоритмі RSA;

DOI 10.15588/1607-3274-2016-2-10

$\langle (e,n),x \rangle$ – трійка публічний параметрів в протоколі OT_n^1;

$f_{\text{ДЛ}}(\ldots)$ – функція дискретного логарифмування;

g – генератор мультиплікативної групи;

$hash(r_2)$ – значення хеш – функції від r_2;

$k < n$ – випадкове числове значення;

k' – проміжне числове значення;

m – секретне повідомлення, яке належить до групи Z_N;

m' – фіктивне повідомлення, яке належить до групи Z_N;

(m_1, m_2) – пара числових значень m_1 і m_2;

(m,r) – пара числових значень, еквівалентна m і r_2;

N – модуль утворений добутком чисел p і q;

$\langle (N,g,h),(p,q) \rangle$ – пара публічного та секретного ключів одержувача;

$ord(\ldots)$ – порядок будь-якого числового елемента групи;

OT_n^1 – Oblivious Transfer Protocol;

p – модуль перетворень еквівалентний N^2;

p і q – великі прості сильні числа (p' і q');

r – випадковий елемент мультиплікативної групи, еквівалентний r_2;

r_1 – випадковий елемент мультиплікативної групи;

$r_2 \in \langle g \rangle$ – випадковий елемент мультиплікативної групи, побудований на g;

$\{T_i, M_i\}$ – пара секретного та фіктивного повідомлень в алгоритмі Рабіна;

t_p – час виконання будь – якої операції при даному розмірі модуля p;

$t_{\text{гк}}$ – числове значення часу генерації ключів в алгоритмі;

ν – проміжне числове значення;

$X(t)$ – числове значення псевдовипадкової послідовності;

$x < n$ – випадкове числове значення;

$\langle (y,g,p),a \rangle$ – пара публічного та секретного ключів відправника;

γ_1 – проміжне числове значення;

$Z^*_{N^2}$ – мультиплікативна група для числа N^2.

ВСТУП

Сучасні алгоритми шифрування не можуть забезпечувати абсолютну стійкість до атак зловмисників як зовні, так і з середини системи. Атаки на основі примушування можна застосовувати для отримання будь-якої секретної інформації. Вирішення цієї проблеми полягає у застосуванні алгоритмів «неоднозначного» або заперечуваного шифрування.

Наукова новизна полягає у функціональній заміні задачі дискретного логарифмування, яка використовується в процедурі розподілу ключів, на протокол «непомітної» передачі OT_n^1 в алгоритмі заперечуваного шифрування Менга.

Актуальність теми статті полягає у зниженні ефективності захисту інформації сучасними криптографічними системами та необхідність пошуку нових рішень для виправлення цієї проблеми.

Об'єкт дослідження – процедура розподілу ключів між абонентами в алгоритмі заперечуваного шифрування Менга.

Актуальність теми статті полягає у зниженні ефективності захисту інформації сучасними криптографічними системами та необхідність пошуку нових рішень для виправлення цієї проблеми.

Об'єкт дослідження – процедура розподілу ключів між абонентами в алгоритмі заперечуваного шифрування Менга.

Предмет дослідження – це властивостей алгоритму заперечуваного шифрування Менга та особливостей протоколу «непомітної» передачі OT_n^1.

Мета роботи полягає в модифікації алгоритму заперечуваного шифрування Менга шляхом огляду та аналізу існуючих алгоритмів і протоколів безпечної передачі інформації. Для досягнення цієї мети необхідно виконати наступні завдання:

– зробити огляд аналогічних рішень у подібних алгоритмах шифрування персональних даних;

– виконати аналіз структури та особливостей захисту інформації подібними алгоритмами заперечуваного шифрування;

– виконати модифікацію процедури розподілу ключів у алгоритмі заперечуваного шифрування Менга;

– виконати порівняння швидкодії процедур розподілу ключів в первісному та модифікованому алгоритмах заперечуваного шифрування Менга, зробити висновки щодо результів модифікацій алгоритму та їх вплив на ефективність захисту інформації.

1 ПОСТАНОВКА ЗАДАЧІ

Основна проблема при використанні алгоритму заперечуваного шифрування Менга полягає в умовності його структури, що унеможливлює його практичне застосування для захисту інформації в реальних комп'ютерних мережах. Оскільки вона виникає на етапі генерації ключів, то необхідно виконати модифікацію процедури розподілу ключів, але не робити значних змін у структурі самого алгоритму шифрування.

Суть проблеми полягає у неможливості виконання розподілу ключів між абонентами через використання задачі дискретного логарифмування для передачі секретного ключа a відправника одержувачеві. Оскільки задача дискретного логарифмування за складністю обчислень еквівалентна до задачі з факторизації, то при обчисленні одержувачем секретного ключа a відправника з публічного параметру h і модуля $p \sim N^2$ час виконання процедури розподілу ключів можна описати виразом $t_{p \sim N^2} \to \infty$.

Для забезпечення оптимального часу виконання процедури генерації та розподілу ключів використати протокол «непомітної» передачі OT_n^1, який описано в [2] і застосовано для вирішення подібної проблеми в алгоритмі заперечуваного шифрування Ібраxіма [3]. Оскільки стійкість протоколу «непомітної» передачі ґрунтується на вирішенні задачі з факторизації, то необхідно виконати аналіз швидкодії даного протоколу із швидкістю вирішення еквівалентної задачі – дискретного логарифмування, в оригінальному алгоритмі заперечуваного шифрування Менга.

