Міністерство освіти і науки України

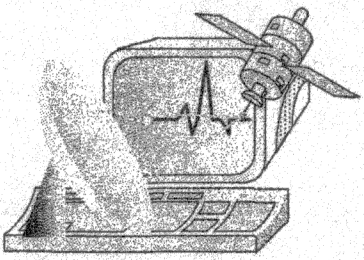
Вінницький національний технічний університет

Вінницька філія ВАТ „Укртелеком"

Інститут кібернетики ім. В.М. Глушкова НАНУ

Вінницьке обласне науково-технічне товариство
радіотехніки, електроніки та зв'язку

Ліга радіоаматорів України



СПРТП-2009

**Матеріали IV Міжнародної
науково-технічної конференції**

СУЧАСНІ ПРОБЛЕМИ РАДІО-ЕЛЕКТРОНІКИ, ТЕЛЕКОМУНІКАЦІЙ ТА ПРИЛАДОБУДУВАННЯ (СПРТП-2009)

*Присвяченої 40-річчю
Факультету радіотехніки та телекомунікацій
Інституту радіотехніки, зв'язку
та приладобудування ВНТУ*

Частина 1

**м. Вінниця, Україна
8 – 10 жовтня 2009 року**

УДК 621.38+621.39+681.2
С 91

Друкується за рішенням Вченої Ради Вінницького національного технічного університету Міністерства освіти і науки України

Відповідальний редактор Н.Г. Курилова

Матеріали статей опубліковані в авторській редакції

С 91 **Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування (СПРТП-2009).** Матеріали IV міжнародної науково-технічної конференції. м. Вінниця, 8 – 10 жовтня 2009 року. Частина 1. – Вінниця, 2009. – 108 с.

Збірка містить матеріали доповідей IV Міжнародної науково-технічної конференції з сучасних проблем радіоелектроніки, телекомунікацій та приладобудування за такими основними напрямками: теорія кіл, математичне моделювання, захист інформації та програмне забезпечення радіоелектронних, телекомунікаційних та біотехнічних систем; обробка сигналів і зображень в радіоелектронних та телекомунікаційних системах; пристрої радіоелектроніки та засоби телекомунікацій; радіотехнічні, телекомунікаційні та оптоелектронні комплекси та системи; радіоелектронні засоби в біомедичній інженерії; радіовимірювальні пристрої та системи; сучасні аспекти розвитку радіоаматорства

УДК 621.38+621.39+681.2

УДК 511.17, 003.26

Дмитришин О. (Україна, м.Вінниця)

ШИФРУВАННЯ ДАНИХ НА ОСНОВІ АРИФМЕТИЧНИХ ОПЕРАЦІЙ ЗА ДОВІЛЬНИМ МОДУЛЕМ

Сучасна комп'ютерна та телекомунікаційна техніка для передачі даних використовує двійкові n-розрядні процесори, що дозволяють виконувати криптографічні перетворення за модулем $m = 2^n$. Модульна арифметика дозволяє реалізовувати два базових перетворення:

– додавання

$$a+b \equiv c \bmod m,$$

– віднімання

$$a \cdot p \equiv d \bmod m,$$

де найбільший спільний дільник (НСД) p і m має бути рівним 1, тобто НСД(p, m) = 1.

При цьому, якщо відомі значення модуля m, c і d, то використовуючи метод повного перебору, який полягає в тому, що для пошуку секретних складових виконується перебір всіх можливих варіантів, можна знайти b і p. Якщо арифметичні операції використовуються в шифруванні, то для операції множення таких варіантів існує – 2^{n-1}, а для операції додавання -2^n-1.

Проте, існує інший підхід до використання модульної арифметики, виконання арифметичних операцій за довільним модулем, що використовується в асиметричних блокових шифрах, зокрема в RSA, DSA. Незручність використання такого підходу полягає в тому, що виконується піднесення до степеня за великим модулем.

В даній роботі, поставлена мета досягти можливості використання операцій додавання та множення в симетричних блокових шифрах при збереженні вище зазначеної криптографічної стійкості з урахуванням розрядності сучасних процесорів.

Головна ідея виконання арифметичних операцій за модулем полягає в використанні такого алгоритму для n-розрядних вхідних та вихідних даних:

Вхід: x – дані, a, a` – секретні складові, m – секретний модуль.

Вихід: y – зашифровані дані.

Алгоритм:

1) якщо $x < m$.

2) то $y = x \circ a \bmod m$.

3) інакше $y = (x-m) \circ a` \bmod (2^n-m)$.

де ° – відповідно або операція додавання (+), або операція множення (·).

Під час виконання операції множення повинні забезпечуватися такі умови: НСД(a`, 2^n-m) = 1 і НСД(a, m) = 1. Значення модуля $m \in (2^{n-2}; 3 \cdot 2^{n-2}]$. Алгоритм розшифрування аналогічний алгоритму за шифрування.

При цьому криптографічна стійкість отриманого перетворення до методу повного перебору складає для операції:

1) додавання: якщо a і m (a` і 2^n-m) є незалежними один від одного, то криптостійкість рівна $\Pi i \cdot 2^{n-2}$, де $i = 2^{n-2}, 2^{n-2}+1, \ldots, 3 \cdot 2^{n-2}$;

2) множення: якщо a і m (a` і 2^n-m) є незалежними один від одного, то криптостійкість рівна $\Pi f(i) \cdot 2^{2n-2}$, де $f(i)$ – функція Ейлера, $i = 2^{n-2}+1, 2^{n-2}+2, \ldots, 3 \cdot 2^{n-2}$.

Таким чином, в роботі, розглянута можливість використання арифметичних операцій за довільним модулем при проектуванні симетричних блокових шифрів.