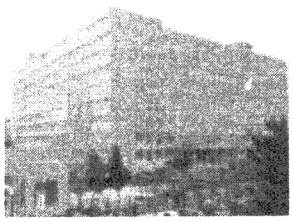
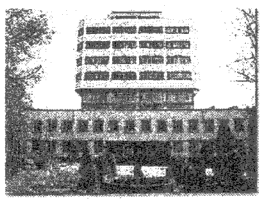
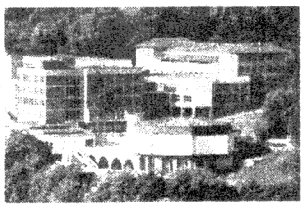
BAKU STATE UNIVERSITY

VINNYTSIA NATIONAL TECHNICAL UNIVERSITY

St. CYRIL and St. METHODIUS UNIVERSITY of VELIKO TURNOVO

Proceedings of the Forth International Conference

INTERNET EDUCATION SCIENCE

IES-2004

Volume 2

NEW INFORMATIONAL AND COMPUTER TECHNOLOGIES IN EDUCATION AND SCIENCE

AZERBAIJAN – UKRAINE – BULGARIA

September 28 – October 16, 2004

УДК 378 + 681.324
І73

Друкується за рішенням Ученої ради Вінницького національного технічного університету Міністерства освіти і науки України

Відповідальний за випуск *В. В. Грабко*

Підготовлено до друку: *В. В. Грабко, В. І. Месюра, І. Р. Арсенюк, В. В. Седлецький, О. А. Дячок*

І73 **«ІНТЕРНЕТ — ОСВІТА — НАУКА — 2004», четверта міжнародна конференція ІОН — 2002**, 28 вересня — 16 жовтня, 2004 р. Збірник матеріалів конференції. Том 2. — Вінниця: УНІВЕРСУМ-Вінниця, 2004. — 380 с.

ISBN 966-641-104-0 (том 2)

Четверта міжнародна конференція «ІНТЕРНЕТ — ОСВІТА — НАУКА — 2004» (ІОН — 2004) присвячена обговоренню питань застосування в освіті та наукових дослідженнях нових інформаційних технологій, що спираються на можливості Інтернет.

УДК 378 + 681.324

Доповіді у збірнику згруповані по секціях, відповідно до основних напрямків конференції:

Том1:

- **A** Інтернет та інформаційні технології в освіті та наукових дослідженнях
- **B** Методологія та практика дистанційної освіти
- **C** Соціальні та психологічні аспекти використання інформаційних технологій

Том 2:

- **D** Корпоративні мережі і розподілені системи керування
- **E** Інтелектуальні комп'ютерні системи
- **F** Телекомунікаційні технології для Інтернет

Матеріали доповідей представлені також на Web-сайті конференції (http:/www.vstu.vinnica.ua/ies2004), що містить електронну версію даного збірника доповнену наданими авторами перекладами окремих доповідей, і базу даних з відомостями про учасників конференції.

Тексти доповідей друкуються в авторській редакції.

ISBN 966-641-102-4 (загальний)
ISBN 966-641-104-0 (том 2)

ALGORITHM OF BLOCK SYMMETRIC ENCODING BASED ON ARITHMETIC OPERATIONS MODULO 2^N

Vitaly Sokiruk, Vladimir Luzhetsky

Vinnytsia National Technical University
Khmelnitske Shose, 95, Vinnytsia, 21021, Ukraine, Tel.: (0432-44-03-86)

Abstract

The algorithm of block symmetric encoding is based on principles, which were not used at construction of block ciphers earlier, is offered. The main idea is that arithmetic operations, which are effectively realized on modern processors, are used. Blocks of information and private keys are considered as n-bit integers. Above these numbers operations of multiplication, division, addition and subtraction modulo 2n, where n - a block size are carried out.

The offered algorithm has simple mathematical structure and possesses a high speed, as arithmetic operations modulo 2n are natural and fast for modern computers and hardware. The algorithm takes into account modern tendencies of computer evolution, namely: increases of processor's word width and extensions of machine instructions for efficient big number arithmetic implementation.