2 ОГЛЯД ЛІТЕРАТУРИ

Для надійного захисту інформації, як на локальних комп'ютерах так і тієї, що передається по мережі, використовуються криптографічні засоби захисту інформації. Одним із напрямів криптографічного захисту інформації є шифрування. В зв'язку з цим проводиться безперервні дослідження існуючих криптографічних схем шифрування та створення нових криптографічних схем, на їх базі. Як новий напрям, в криптографії виділяють розробку та дослідження алгоритмів заперечуваного шифрування. В сучасній літературі для цього напряму використовують такі ж поняття, як «неоднозначне», «суперечливе» або «заперечуване».

Існує не так багато джерел, які описують алгоритми заперечуваного шифрування, на відміну від інших. Така тенденція пов'язана з одним із основним аспектів заперечуваного шифрування, який гарантує надійність захисту – таємність алгоритмів заперечуваного шифрування. В результаті досліджень даного напряму було знайдено деякі публікації і статті, які описують перспективність алгоритмів заперечуваного шифрування для застосування в сфері криптографічного захисту інформації.

Досліджені алгоритми заперечуваного шифрування, здебільшого, побудовані на основі криптографічних систем з відкритим ключем, оскільки останні набули популярності в останні роки. До таких алгоритмів можна віднести алгоритми заперечуваного шифрування розроблені: Раном Канетті, Хамадою Ібрахімом, Джин – Квін Вангом і Бо Менгом, М. А. Молдов'яном і О.О. Горячевим, Шаффі Голвасером і С. Мікалі [4] та ін.

Алгоритм заперечуваного шифрування Рана Канетті [4] є криптографічною системою з відкритим ключем, яка дозволяю користувачам не виконувати попередній обмін секретними параметрами для шифрування/дешифрування інформації. Алгоритм заперечуваного шифрування Канетті передбачає реалізацію механізму побітового шифрування даних, тому він є менш продуктивним, але має досить надійний рівень захисту.

Алгоритм заперечуваного шифрування Хамади Ібрахіма [3] побудовано на базі протоколу RD – PKE, який дозволяє повністю захистити одержувача секретної інформації від застосування примушування. Така змога надається шляхом поділу секретного ключа між одержувачем та довіреною стороною безпеки за допомогою протоколу [3]. Оскільки одержувач не має достатньої кількості інформації для самостійного розшифрування криптограми, то застосування примушування стосовно нього не є ефективним.

Алгоритм заперечуваного шифрування М. А. Молдов'яна і О. О. Горячева[5] побудовано на базі розширеної криптографічної схеми Рабіна з відкритим ключем. Даний алгоритм заперечуваного шифрування на достатньому рівні вирішує завдання пов'язані зі стійкістю криптографічної системи до атак заснованих на базі примушування. Модифікація алгоритму шифрування Рабіна передбачає відновлення чотирьох різних пар секретних/фіктивних повідомлень $\{T_i, M_i\}$, три з яких мають випадковий характер. Оскільки даний алгоритм відноситься до криптографічних систем з відкритим ключем, то основою захисту є обчислювальна складність, яка базується на вирішенні задачі факторизації. Таким чином, секретність власне алгоритму не є критичною.

Алгоритм заперечуваного шифрування Шафі Голдвасера і Сильвіо Мікалі [4] побудовано на базі комбінованого алгоритму ймовірнісного шифрування [6]. В літературі даний алгоритм отримав назву – асоційований алгоритм ймовірнісного шифрування. Основним критерієм захисту є неоднозначність дешифрованих повідомлень, тобто ймовірність того, що зловмисник має змогу дешифрувати криптограму та відрізнити результати від випадкових значень досить низька. Проте його недоліком є можливість дешифрування лише одного повідомлення.

Алгоритм заперечуваного шифрування Джин-Квін Ванга і Бо Менга [1] побудовано на базі протоколу BCP [7] та ідей запропонованих Клоновскі [8]. В даному алгоритмі комбіновано кращі сторони алгоритмів RSA та Ель-Гамаля, саме тому він має більш кращі показники захищеності та продуктивності роботи. Представлений алгоритм заперечуваного шифрування передбачає використання двох алгоритмів розшифрування захищеного повідомлення, який катастрофічно знижував ефективність захисту. Але використання двох пар секретних ключів і обчислювальна складність криптографічних систем з відкритим ключем забезпечують досить надійний захист секретної інформації та досить високий рівень продуктивності.

3 МАТЕРІАЛИ І МЕТОДИ

Алгоритм заперечуваного шифрування Менга вирішує проблему щодо атак на основі примушування, яке застосовується як до відправника та одержувача, так і до обох одночасно. Таким чином виключається будь – яка можливість отримання секретної інформації зловмисником. Структурна схема алгоритму заперечуваного шифрування Менга приведена в Додаток А.

Оскільки на етапі генерації ключів виникає проблема пов'язана з розподілом ключів між абонентами, то її вирішення полягає у модифікації первісного алгоритму (Додаток А) шляхом функціональної заміни задачі дискретного логарифмування на протокол «непомітної» передачі OT_n^1 (рис. 1).

Згідно з результатами експериментів проведених у пункті 4 можна зробити висновок, що застосування протоколу «непомітної» передачі OT_n^1 в процедурі розподілу ключів алгоритму заперечуваного шифрування Мен-

га має більш оптимальний час і спрощує його технічну реалізацію. Таким чином модифікований варіант алгоритму заперечуваного шифрування Менга приведено в Додаток Б, а приклад його роботи приведено нижче (в якості тестових повідомлень використані «Security» і «United Ukraine» відповідно секретне та фіктивне тестові повідомлення).

