UDC 004.7 **doi: 10.26906/SUNZ.2021.3.078**

G. Golovko, V. Pokhodun

National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, Ukraine

ANALYSIS AND SOFTWARE IMPLEMENTATION OF MODULAR MULTIPLICATION-BASED BLOCK CIPHER

Abstract. This article highlights the ever-increasing need and importance of information protection and data safety in modern reality, presents the possibilities of encrypting data using the tools of cryptography, particularly concentrating on the Modular Multiplication-based Block Cipher. Review of available sources indicated that there are no publically accessible software implementations of the algorithm available at the moment of writing this article. To achieve a goal of creating such an implementation, information has been compiled for creating a comprehensible and adequate mathematical description of the algorithm. Presented the information security system, an application in C # to encrypt files of any extension using the block encryption algorithm MMB.

Keywords: MMB, information protection, information security, cryptography, complex methods of information protection, encryption.

Introduction

Cryptography is an integral part of the information security world. It is necessary whenever the secrecy of communications is required to be kept or when authenticity of an incoming message needs to be proven. It can be used for developing multiple multi-party protocols in such a way, that makes its surpassing, cracking or cheating extremely difficult and prohibitively expensive [1]. In fact, range of application of cryptography is astoundingly wide and it would have been impossible to compile any remotely complete list of all the functional abilities that can be achieved through its use.

Historically, the oldest and the main aim of cryptography is confidentiality of the information and there is a variety of methods and algorithms existing that can be used for reaching such a goal. One of them is the Modular Multiplication-based Block Cipher, also known as MMB.

The research purpose. Study of mechanisms and algorithms for personal data protection with further development of a software product that provides an interface for reliable encryption of confidential information and becomes an easily accessible public implementation of an MMB cipher, which at the moment there is a lack of. Mathematical formalization of algorithms, implementation of encryption algorithms, substantiation of reliability of use, application of algorithm.

Literature review. When analyzing issues related to information security, it is necessary to take into account the specifics of this aspect of security such as it being an integral part of information technology - an area that is developing at an unprecedented rate. What is important here is not so much individual solutions (laws, training courses, software and hardware) that are at the current level, but mechanisms for generating new solutions that allow to live in the pace of technological progress.

With an increasing effect information has on our life, so does its protection increasingly become a much more prominent recurring topic in a variety of scientific research. This applies to cryptography. But, interestingly enough, it can be quite a challenging task to find information on a specific method or algorithm, especially if it’s less used comparatively to some other more popular ones.

Majority of information about MMB cipher can be found in the works of its creator himself, Joan Daemen [2], but there are also works by other authors, such as Wang M., Nakahara J., Sun Y [3] and Bruce Schneier [4].

After a thorough review and analysis, we can conclude that there are no easily available public implementations of MMB cipher in any of the popular programming languages, further supporting the importance of the goals set by this work.

Research results

Block cipher of MMB has been created by Joan Daemen[5] back in 1993 and was proposed as an alternative to the IDEA cipher[6]. MMB was developed specifically to withstand the differential cryptanalysis [7]. Its main innovation has become the use of cyclical multiplication inside of the $Z_2{}^{n}{}_{-1}$ group, where *n* – is the length of a single word on which operations will be performed upon. All internal operation in MMB are performed with *n*-bit words. The creators of the cipher proposed *n* = 32, thus multiplication are made inside the $Z_{2^{32}-1}$ range. It is also worth mentioning that

$$2^{32}-1 = (2^{16}+1)\cdot(2^{8}+1)\cdot(2^{4}+1)\cdot(2^{12}+1)\cdot(2^{3}+1) =$$
$$= 65537\cdot 257\cdot 17\cdot 5\cdot 3 = 4294967295,$$

product of all the Fermat numbers. MMB is an iterative cipher, which consists of six rounds. MMB operates with 128-bit text sub-blocks and uses a 128-bit key. Flowchart of the algorithm is presented in Fig. 1.

MMB operates with 32-bit sub-blocks of text (x_0, x_1, x_2, x_3) and 32-bit sub-blocks of key (k_0, k_1, k_2, k_3). This makes it convenient to implement the algorithm on the 32-bit processors. Iterating with XOR operation, the non-linear function *f* is performed six times.

