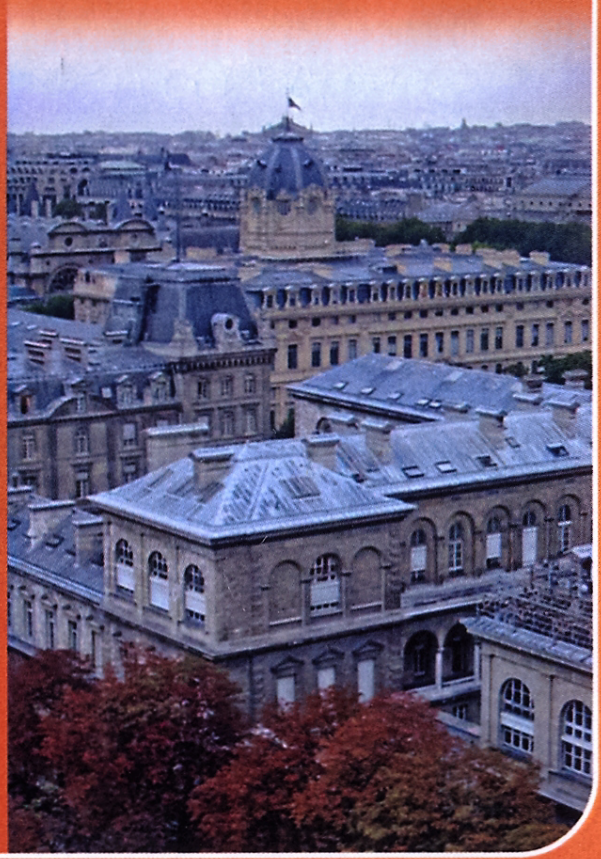
10

МАТЕРИАЛИ
ЗА V МЕЖДУНАРОДНА
НАУЧНА ПРАКТИЧНА
КОНФЕРЕНЦИЯ
1–15 октомври 2007 година

«СТАВАЙКИ СЪВРЕМЕННА НАУКА – 2007»

Математика
Фізика
Съвременни технологии на информации
Физическа култура и спорт

Том 10



София
«Бял ГРАД-БГ» ООД
2007

МАТЕРИАЛИ

ЗА V МЕЖДУНАРОДНА
НАУЧНА ПРАКТИЧНА КОНФЕРЕНЦИЯ

«СТАВАЙКИ СЪВРЕМЕННА НАУКА - 2007»

1-15 октомври 2007 година

Том 10
Математика
Физика
Съвременни технологии на информации
Физическа култура и спорт

София
«Бял ГРАД-БГ» ООД
2007

То публикува «Бял ГРАД-БГ» ООД, Република България, гр.София, район «Триадица», бул. «Витоша» №4, ет.5

Материали за 5-а международна научна практична конференция, «Ставайки съвременна наука», - 2007.
Том 10. Математика. Физика. Съвременни технологии на информации. Физическа култура и спорт.
София. «Бял ГРАД-БГ» ООД - 64 стр.

Редактор: Милко Тодоров Петков

Мениджър: Надя Атанасова Александрова

Технически работник: Татяна Стефанова Тодорова

Материали за 5-а международна научна практична конференция, «Ставайки съвременна наука», 1-15 отомври, 2007 на математика, физика, съвременни технологии на информации, физическа култура и спорт.

За ученици, работници на проучвания.

Цена 10 BGLV

ИНФОРМАТИВНАТА БЕЗОПАСНОСТ

д.т.н., професор, Лукашенко В.М.,
Рудаков К.С., Юпин Р.Є.
Черкаський державний технологічний університет

КРИПТОГРАФІЧНИЙ ПРИСТРІЙ ЗАХИСТУ ІНФОРМАЦІЇ

Актуальність теми. Криптографія є одним з основних інструментів, що забезпечують конфіденційність, довіру, авторизацію, електронні платежі, корпоративну безпеку й незліченну кількість інших важливих речей.

Системам криптографічного захисту інформації і алгоритмічним датчикам випадкових чисел присвячено багато робіт [1-4, 8]. Наприклад в роботах авторів І. Асніса, С. Федоренка, К. Шабунова та інших розглядаються наступні методи криптографічного захисту інформації:

- ✓ цифрові підписи;
- ✓ криптографічні хеш-функції;
- ✓ криптографічні генератори псевдовипадкових чисел;
- ✓ симетричні алгоритми криптографічного захисту інформації;
- ✓ асиметричні алгоритми криптографічного захисту інформації.

Проте в них недостатньо уваги приділяється надійному функціонуванню і гарантованому виявленню помилок під час обробки інформації.

Покладені в основу більшості алгоритмів криптографічного шифрування та дешифрування інформації логічні операції, диктують необхідність забезпечити високу надійність їх виконання.

Авторами пропонується на основі використання двійково-четвіркової системи числення з постійною кількістю одиниць спеціалізований пристрій криптографічного захисту інформації структурна схема якого представлена на рисунках (рисунок 1, 2).