На етапі підготовки було виконано генерацію секретних і публічних ключів одержувача $\langle (N,g,h),(p,q) \rangle$ та відправника $\langle (y,g,p),a \rangle$, які приведено в табл. 1.

На етапі шифрування було виконано обчислення криптограми $\langle (\partial,\wp),B \rangle$, яку відправник передає по відкритому каналу одержувачеві. Результати обчислень приведено в табл. 2.

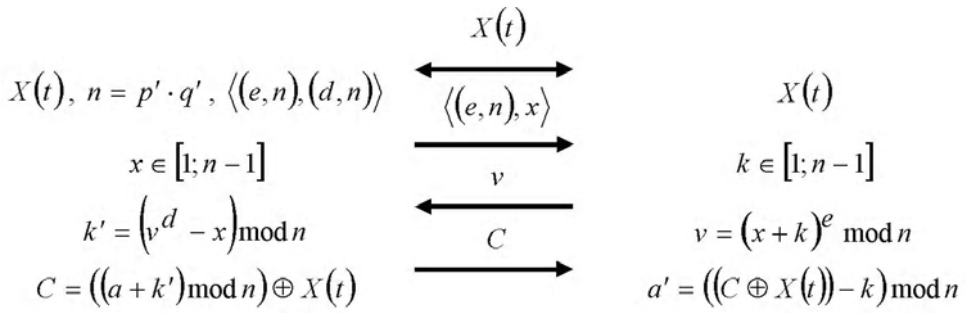


Рисунок 1 – Структурна схема протоколу «непомітної передачі» OT_n^1

Таблиця 1 – Секретний та відкритий ключі відправника та одержувача

Абоненти	Позначення	Значення
Відправник	N	*340282393626195344062954022172595310137*
	g	*45769203547515261684864 4*
	h	*109066888395335831186793921949405725400121626796378019323902565298338926914653*
	p	*18446744847862403543*
	q	*18446744747251547759*
Одержувач	$X(t)$	*454517681881*
	(e,d,n)	*(325514516927,13740242815079940142790 3,663108052854589966200253)*
	x	*233168199764*
	k	*365161775673*
	v	*210858578369542822886041*
	a	*775224541535*
	C	*1513289100609*
	a'	*775224541535*
	y	*109066888395335831186793921949405725400121626796378019323902565298338926914653*
	g	*45769203547515261684864 4*
	p	*11579210741197294971852128355385294945305813979775842618871218310928721495876 9*

Таблиця 2 – Обчислення криптограми $\langle (\partial,\wp),B \rangle$

Позначення параметрів	Значення
r_2	*976111453564*
m	*8751735916204352851*
$C(r_2,m)$	*4944128327931454803528618175015452521801373092820406824902092812272307796148 8*
m'	*2057271081577553248481314125475413*
r_1	*2744558201036439643830698319078052477901324357140583800248748001864070337832 6*
$C(r_1,m')$	*4944128327931454803528618175015452521801373092820406824902092812272307796148 8*
$hash(r_2)$	*976111453573*
B	*4944128327931454803528618175015452521801373092820406824902092812272307796148 8*
∂	*7120757359751600539380457168433360239215956805097502870744764841488557454648*
$\wp$	*8983929684275778172654129352885340170739411186409128932028046571941013467619 3*

На етапі розшифрування одержувачем було відновлено секретне повідомлення m з криптограми $\langle(\partial,\wp),B\rangle$, результати обчислень якого приведено в табл. 3.

В результаті виконаних обчислень одержувач отримав секретне повідомлення «Security», яке було адресоване йому.

На етапі дешифрування, в результаті застосування примусу, одержувач виконав відновлення фіктивного повідомлення m' з криптограми $\langle(\partial,\wp),B\rangle$, яке призначене власне для зловмисника, результати обчислень якого приведено в табл. 4.

В результаті виконаних обчислень одержувач відновив фіктивне повідомлення «United Ukraine» та передав його зловмисникові.

Таким чином було виконано моделювання роботи модифікованого алгоритму заперечуваного шифрування Менга за допомогою 128-бітного ключа та продемонстровано його особливості, які забезпечують надійний захист інформації від атак на основі примусу. Для оцінки ефективності виконаних модифікацій алгоритму авторами проведено експерименти щодо визначення оптимальної швидкодії його роботи шляхом порівняння швидкодії первісного та модифікованого алгоритмів.

Оскільки модифікація полягала в покращенні часових характеристик процедури генерації та розподілу ключів, то для спрощення експериментів, у пункті 4, було досліджено швидкодії процедур генерації ключів $t_{\text{ГК}}$: на основі задачі дискретного логарифмування та протоколу «непомітної» передачі OT_n^1.

4 ЕКСПЕРИМЕНТИ

Для покращення часових характеристик процедури генерації та розподілу ключів авторами було проведено експерименти з дослідження швидкодії процедур генерації ключів $t_{\text{ГК}}$: на основі задачі дискретного логарифмування та протоколу «непомітної» передачі OT_n^1 (рис. 2).