The algorithm:

```
$x_i = x_i \oplus k_i$, for I = 0 to 3
$f(x_0, x_1, x_2, x_3)$
$x_i = x_i \oplus k_{i+1}$, for I = 0 to 3
$f(x_0, x_1, x_2, x_3)$
```

$x_i = x_i \oplus k_{i+2}$, *for I = 0 to 3*
$f(x_0, x_1, x_2, x_3)$
$x_i = x_i \oplus k_i$, *for I = 0 to 3*
$f(x_0, x_1, x_2, x_3)$
$x_i = x_i \oplus k_{i+1}$, *for I = 0 to 3*
$f(x_0, x_1, x_2, x_3)$
$x_i = x_i \oplus k_{i+2}$, *for I = 0 to 3*
$f(x_0, x_1, x_2, x_3)$

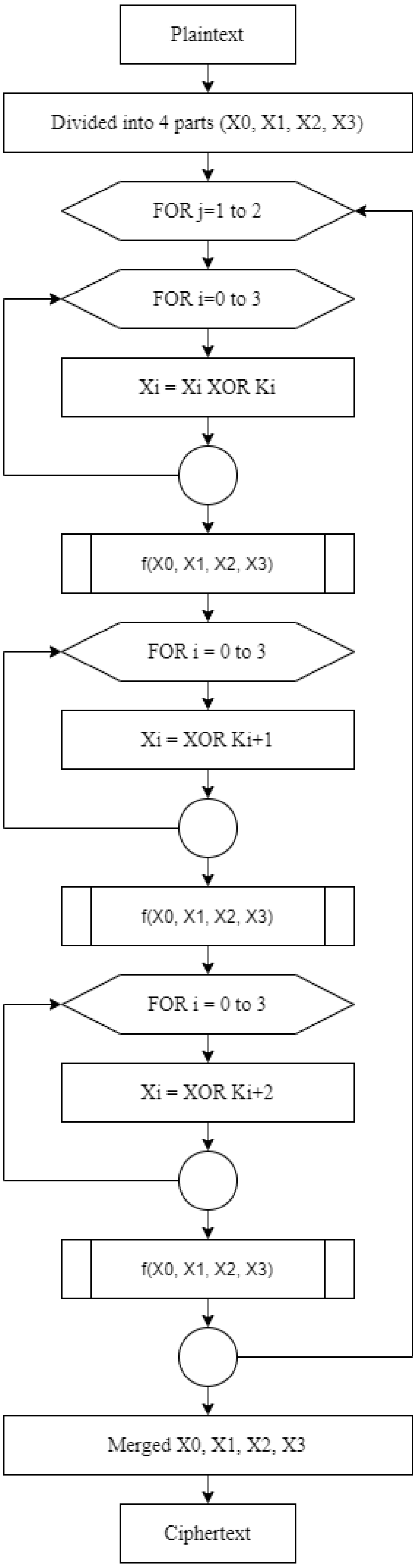


Fig. 1. MMB algorithm flowchart

Function *f* has three stages:

(1) $x_i = c_i$, for I = 0 to 3 (If all bits of input are 1, then outputs bits are also all 1)

(2) If the least significant bit $x_0 = 1$,
then $x_0 = x_0 \oplus$ C.
If the least significant bit $x_3 = 1$, then $x_3 = x_3 \oplus$ C.

(3) $x_i = x_{i-1} \oplus x_i \oplus x_{i+1}$, for I = 0 to 3

All indexed operations are performed by the module 3. Multiplications at the stage (1) are performed by the module 2^{32}-1.

In this algorithm if the second operand = 2^{32}-1, then result is also 2^{32}-1.

Constants used:

C=2aaaaaaa;

c_0=025flcdb;

$c_1=2 * c_0$;

$c_2=2^3 * c_0$;

$c_3=2^7 * c_0$.

The constant C is the "simplest" constant with a high ternary weight, zero least significant bit and no circular symmetry.

The constant c_0 has slightly different characteristics. Other constants are offset versions of c_0, and are used to prevent symmetry-based disclosure.

Decryption is the reverse process.

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: j:

- $\sigma[k^j]$: exclusive disjunction is applied to each data word with sub-key block k^j, where j is the index of the round. The formal representation is represented in formula (1), where $\oplus$ means bitwise exclusive disjunction, $a_i, k_i^j \in \mathbb{Z}_{2^{32}}$ for $0 \le i \le 3$.

The operation $\sigma[k^j]$ is an involution and is the only operation that depends on key in the round.

$$\sigma[k^j](a_0,a_1,a_2,a_3) = \left(a_0 \oplus k_0^j, a_1 \oplus k_1^j, a_2 \oplus k_2^j, a_3 \oplus k_3^j\right) \quad (1)$$

- γ: modular multiplication of each word of data with fixed 32-bit constants Gi (Formula 2), where

$a \otimes b = a * b \bmod (2^{32} - 1)$,
G0 = 025F1CDBx,
$G1 = 2 \otimes G0$ = 04BE39B6x,
$G2 = 8 \otimes G0$ = 12F8E6D8x,
$G3 = 128 \otimes G0$ = 2F8E6D81x,

which can be efficiently calculated because

$$(A * 2^x) \bmod (2^{32} - 1) = (A \ll x) \bmod (2^{32} - 1).$$

In multiplication modulo 2^{32} - 1, a wrapping effect is observed, because $2^{32} \equiv 1 \bmod (2^{32} - 1)$, which means that the bits on the (32 + i)-th LSB (lower bit) position are shifted to the i-th position of the LSB.