Introduction

Symmetric-key block ciphers are the very important elements in many cryptographic systems. They are widely applied to data protection in modern information community. They solve a big number of modern cryptographic tasks. Block ciphers are used for enciphering great volumes of data where the high speed of the algorithm is extremely important. They also applied for enciphering of important confidential information where using of strengthened methods of protection is required. To modern block ciphers high requirements are put forward. They should possess high speed and universality, support operating modes for different levels of cryptographic security and, accordingly, the different block and key sizes, have simple hardware implementation, etc. [1].

The majority of known block ciphers are constructed on principles, which have been incorporated by developers of algorithm DES in the beginning of 70th years. The information block is considered as a set of bits and partitioned to the separate groups called subblocks. The cipher has iterative structure, on each round repeating simple logical and arithmetic operations are carried out. Such way achieves confusion and diffusion of a plain text bits [2]. That structure is oriented, first of all, to the simple hardware implementation. Program implementations of such algorithms are usually ineffective, as provide execution of a plenty of operations on separate bits.

Modern processors are able to carry out arithmetic and logic operations on 32- and 64-bit numbers very effectively. Besides there are a lot of extended machine instructions for execution of operations above the big numbers. The word width of processors increases, therefore block ciphers should take into account this tendency. The offered algorithm uses possibilities of modern computers maximum effectively.

Information blocks and private keys in algorithm are considered as n-bit integers, where n - length of the block. So in this algorithm arithmetic operation modulo 2^n, which can be efficiently implemented in hardware and software, are used. All operations are executed under the control of secret key, which are portioned to four n-bit subkeys.

Operations of multiplication and division modulo 2^n

Let $Z_m = \{0,1,2,...,m-1\}$ is a set of all positive integer numbers. The operation of multiplication of numbers $A, B \in Z_m$ modulo m is described by such expression:

$$A \cdot B \equiv C \pmod{m} \tag{1}$$

Let's assume, the result of multiplication modulo m and one of multipliers, for example, number B are known. Then for finding unknown multiplier A is necessary to perform the operation of division modulo m:

$$A = \left(\frac{C}{B}\right)_{\bmod m} = \left(C \cdot \frac{1}{B}\right)_{\bmod m} = \left(C \cdot \left(\frac{1}{B}\right)_{\bmod m}\right)_{\bmod m} \tag{2}$$

From a number theory it is known [3], that the equation (2) has single solution only if a number $\left(\frac{1}{B}\right)_{\bmod m}$ exists, that satisfying:

$$\gcd(B,m) = 1 \tag{3}$$

For calculation of number $\left(\frac{1}{B}\right)_{\mathrm{mod}\, m}$ extended Euclidian algorithm [3] can be used. It is known, that its implementation for the big numbers is difficult.

If we use the number 2^n as m, it is possible to essentially simplify operations of multiplication and division modulo m. In the case of such modulus usage, the operation of division (2) provides unique solution when number K is odd positive integer number, so the condition (3) satisfies.

Known algorithms of multiplication modulo consist of operations, which realize directly multiplication, and operations, which determine a remainder of division of result (intermediate or final) on modulus value [3]. The feature of implementation of the operation of multiplication modulo 2^n is that additional arithmetic operations are not longer needed for obtaining the rests. It is enough to discard digits of bits which have numbers bigger than n. It essentially simplifies implementation of the operation of multiplication modulo 2^n.

The most known algorithm of multiplication is algorithm of multiplication "in a column" with sequential multiplications and distribution of carries from low order to high order positions. It allows presenting of big integer numbers multiplication as a sequence of operations on smaller numbers.

For the implementation of division modulo 2^n operation there is fast and simple algorithm too. Let's write n-bit integers A and B in binary representation where the rightmost bit is the less significant bit. So, $A = \{a_{n-1}, a_{n-2}, ..., a_0\}$ and $B = \{b_{n-1}, b_{n-2}, ..., b_0\}$. The result of multiplication of these numbers modulo 2^n is n low order bits of number C which values are determined as:

$$\begin{cases} c_0 = a_0 b_0, \\ c_1 = a_1 b_0 + a_0 b_1, \\ c_2 = a_2 b_0 + a_1 b_1 + a_0 b_2, \\ \ldots \\ c_{n-1} = a_{n-1} b_0 + a_{n-2} b_1 + \ldots + a_0 b_{n-1}. \end{cases} \quad (4)$$