Для виконання експериментів було використано структурні схеми первісного та модифікованого алгоритмів заперечуваного шифрування Менга (Додаток А і Додаток Б) і персональний комп'ютер з технічними характеристиками:

– ОС: Windows 7;

– ЦП: AMD Athlon(tm) II P360 Dual – Core Processor 2.3 ГГц;

– ОЗУ: 3 Гб;

– ПЗ: пакет математичних обчислень Maple 14.

Основний показник, який досліджувався в ході експериментів – це швидкодія виконання процедури генерації ключів $t_{\text{ГК}}$. За результатами проведених експериментів автори виконали порівняльну характеристику швидкодії процедур генерації ключів і визначили оптимальний час $t_{\text{ГК}}$ для виконання процедури генерації ключів, а також метод за допомогою якого вона виконана.

5 РЕЗУЛЬТАТИ

В ході проведених експериментів (рис. 2) автори отримали експериментальні дані щодо генерації ключів із використанням задачі дискретного логарифмування (табл. 5).

При досяжності розрядності модуля p у 256 біт і більше, в першому експерименті спостерігається експоненціальне зростання часу відведеного на генерацію ключів. Оскільки за вимогами сучасних криптографічних систем безпечна розрядність ключа повинна складати 1024–2048 біт, то час необхідний для генерації ключів можна описати виразом $t_p \to \infty$.

В ході проведення другого експерименту (рис. 2) експериментальні дані, отримані авторами, носять практично константний характер, тобто одне й те саме значення для ключів, яке складає 15–16 мс для ключів розрядністю до 2048 біт і більше (коливання часу на рівні 1 мс).

Таблиця 3 – Відновлення секретного повідомлення m

Позначення параметрів	Значення
D	*29605105317476900925245466022643727530484548476548504967891351479412026975 42*
π	*58422416232404436471085961576632679733*
m	*8751735916204352851*

Таблиця 4 – Відновлення секретного повідомлення m'

Позначення параметрів	Значення
r_2	*976111453564*
r_1	*27445582010364396438306983190780524779013243571405838002487480018640703378326*
A_1	*86120330409262410220532378382346931244890834587769244209422058121590708003399*
A_2	*42368364285961378337324940846616483686887069999828052556155055445614458883516*
m_1	*20572710815775532484813141254754 13*
m_2	*8751735916204352851*
m	*8751735916204352851*
r	*976111453564*
m'	*20572710815775532484813141254754 13*

