# ПРОГРАМНО-ТЕХНІЧНІ КОМПЛЕКСИ

УДК 004.056.55

**Я.М. НИКОЛАЙЧУК**
Західноукраїнський національний університет, Тернопіль, Україна,
e-mail: *kmm@wunu.edu.ua.*

**І.З. ЯКИМЕНКО**
Західноукраїнський національний університет, Тернопіль, Україна,
e-mail: *jiz@wunu.edu.ua.*

**Н.Я. ВОЗНА**
Західноукраїнський національний університет, Тернопіль, Україна,
e-mail: *nvozna@ukr.net.*

**М.М. КАСЯНЧУК**
Західноукраїнський національний університет, Тернопіль, Україна,
e-mail: *kasyanchuk@ukr.net.*

## АСИМЕТРИЧНІ АЛГОРИТМИ ШИФРУВАННЯ У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

**Анотація.** Розроблено теоретичні основи асиметричного шифрування на базі системи залишкових класів та її модифікованої досконалої форми. При цьому модулі системи залишкових класів являють собою таємні ключі. Під час відновлення числа за його залишками множення відбувається на довільно вибрані коефіцієнти (відкриті ключі). Встановлено, що криптостійкість запропонованих алгоритмів ґрунтується на розв'язанні задачі факторизації або повного перебору наборів модулів. Розроблені підходи дають змогу практично необмежено збільшувати блок відкритого тексту, усуваючи необхідність використання різних режимів шифрування.

**Ключові слова:** система залишкових класів, криптоалгоритм, асиметрична криптосистема, шифртекст, криптоаналіз, стійкість.

### ВСТУП

На сучасному етапі розвитку інформаційних технологій [1, 2] потрібно розв'язувати низку проблем та науково-технічних задач, пов'язаних з підвищенням стійкості комп'ютерних систем до різного виду атак [3, 4], швидкодії алгоритмів шифрування/розшифрування [5], зменшенням часових складностей виконання базових операцій в асиметричних криптоалгоритмах [6] та створенням засобів захисту інформаційних потоків [7, 8]. Досвід використання відомих алгоритмів шифрування на основі важкооборотних функцій хешування, факторизації [9], дискретного логарифмування, модулярних та інших операцій [10] і розвиток теорії алгоритмів [11], які широко застосовуються на практиці, показує, що їхній потенціал вже наближається до меж своїх можливостей і надалі вони не зможуть бути основою розвитку та вдосконалення засобів захисту інформаційних потоків у сучасних комп'ютерних системах [12, 13].

Зазначимо, що в сучасних асиметричних криптоалгоритмах, які ґрунтуються на позиційних системах числення, є нагальна потреба у розв'язанні трудомістких обчислювальних науково-практичних задач [14], які полягають у необхідності виконання значних обсягів обчислень в реальному часі [15, 16]. Таким чином, важливі та актуальні дослідження з вдосконалення наявних і розроблення нових методів і засобів підвищення продуктивності асиметрич-