Let the result of multiplication of these numbers modulo 2^n and multiplier B is known. As coefficients $b_0, b_1, ..., b_{n-1}$ and $c_0, c_1, ..., c_{n-1}$ are known, we have the system from n equations with n variables. To comply with a condition (3) number B should be odd integer, that is $b_0 = 1$. So it is possible to write a set of equations for finding bits of unknown number A:

$$\begin{cases} a_0 = c_0, \\ a_1 = c_1 - a_0 b_1, \\ a_2 = c_2 - a_1 b_1 - a_0 b_2, \\ \ldots \\ a_{n-1} = c_{n-1} - a_{n-2} b_1 - \ldots - a_0 b_{n-1}. \end{cases} \quad (5)$$

The process of solution system (5) is reduced to the procedure of sequential definition of digits a_i. It is similar to how it is made during usual division. Difference will consist only that firstly determines digit of the low order bits, instead of the high order. As $b_0 = 1$, the rightmost bit of multiplier A is equal to appropriate bit of number C. Substituting value a_0 in the second equation of the system, we can calculate value a_1. Then we substitutes values a_0 and a_1 in the third equation of the system and find value a_2. Similarly it is possible to determine digits of other unknown bits a_3... a_{n-1}.

Encryption and decryption

The procedure of encryption consists in conversion of the block of a plain text M into the block of cipher text C under the control of a private subkeys K_1-K_4.

The operation of encryption is represented by expression

$$C = \left(\left(\left(\left(M \times K_1\right)_{\mathrm{mod}\, 2^n} \oplus K_2\right) \times K_3\right)_{\mathrm{mod}\, 2^n} + K_4\right)_{\mathrm{mod}\, 2^n} \quad (6)$$

It consists of two operations of multiplication modulo 2^n, one operation of addition modulo 2^n, and also operation of addition modulo 2. It is known that integer multiplication is a very effective "diffusion" primitive [4]. Thus the operations of multiplication provide confusion and diffusion of plain text M bits. The operation of addition modulo 2 and subkey K_4 are used for preventing known-plaintext attacks, when plaintext-ciphertext pairs are available.

For restoring the block of plain text M from the block of cipher text C it is necessary to perform inverse arithmetic operations, that is:

$$M = \left(\left(\left(\left(C - K_4\right)_{\mathrm{mod}\,2^n} / K_3\right)_{\mathrm{mod}\,2^n} \oplus K_2\right) / K_1\right)_{\mathrm{mod}\,2^n} \qquad (7)$$

The operation of encryption consists of two operations of division modulo 2^n, operation of subtraction modulo 2^n, and operation of addition modulo 2.

The necessary and sufficient condition of assured and unique playback of the plain text block M is choosing such subkeys K_1 and K_3, which are odd integers.

Conclusions

The algorithm of block symmetric encoding with usage of arithmetic operations modulo 2^n is offered. All operations in algorithm are carrying out on entire blocks, which are represented as n-bit integers. Operations of encryption and decryption use four n-bit private subkeys and a small amount of arithmetic and logic operations.

The algorithm can be effectively realized both on modern computers, and in the hardware. Its construction allows using additional possibilities of modern processors for fast execution of arithmetic operations on big integer numbers.

The block size n is not limited and can be selected arbitrary from reasons of required speed and cryptography security. Algorithms of bit number arithmetic are universal and can be used for numbers of any sizes. For effective program and hardware implementation the value n should be multiple to machine word size.

References:

[1] A.V.Poty, O.I. Oleshko. New demands and principles of development of modern block encryption algorithms (by results of the analysis of algorithms - candidates in AES) // Open information and computer technologies. 2000. Vol. 12. With. 30-45.

[2] William Stollings. Cryptography and protection of networks: principles and practice, 2 edition.-:"Williams", 2001. - 672c.

[3] Petrov A.A.Computer safety. Cryptography methods of protection.-:DMK, 2000. - 448c.

[4] Ronald L. Rivest, M.J.B. Robshaw, R. Sidney, and Y.L. Yin. The RC6 Block Cipher, version 1.1 – 06.1998