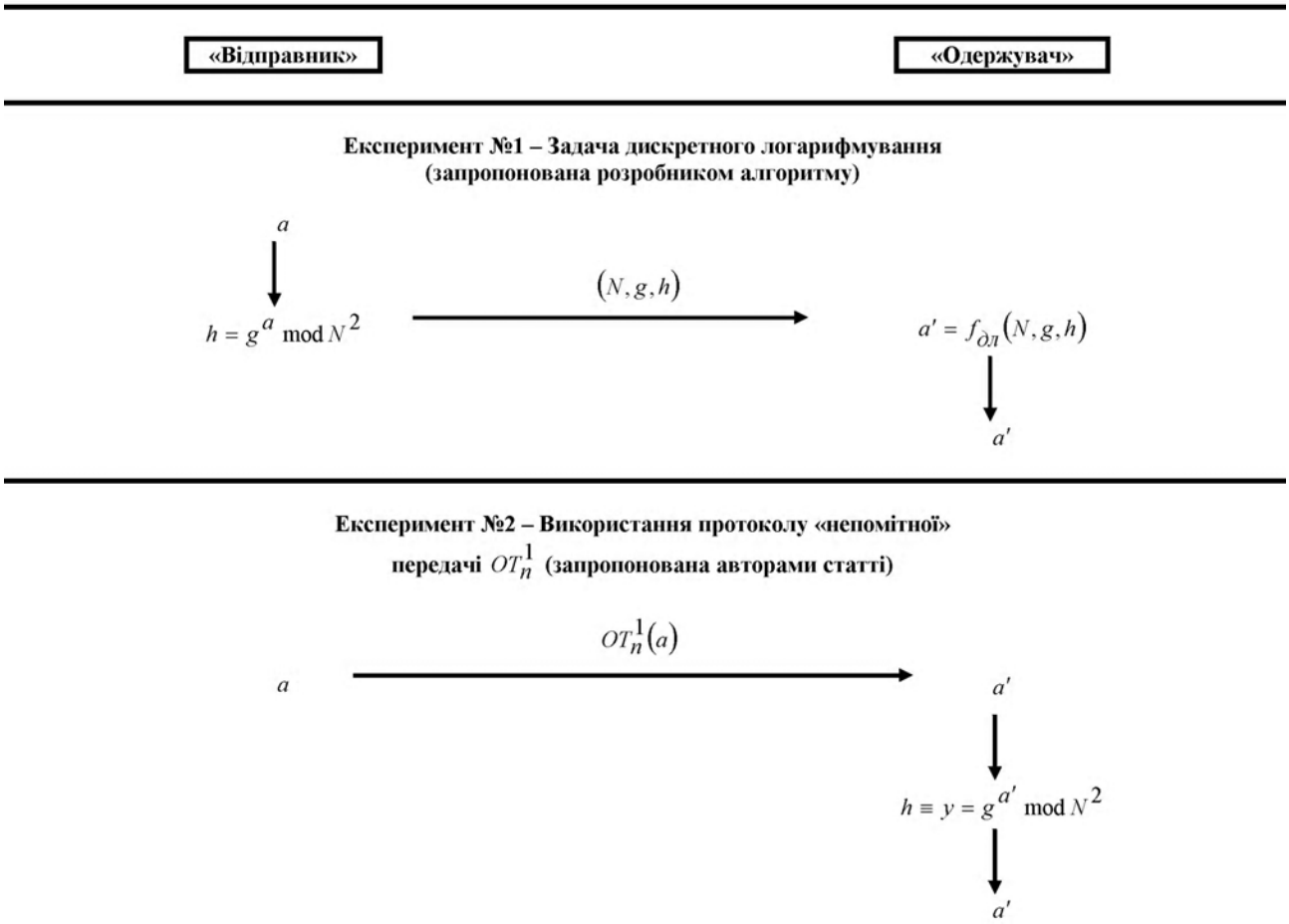


Рисунок 2 – Схема експериментів

Таблиця 5 – Дані отримані з першого експерименту

Модуль p, біт	8	16	32	64	128	256
Час $t_{ГК}$, секунд	0,051	0,46	0,61	6,19	598,92	8329,3

6 ОБГОВОРЕННЯ

Проблема практичної реалізації алгоритму заперечуваного шифрування Менга на початку статті полягала обчислювальній стійкості задачі дискретного логарифмування, при якій час генерації виконання усього алгоритму в цілому описується виразом $t_p \to \infty$. Використовуючи експериментальні дані з табл. 5 автори зробили теоретичний прогноз щодо зростання часу генерації ключів, який відображає графік на рис. 3.

Згідно із прогнозом авторів у першому експерименті, для генерації ключів в алгоритмі заперечуваного шифрування Менга розрядністю до 4096 біт, комп'ютеру із запропонованими тестовими характеристиками необхідно витратити до 596 днів машинного часу. Що згідно зі стандартами криптографічних систем, які декларують безпечну розрядність ключа в 1024–2048 біт, є не оптимальним застосуванням алгоритму для вирішення прикладних завдань.

За результатами другого експерименту авторами було встановлено, що оптимальний час для виконання всього алгоритму заперечуваного шифрування Менга складає 15–16 мс для ключів розрядністю до 4096 біт і

Рисунок 3 – Прогнозована оцінка зростання часу виконання процедури генерації ключів в першому експерименті

більше. Таким чином, дані отримані в результаті проведення другого експерименту (рис. 2), із використанням протоколу «непомітної» передачі OT_n^1, свідчать про ефективність виконаних модифікацій в алгоритмі заперечуваного шифрування Менга. Отже підхід запропонований авторами для вирішення проблеми у первісного алгоритму є прийнятним з точки зору інформаційної безпеки та практичної реалізації власне алгоритму, а отже застосування протоколу «непомітної» передачі в достатній мірі вирішує проблему пов'язану зі структурою первісного алгоритму заперечуваного шифрування Менга [7].

ВИСНОВКИ

Згідно з метою, поставленою на початку статті, авторами вирішено проблему практичного застосування алгоритму заперечуваного шифрування Менга. В результаті проведених досліджень та експериментів було вирішено наступні завдання:

– виконано огляд рішень проблеми, яку автори визначили структурі алгоритму заперечуваного шифрування Менга, на основі аналогічних алгоритмів заперечуваного шифрування персональних даних;

– виконано аналіз структури та особливостей подібних алгоритмів заперечуваного шифрування та визначено методи для вирішення проблеми;

– виконано модифікацію алгоритму заперечуваного шифрування Менга за допомогою використання протоколу «непомітної» передачі OT_n^1;

– на основі проведених експериментів було проведено аналіз ефективності виконаних модифікацій і доведено ефективність використання протоколу «непомітної» передачі OT_n^1 для усунення недоліків первісного алгоритму заперечуваного шифрування Менга.

За результатами досліджень автори виконали модифікацію алгоритму заперечуваного шифрування Менга (Додаток Б). Для вирішення проблеми було використано новий підхід заснований на використанні протоколу «непомітної» передачі OT_n^1, що дозволило суттєво зменшити час роботи алгоритму Менга та зробити можливим його використання для вирішення практичних завдань в сфері інформаційної безпеки.

Наукова новизна полягає у використанні протоколу «непомітної» передачі для розподілу ключів між абонентами, що є принципово новим підходом до захисту інформації в алгоритмі заперечуваного шифрування Менга.

Робота виконана на кафедрі захисту інформації в рамках НДКР №04515 «Дослідження і розробка криптографічних та технічних засобів захисту інформації».

