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

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

Перевіряється повністю сайт, щоб всі елементи відображалися 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 серез 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. Головко, 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 Z2n-1, where n is the length of one word within witch operations will be performed. All internal MMB operations

are performed with n-bit words. The creators of the cipher suggested n = 32, so the multiplication occurs in the group Z232 - 1. The MMB cipher block has the structure of a Substitution-Permutation network (SP-network) and works in 128-bit text blocks, uses a 128-bit key and has six iterations. One round of MMB consists of four transformations

MMB operates with 32-bit text sub-blocks (x0, x1, x2, x3) and 32-bit key sub-blocks (k0, k1, k2, k3). This makes it convenient to implement the algorithm on 32-bit processors. Alternating with XOR, the nonlinear function f is used six times.

Algorithm:

xi = xi⊕ ki, for I = 0 to 3
f(x0, x1, x2, x3)
xi = xi⊕ ki+1, for I = 0 to 3
f(x0, x1, x2, x3)
xi = xi⊕ ki+2, for I = 0 to 3
f(x0, x1, x2, x3)
xi = xi⊕ ki, for I = 0 to 3
f(x0, x1, x2, x3)
xi = xi⊕ ki+1, for I = 0 to 3
f(x0, x1, x2, x3)
xi = xi⊕ ki+2, for I = 0 to 3
f(x0, x1, x2, x3)

Function f has three steps:

(1) xi=ci, for I= 0 to 3 (If input bits are all 1, then all output bits are also 1.)

(2) If least significant bit x0 = 1, then x0 = x0⊕ C. If least significant bit x3 = 1, then x3 = x3⊕ C.

(3) xi = xi-1⊕ xi⊕ xi+1, for I = 0 to 3

All index operations are performed as multiplication modulo 3. The operation in step (1) is performed as multiplication modulo 232-1. In this algorithm, if the second operand is 232-1, then the result is also 232-1. Algorithm uses constants:

C=2aaaaaaa
c0=025f1cdb
c1=2 * c0
c2=23 * c0
c3=27 * c0

Decryption is the reverse process.

Bibliography

1. Daemen, J., Govaerts, R., Vandewalle, J.: Block Ciphers Based on Modular Multiplication. In: Wolfowicz, W. (ed.) Proceedings of 3rd Symposium on State and Progress of Research in Cryptography, Fondazione Ugo Bordoni, pp. 80–89 (1993).

2. Daemen, J.: Cipher and Hash Function Design – Strategies based on Linear and Differential Cryptanalysis. PhD Thesis, Dept. Elektrotechniek, Katholieke Universiteit Leuven, Belgium (1995)