This effect is similar to the multiplication operation modulo $2^{16}+1$ in IDEA.

The whole operation can also be described by formula 3.

$$\gamma(a_0,a_1,a_2,a_3) = (a_0 \oplus G_0, a_1 \oplus G_1, a_2 \oplus 2, a_3 \oplus G_3)\ (2)$$

$$a \otimes b = a * b \bmod (2^{32}-1) = \left(a * b \bmod 2^{32} + \left\lfloor \frac{a * b}{2^{32}} \right\rfloor\right) \bmod (2^{32}-1)\ (3)$$

Note that γ is inverse but not involution. Each 32-bit multiplication can be interpreted as a huge 32 × 32-bit S-block, because one of the operands in the multiplication is always fixed. For any Gi there are two fixed points: 0 ⊗ Gi = 0, and $(2^{32} - 1) \otimes \mathrm{Gi} = 2^{32} - 1$.

- η: data-dependent transformation that works on two of the four inputs of the word (a_0,a_1,a_2,a_3) (Formula 4), where 'lsb' denotes the least significant (least significant) bit, and δ = 2aaaaaaax; η is an involution and a nonlinear operation.

$$\eta(a_0,a_1,a_2,a_3) = \big(a_0 \otimes (\mathrm{lsb}(a_0) * \delta), a_1, a_2, a_3 \otimes (1 \otimes \mathrm{lsb}(a_3) * \delta)\big)(4)$$

- θ: the sole diffusion operation in MMB (Formula 5), where $a_i \in \mathrm{Z}_{2^{32}}$, at 0 ≤ i ≤ 3. θ – involution

$$\theta(a_0,a_1,a_2,a_3) = (a_3 \otimes a_0 \otimes a_1, a_0 \otimes a_1 \otimes a_2, a_1 \otimes a_2 \otimes a_3, a_2 \otimes a_3 \otimes a_0)(5)$$

There are two pairs of operations that can be interchangeable:

$(\theta, \sigma[k^j])$ and $(\eta, \sigma[k^j])$.

In each case, the key k^j is converted into an equivalent key $\theta(k^j)$ or $\eta(k^j)$, respectively.

The J-th (full) round of MMB transformation can be represented by formula 6.

$$\rho[k^j](X) = \theta \circ \eta \circ \gamma \circ \sigma[k^j](X) = \theta\left(\eta\left(\gamma\left(\sigma[k^j](X)\right)\right)\right)(6)$$

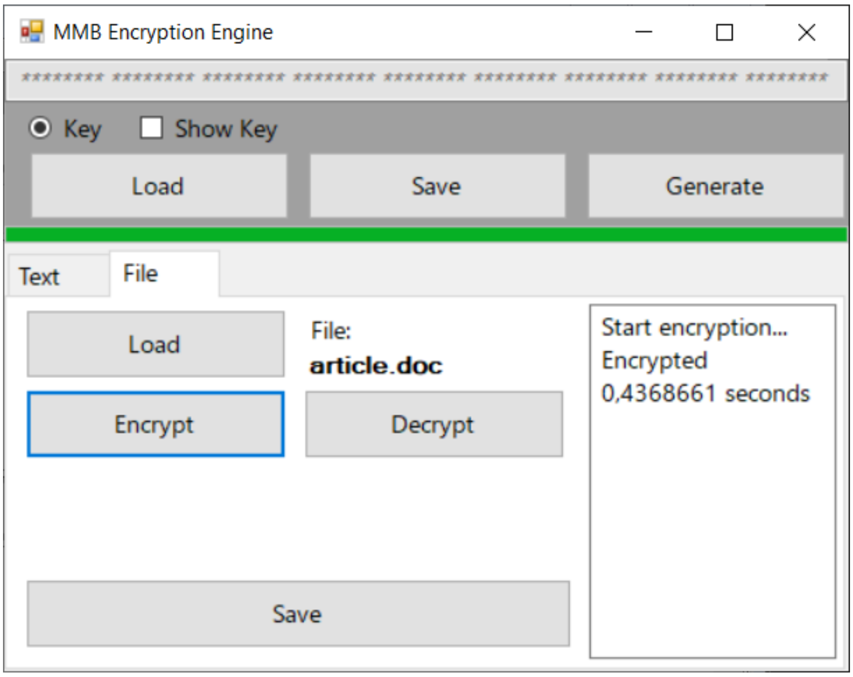
The complete process of encrypting plaintext P by the MMB algorithm is presented in formula 7.

$$\mathrm{MMB}(P) = \sigma[k^6] \circ \rho[k^5] \circ \rho[k^4] \circ \rho[k^3] \circ \rho[k^2] \circ \rho[k^1] \circ \sigma[k^0](P)(7)$$

The C # programming language was chosen to implement the MMB cipher because it has the necessary set of tools for working with ciphers, and based on experience.