СПИСОК ЛІТЕРАТУРИ

1. Wang J. A Receiver Deniable Encryption Scheme / J. Wang, Bo Meng // Proceedings of the 2009 International Symposium on Information Processing (ISIP'09), 21–23 August 2009: proceedings. – Huangshan : P. R. China, 2009. – P. 254–257.
2. Naor M. Efficient oblivious transfer protocols / M. Naor, B. Pinkas // Proceedings of SIAM Symposium on Discrete Algorithms (SODA '01), 2001: proceedings. – Society for Industrial and Applied Mathematics, 2001. – P. 448–457.
3. Ibrahim H. Receiver–deniable Public–Key Encryption / H. Ibrahim // International Journal of Internet Security. – 2009. – Vol. 8, № 2. – P. 159–165.
4. Козіна Г. Л. Заперечуване шифрування / Г. Л. Козіна, А. В. Гальченко // Тиждень науки – 2015: Тези доповідей щорічної наук. – практ. конф. викладачів, науковців, молодих учених, аспірантів, студентів ЗНТУ, Запоріжжя, 13–17 квітня 2015 р. – Запоріжжя : ЗНТУ, 2015.
5. Canetti R. Deniable Encryption / [R. Canetti, C. Dwork, M. Naor, R. Ostronsky] // Advances in Cryptology. – CRYPTO, 1997, Proceedings. – P. 90–104.
6. Молдовян Н.А. Расширение криптосхемы Рабина: алгоритм отрицаемого шифрования по открытому ключу / Н. А. Молдовян, А. А. Горячев, М. А. Вайчикаускас // ВЗИ. Журнал по вопросам защиты информации. – ФГУП «ВИМИ», 2014. – № 2. – С. 12–16.
7. Фисун С.Н. Комбинированный алгоритм вероятностного шифрования / С. Н. Фисун, О. И. Куржиевская // Изд-во СевНТУ, 2010. – № 101. – С. 37–40.
8. Bresson E. A Simple Public – Key Cryptosystem with a Double Trapdoor Decryption Mechanism and its Applications / E. Bresson, D. Catalano, D. Pointcheval // Advances in Cryptology – ASIACRYPT, 2003. LNCS, Vol. 2894. Springer, Heidelberg, 2003. – P. 37–54.
9. Klonowski M. Practical Deniable Encryption // M. Klonowski, P. Kubiak, and M. Kutyiowsk // SOFSEM 2008: Theory and Practice of Computer Science, 34th Conference on Current Trends in Theory and Practice of Computer Science, Slovakia : Novy Smokovec, 19–25 January 2008: proceedings. – 2008. – P. 599–609.
10. Николенко С. Поиск дискретного логарифма [Электронный ресурс] / С. Николенко. – Режим доступа: https://compscicenter.ru/media/slides/cryptoprotocols2014_2015_spring/2015_03_11_cryptoprotocols2014_2015_spring_lGKdY5s.pdf.
11. Горбенко И. Д. Методы распараллеливания алгоритма Полларда решения задачи дискретного логарифмирования для систем с общей памятью / И. Д. Горбенко, Е. Г. Качко, К. А. Погребняк // Изд-во ХНУРЭ, 2012. – С. 1–6.

Стаття надійшла до редакції 16.12.2015.
Після доробки 20.12.2015.

Гальченко А. В.[1], Козина Л.[2]

[1]Ст. гр. РТ – 710М, магистр кафедры защиты информации Запорожского национального технического университета, Запорожье, Украина

[2]Канд. физ.-мат. наук, доцент кафедры защиты информации Запорожского национального технического университета, Запорожье, Украина

МОДИФИКАЦИЯ АЛГОРИТМА ОТРИЦАЕМОГО ШИФРОВАНИЯ МЕНГА

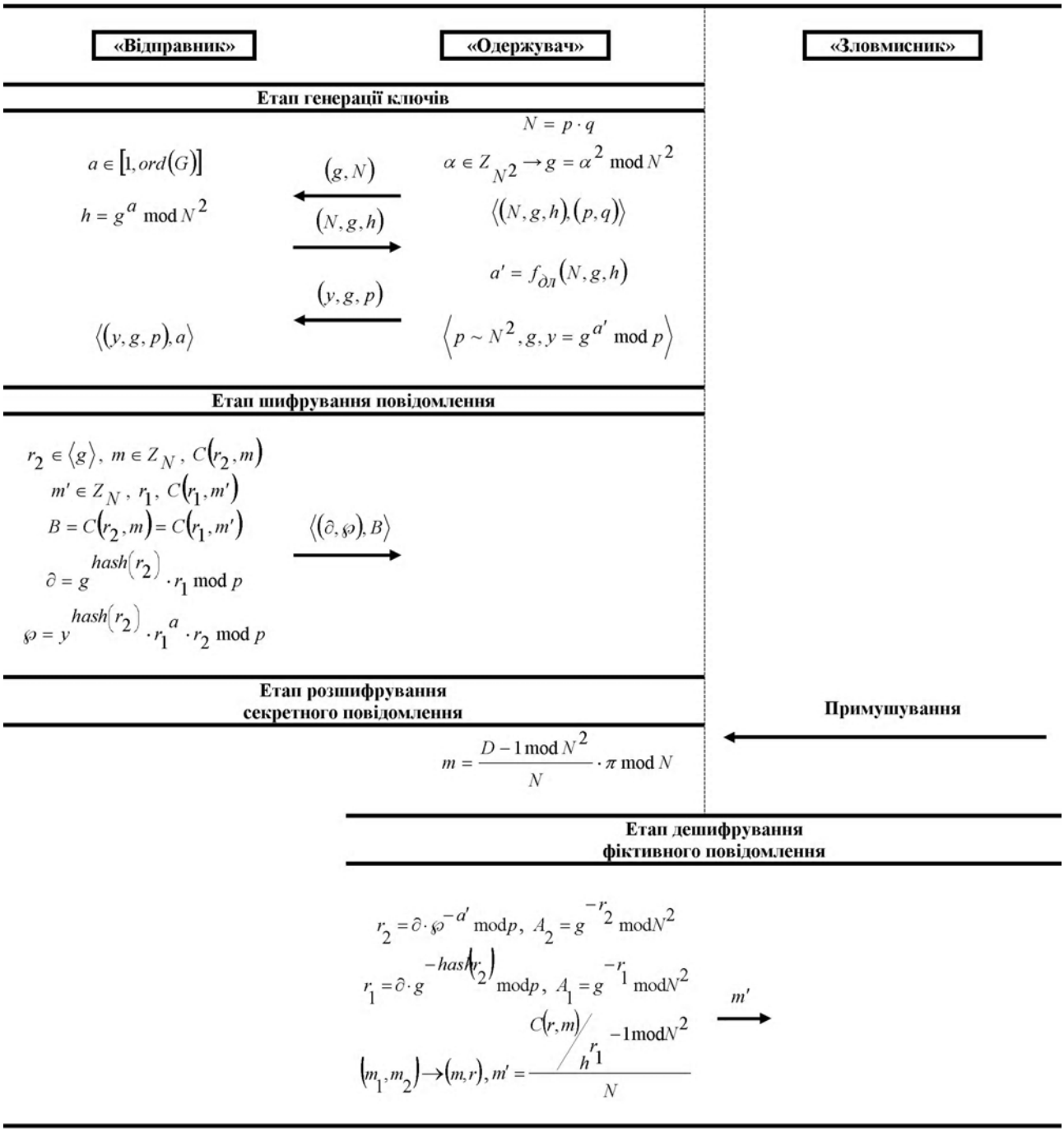
В статье обсуждается проблема устойчивости современных криптографических систем к атакам на основе принуждения в отношении абонентов криптографических систем. В связи со стремительным развитием отрасли информационных технологий эта проблема актуальна в сфере информационной безопасности. Для решения проблемы устойчивости современных криптографических систем авторы предлагают использовать алгоритмы отрицаемого шифрования, которые гарантируют, что злоумышленник не имеет возможности получить какую – либо ценную информацию от абонентов. Решение проблемы заключается в использовании алгоритма отрицаемого шифрования Менга, который гарантирует защиту не только информации, но и самих участников обмена.

