

Міністерство освіти і науки України  
Північно-Східний науковий центр НАН України та МОН України  
Національний університет  
«Полтавська політехніка імені Юрія Кондратюка»

# Тези

**73-ї наукової конференції професорів, викладачів,  
наукових працівників,  
аспірантів та студентів університету**

**Том 1**

**21 квітня – 13 травня 2021 р.**

Полтава 2021

загальному вигляді: нехай  $A = (a_1, \dots, a_n)$ ,  $B = (b_1, \dots, b_n)$ , тоді:

$$C = A \odot B = [(a_1 \odot b_1) \bmod m_1, (a_2 \odot b_2) \bmod m_2, \dots, (a_n \odot b_n) \bmod m_n]$$

Основні властивості НСЧ (незалежність залишків, рівноправність залишків, малорозрядність залишків) дозволяють усунути недоліки ПСЧ. За рахунок незалежності залишків за прийнятою системою основ, відкриваються широкі можливості в побудові не тільки нової машинної арифметики, але й принципово нової схемної реалізації КЗОД, котра, в свою чергу помітно розширює застосування машинної арифметики [4]. Це дає можливість широкого вибору варіантів системотехнічних рішень при реалізації модульних арифметичних операцій, заснованих за допомогою наступних методів (принципів):

- суматорний метод (на базі малорозрядних двійкових суматорів);
- табличний метод (на основі використання таблиць ПЗП);
- метод кільцевого зсуву, заснований на використанні кільцевих регістрів зсуву.

#### *Література*

1. Андреева Е., Фалина И. Системы счисления и компьютерная арифметика. - Учебное пособие.- БИНОМ, 2004.
2. Мельник А. О. Архитектура компьютера / А.О. Мельник. – Луцьк: Волинська обласна друкарня, 2008. –470 с.
3. Акушский И.Я. Машинная арифметика в остаточных классах / И. Я. Акушский, Д. И. Юдицкий. – М. : Советское радио, 1968. – 440 с.
4. Барсов В. И. Методы многоверсионной обработки информации в модулярной арифметике: моногр. / В. И. Барсов, В. А. Краснобаев, А. А. Сиора, И. В. Авдеев. – Х.: МОИ, УИПА, 2008. – 460 с.

**УДК 004.9**

*Г.В. Головка, к.т.н., доцент  
Р.В. Деменко, магістр*

*Національний університет  
«Полтавська політехніка імені Юрія Кондратюка»*

## **ВЕБ ДОДАТОК ТЮНІНГУ АВТОМІБІЛІВ**

З появою Web-технології комп'ютери починають використовувати абсолютно нові верстви населення Землі. Можна виділити дві найбільш характерні групи, що знаходяться на різних соціальних полюсах, які були стрімко залучені в нову технологію, можливо, навіть крім їх власного бажання. З одного боку, це були представники елітарних груп суспільства – керівники великих організацій, президенти банків, топ-менеджери, впливові державні чиновники тощо. З іншого боку, це були представники найширших верств населення – домогосподарки, пенсіонери, діти.

Спектр соціальних груп, що підключаються до мережі Інтернет і що шукають інформацію в WWW, весь час розширюється за рахунок користувачів, що не відносяться до категорії фахівців в області

інформаційних технологій. Це лікарі, будівельники, історики, юристи, фінансисти, спортсмени, мандрівники, священнослужителі, артисти, письменники, художники. Список можна продовжувати нескінченно. Той, хто відчув корисність і незамінність Мережі для своєї професійної діяльності або захоплені, приєднується до величезної армії споживачів інформації у «Всесвітній Павутині».

Web-технологія повністю перевернула наші уявлення про роботу з інформацією, та й з комп'ютером взагалі. Виявилось, що традиційні параметри розвитку обчислювальної техніки – продуктивність, пропускна здатність, ємність запам'ятовуючих пристроїв – не враховували головного «вузького місця» системи – інтерфейсу з людиною. Застарілий механізм взаємодії людини з інформаційною системою стримував впровадження нових технологій і зменшував вигоду від їх застосування. І тільки коли інтерфейс між людиною і комп'ютером був спрощений до природності сприйняття звичайною людиною, послідував безпрецедентний вибух інтересу до можливостей обчислювальної техніки.