Example of GUI is presented in Fig. 2.

By reading files directly as bit strings, application is capable of encrypting and decrypting data of any extension.



```
Start encryption...
Encrypted
0,4368661 seconds
```

Fig. 2. GUI of a developed encryption system

A custom format was developed to create, store and utilize required cryptographic keys.

The program successfully utilizes the MMB algorithm to perform inverse encryption and decryption operations with all expected properties:

reliability,
robustness,
retaining cryptographic strength;
fast execution time.

Conclusions

People tend to protect their secrets. The development of information technologies, their penetration into all spheres of human activity leads to the fact that the problems of information security are becoming more and more relevant every year - and at the same time more and more complex.

Therefore, information security is often considered as a set of informal recommendations for building information security systems of one type or another. However, the practical methods of building protection systems are general laws that do not depend on the technical features of their implementation.

In the course of the work a number of sources were studied.

Presented mathematical formalization of algorithm, implementation of encryption algorithm, substantiation of reliability of use, application of algorithm.

Information security system, an application in C # to encrypt files of any extension using the block encryption algorithm MMB was developed, in particular:

- Analyzed subject area;
- The general architecture of the program was developed;
- The created program was tested;
- The program is successfully implemented.

Reference

1. A. Joux, Algorithmic Crypanalysis, United States: CRC Press, 2009.
2. Daemen, J., Van Linden, L., Govaerts, R., Vandewalle, J.: Propagation Properties of Multiplication Modulo $2^n - 1$. In: Proceedings of the 13th Symposium on Information Theory in the Benelux, Werkgemeenschap voor informatie- en Communicatietheorie, Enschede, The Netherlands, pp. 111–118 (1992)
3. Wang M., Nakahara J., Sun Y. (2009) Cryptanalysis of the Full MMB Block Cipher. In: Jacobson M.J., Rijmen V., Safavi-Naini R. (eds) Selected Areas in Cryptography. SAC 2009. Lecture Notes in Computer Science, vol 5867. Springer, Berlin, Heidelberg.
4. Bruce Schneier. Applied Cryptography (2nd Ed.): Protocols, Algorithms, and Source Code in C. John Wiley & Sons, Inc., USA, 1995.
5. Daemen, J., Govaerts, R., Vandewalle, J.: Block Ciphers Basedon 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).
6. Lai, X.: On the Design and Security of Block Ciphers. In: Massey, J.L. (ed.) ETH Series in Information Processing, vol. 1. Hartung-Gorre Verlag, Konstanz (1995)
7. Daemen, J.: Cipher and Hash Function Design – Strategies based on Linear and Differential Cryptanalysis. PhD Thesis, Dept. Elektrotechniek, Katholieke Universiteit Leuven, Belgium (1995)

Received (Надійшла) 13.07.2021
Accepted for publication (Прийнята до друку) 25.08.2021

Аналіз та програмна реалізація модульного блокового шифру на основі множення

Г. Головко, В. Походун

Анотація. Людям властиво захищати свої секрети. Розвиток інформаційних технологій, їх проникнення у всі сфери людської діяльності призводить до того, що проблеми інформаційної безпеки з кожним роком стають все більш і більш актуальними – і водночас дедалі складнішими Технології обробки інформації безперервно удосконалюються, а разом з ними змінюються і практичні методи забезпечення інформаційної безпеки. Безперечно, універсальних методів захисту не існує, багато в чому успіх при побудові механізмів безпеки для реальної системи залежатиме від її індивідуальних особливостей, облік яких погано піддається формалізації. Тому часто інформаційну безпеку розглядають як певну сукупність неформальних рекомендацій по побудові систем захисту інформації того або іншого типу. Однак за практичними прийомами побудови систем захисту лежать загальні закономірності, які не залежать від технічних особливостей їх реалізації. У цій статті висвітлюється постійно зростаюча потреба та важливість захисту інформації та безпеки даних у сучасних реаліях, представлені можливості шифрування даних за допомогою інструментів криптографії, особливо зосереджуючись на модульному блочному шифрі на основі множення. Огляд доступних джерел показав, що на момент написання цієї статті немає загальнодоступних програмних реалізацій алгоритму. Для досягнення мети створення такої реалізації була зібрана інформація для компіляції зрозумілого та адекватного математичного опису алгоритму. Представлена практична розробка системи захисту інформації, додаток на C # для шифрування файлів будь -якого розширення за допомогою алгоритму шифрування MMB.

Ключові слова: MMB, захист інформації, інформаційна безпека, криптографія, комплексні методи захисту інформації, шифрування.