Основная цель статьи состоит в модификации первоначального алгоритма отрицаемого шифрования Менга [1] с помощью протокола «незаметной» передачи OT_n^1, использование которого предложено Мони Наором [2]. Применение протокола «незаметной» передачи позволяет существенно сократить время, необходимое для выполнения алгоритма отрицаемого шифрования Менга, и упрощает его реализацию для решения прикладных задач в области информационной безопасности.

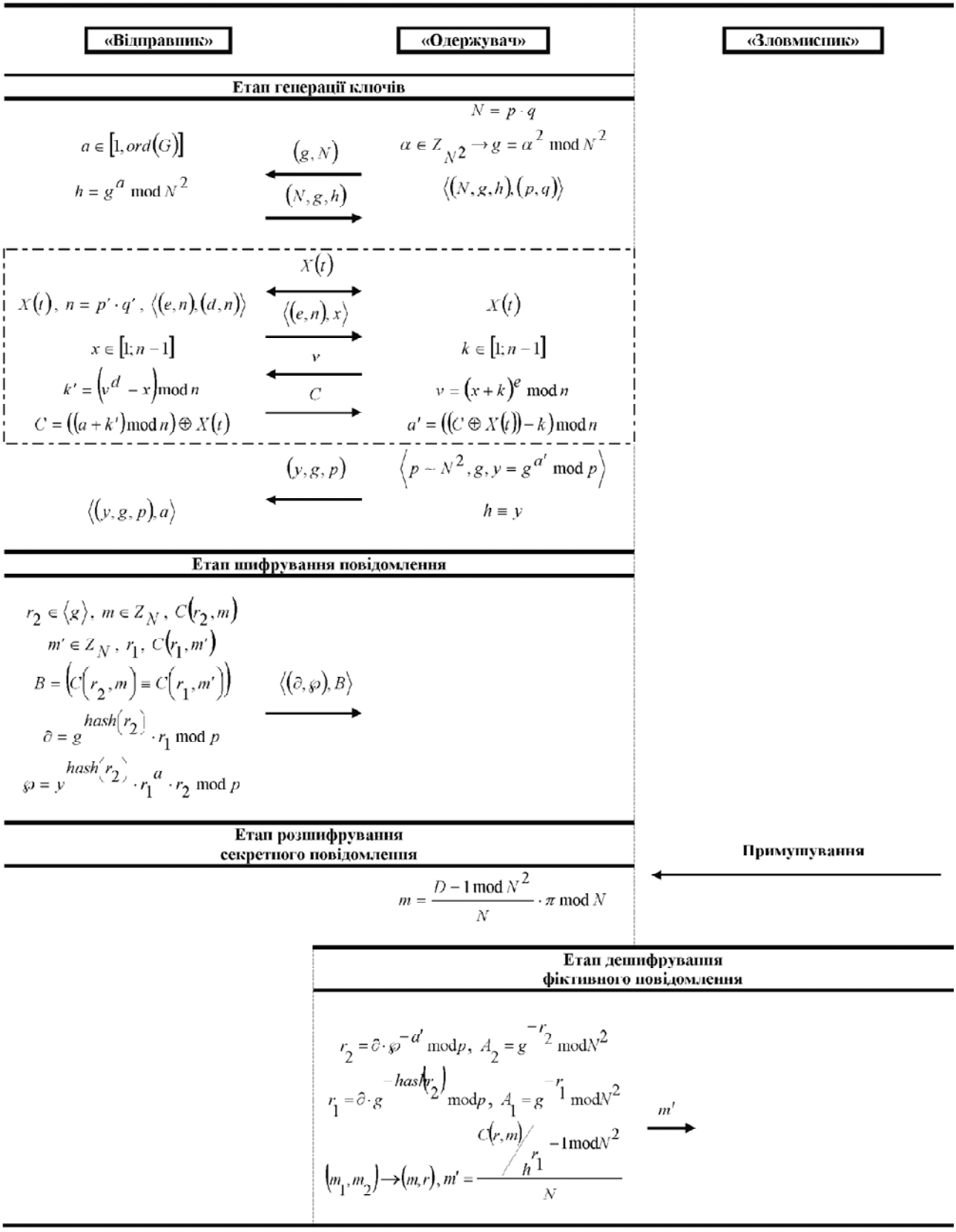
По результатам проведенных экспериментов авторами статьи было подтверждено, что использование протокола «незаметной» передачи является эффективным решением проблемы генерации и распределения ключей в алгоритме отрицаемого шифрования Менга.