Розвиток Інтернет-технологій послужило поштовхом до появи нової гілки в Інтернеті – Інтернет-форумів. Стали з'являтися сайти, і навіть цілі портали, на яких люди з усіх куточків планети можуть спілкуватися, отримувати відповіді на будь-які питання і, навіть, укладати ділові угоди.

Інформаційна система – це набір сторінок в форматі HTML, які лежать на Web-сервері.

Web-сервер – це постійно підключений до Інтернету комп'ютер, який передає ці сторінки за запитом користувачів.

Web-вузол – це набагато більше, ніж просто сукупність Web-сторінок. Це і система гіперпосилань, що зв'язує вузол в єдине ціле, і єдине стилістичне оформлення вузла, і своєчасне оновлення знаходиться інформації на вузлі, і швидкість завантаження окремих сторінок, і багато іншого.

Основна відмінність документів Web від звичайних електронних документів складається в наявності гіперпосилань. Гіпертекстові посилання дозволяють, переглядаючи документ Web, перейти до іншої його частини або іншим документом Web, або звернутися до однієї зі служб Інтернету. Як правило, частина тексту документа Web, відповідна гіперпосиланням, виділяється синім кольором або підкреслюється.

Тема «ВЕБ Додаток тюнінгу автомобілів» є в даний час особливо актуальною, так як, по-перше, зараз всі сервіси та магазини котрі стосуються автомобілів та не тільки, купують у розробників сайти для своїх компаній. По-друге маючи сайт зручніше предоставити клієнту всі свої послуги котрі ви надаєте. По третє, кожна поважна компанія має веб-додаток, де вона викладає свої роботи чи послуги. Об'єктом, дослідження в даній дипломній роботі є створення веб додатку для швидкого пошуку запчастин котрі потрібні для ремонту чи тюнінгу авто.

Данна робота поділена на декілька етапів розробки:

- створюється дизайн за допомогою графічних інструментів таких як Photoshop, Figma чи XD Design.
- вибирається мову програмування та середу розробки. В моєму

випадку мовою програмування буде HTML, CSS, PHP, JS та використання баз даних для збереження інформації. Середою розробки я надаю перевагу PhpStorm, це одна з найкращих програм для WEB розробника.

Перевіряється повністю сайт, щоб всі елементи відображались адекватно та при респонсиві не “ламали” наш сайт.

Звичайний дизайн з можливістю вибору саме вашого авто. На цьому сайті занадто застарілий дизайн.

Як на мене, то це самий гарний дизайн серед українських сайтів по тюнінгу авто.

Головним призначенням інформаційної системи є розміщення матеріалу для клієнтів та гостей, зручний пошук будь-якої інформації та зручна локалізація.

В ході виконання роботи реалізовано ряд функцій:

1. Створення нових сторінок, додавання новин через панель адміністратора.
2. Розроблення модуля, за допомогою якого дуже зручно додавати нових або редагувати вже існуючі.
3. Редагування матеріалу (новин, сторінок) через панель адміністратора.
4. Локалізація сайту на 2-х мовах.

**УДК 004.9**

*Г.В. Головка, к.т.н., доцент  
V. Pokhodun, магістр  
Національний університет  
«Полтавська політехніка імені Юрія Кондратюка»*

## **SOFTWARE IMPLEMENTATION OF THE DECODER BASED ON THE MMB ALGORITHM**

Cryptography is a ubiquitous tool in the world of information security. It is necessary to maintain the confidentiality of communications or to prove the authenticity of the message, it can be used to create various multi-party protocols in such a way that makes their circumvention, hacking or deception difficult and prohibitively expensive. In fact, the scope of cryptography is incredibly wide, and it would be impossible to compile a complete list of functionalities that can be achieved through its use.

Historically, the oldest and most important cryptographic goal is the confidentiality of information, and there are many methods and algorithms that can be used to achieve it. One of them is a modular multiplication-based block cipher - MMB.

The block encryption algorithm MMB was developed by Joan Daemen in 1993, and proposed as an alternative to the IDEA cipher. It was developed specifically to withstand differential cryptanalysis. Its main innovation was the use of cyclic multiplication in the group  $Z_{2^n-1}$ , where  $n$  is the length of one word within which operations will be performed. All internal MMB operations