Аналіз запропонованих структур показав наступні характеристики:

- простота обробки даних, що зменшує часові затрати як шифрування так і дешифрування даних;
- однозначність виявлення помилок чи пошкодженого коду;
- однорідність операцій для різних блоків інформації, що спрощує апаратну реалізацію алгоритму;
- можливість прийняти частину інформацію навіть із пошкодженого шифротексту з високою достовірністю точності;
- захист інформації здійснюється завдяки складності відтворення інформації без знання ключової інформації (ключа для генерації псевдовипадкової послідовності блоків даних та команд) і визначається складністю реалізації генератора псевдовипадкової послідовності.

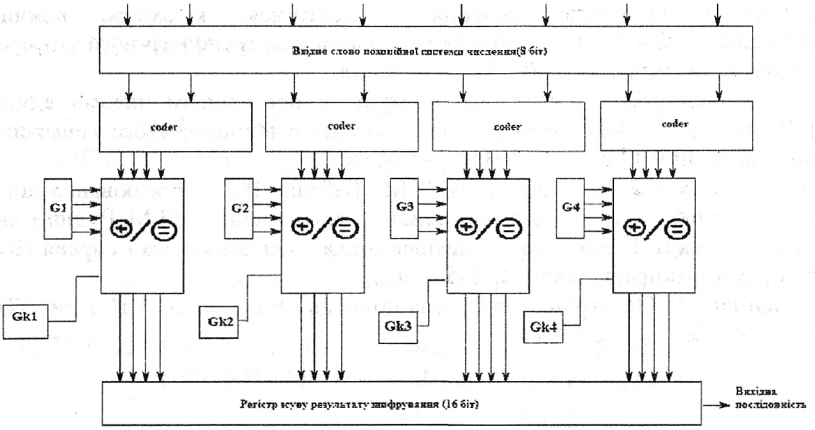


Рисунок 1 Структурна схема шифратора

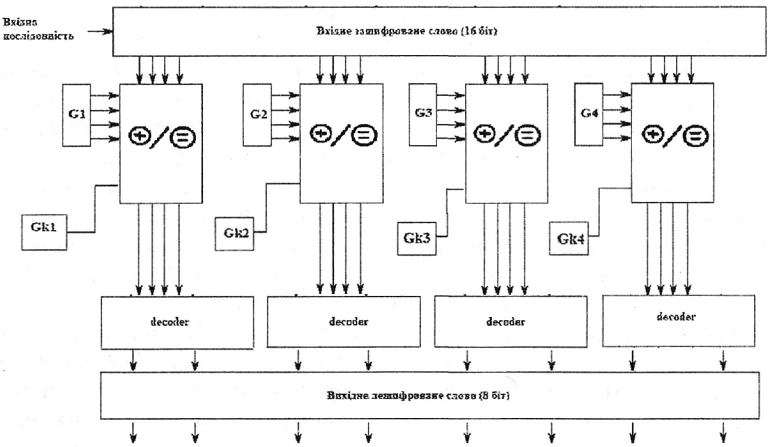


Рисунок 2 Структурна схема дешифратора

Література:

1. Аснис И. Краткий обзор криптосистем с открытым ключом. //И. Аснис, С. Федоренко, К. Шабунов – Защита информации, 1994 - №2. – С.35-44.
2. Першин А. Организация защиты вычислительных систем //А. Першин – Защита информации, 1992. - №1 – С.81-112.

3. Рудницький В.М. Синтез елементів пристроїв криптографічного захисту інформації в системах числення з постійною кількістю одиниць //В.М. Рудницький – Вісник Черкаського державного технологічного університету. Наукові праці ЧДТУ, 2004, №3. – С.96-100.

4. Рудницкий В.Н. Исследование кодов с постоянным числом единиц //В.Н. Рудницкий – Вісник черкаського державного технологічного університету. Наукові праці ЧДТУ, 2003, №3 – С.112-115.

5. Рудницький В.М., Пантєлєєва Н.М., Бабенко В.Г. Моделювання логічного пристрою для систем захисту інформації //В.М. Рудницький, Н.М. Пантєлєєва, В.Г. Бабенко – Українська академія банківської справи НБУ. Збірник наукових праць, 2006 – С.185-190.

6. Юпин Р.Е. Электронно-цифровая подпись / Р.Е. Юпин, А.Н. Приз //Тез. докл. ІСУЕП, 2004 р. – с.83.

СОДЕРЖАНИЕ

МАТЕМАТИКА

РАЗЛИКА И ВГРАЖДАМ ИЗРАВНЯВАНИЯ

ПРИЛОЖНАТА МАТЕМАТИКА

МАТЕМАТИЧЕСКИ АНАЛИЗ

ФИЗИКА

ГЕОФИЗИКА

ЛЕКАРСТВА НА ПОЛИМЕРИ

СЪВРЕМЕННИ ТЕХНОЛОГИИ НА ИНФОРМАЦИИ

КОМПЮТЪРНОТО ИНЖЕНЕРСТВО

ИНФОРМАТИВНАТА БЕЗОПАСНОСТ

ФИЗИЧЕСКА КУЛТУРА И СПОРТ

ФИЗИЧЕСКА КУЛТУРА И СПОРТ: ПРОБЛЕМИ, ПРОУЧВАНИЯ, ПРЕДЛОЖЕНИЯ

ПРОУЧЕТЕ НА ФИЗИЧЕСКАТА СПОСОБНОСТ ЗА РАБОТЕНЕ ЗА СПОРТИСТИТЕ