Ключевые слова: протокол, отрицаемое шифрование, неоднозначность, распределение ключей, фиктивное сообщение, злоумышленник, расширенная схема Рабина, незаметная передача, факторизация, дискретное логарифмирования.

Додаток А – Структурна схема первісного алгоритму заперечуваного шифрування Менга



Додаток Б – Структурна схема модифікованому алгоритму заперечуваного шифрування Менга



Galchenko A. V.[1], Kozina G. L.[2]

[1]Gr. RT – 710M, Master of the Department of Information Protection of Zaporozhzhya National Technical University, Zaporizhzhya, Ukraine

[2]Candidate of Phys.-Math. sciences, Associate Professor of the Department of Information Protection of Zaporozhzhya National Technical University, Zaporizhzhya, Ukraine

MODIFICATION OF MENG'S DENIABLE ENCRYPTION ALGORITHM

The article discusses the stability of modern cryptographic systems to attack from coercion in respect of subscribers cryptographic systems. Due to the rapid development of information technology, this problem is relevant in the field of information security. To address the sustainability of modern cryptographic systems use algorithms offered by the authors deniable encryption ensures that the attacker is unable to get any valuable information from subscribers. Solving the problem is to use Meng's deniable encryption algorithm, which guarantees protection not only information, but also the participants of the exchange.

The main purpose of the article is performed by modifying the initial Meng's deniable encryption algorithm [1] with using Oblivious Transfer Protocol , which prompted by Moni Naor [2]. Oblivious Transfer Protocol to significantly reduce the time required to perform the Meng's deniable encryption algorithm, and facilitates its implementation to solve applied problems in the field of information security.

As a result of experiments, the authors confirmed that Oblivious Transfer Protocol using is an effective solution to the problem of generation and distribution of keys in the Meng's deniable encryption algorithm.

Keywords: protocol, deniable encryption, ambiguity, distribution keys, fake messages, an extended Rabin's scheme, oblivious transfer, factorization, discrete logarithm.

REFERENCES

1. Wang J., Meng Bo A Receiver Deniable Encryption Scheme, *Proceedings of the 2009 International Symposium on Information Processing (ISIP'09), 21–23 August 2009: proceedings*, Huangshan, P. R. China, 2009, pp. 254–257.
2. Naor M., Pinkas B. Efficient oblivious transfer protocols, *Proceedings of SIAM Symposium on Discrete Algorithms (SODA '01), 2001: proceedings. – Society for Industrial and Applied Mathematics,* 2001, pp. 448–457.
3. Ibrahim H. Receiver-deniable Public-Key Encryption, International Journal of Internet Security, 2009, Vol. 8, No. 2, P. 159–165.
4. Kozina G. L., Galchenko A. V. Deniable encryption, *Weeak of Science – 2015: Abstracts annual scientific – practical conference of teachers, scientists, young scientists, graduate students ZNTU, Zaporizhzhya , 13–17 April 2015*. Zaporizhzhya, ZNTU, 2015.
5. Canetti R., Dwork C., Naor M., Ostronsky R. Deniable Encryption. Advances in Cryptology – CRYPTO, 1997, Proceedings, pp. 90–104.
6. Moldovyan N. A., Goryachew A. A., Wichikaukas M. A. Extened Rabins's cryptographic scheme: deniable encryption by public key, *VZI. Journal of information security*. FSUE «VIMI», 2014, No. 2, pp. 12–16.
7. Fisun S. N., Kurzhievskaya O. I. Combined probabilistic encryption algorithm, *SevNTU*, 2010, No. 101, pp. 37–40.
8. Bresson E., Catalano D., Pointcheval D. A Simple Public – Key Cryptosystem with a Double Trapdoor Decryption Mechanism and its Applications, *Advances in Cryptology – ASIACRYPT, 2003. LNCS, Vol. 2894*. Springer, Heidelberg, 2003, pp. 37–54.
9. Klonowski M., Kubiak P., and Kutyiowsk M. Practical Deniable Encryption, *SOFSEM 2008: Theory and Practice of Computer Science, 34th Conference on Current Trends in Theory and Practice of Computer Science, Slovakia: Novy Smokovec, 19–25 January 2008: proceedings*. – 2008. P. 599–609.
10. Nikolenko S. Search the discrete logarithm [Electronic resource]. Access: https://compscicenter.ru/media/slides/cryptoprotocols2014_2015_spring / 2015_03_11_cryptoprotocols2014_2015_spring_lGKdY5s.pdf.
11. Gorbenko I. D., Muscled E. G., Pogrebnyak K. A. Methods of algorithm parallelization Pollard solutions discrete logarithm problem for systems with shared memory, *KNURE Publishing House*, 2012, pp. 1–6.