Отчет

**об информационном поиске**

Заявитель: Горшунов А.И.

A. Области поиска:

*Страны: US*

*Период: 1976-2012*

B. Поисковый запрос:

**Query**[**[Help]**](http://www.uspto.gov/patft/help/helpbool.htm)

**Term 1:** Rivest Ronald in **Field 1:** Inventor Name

**Term 2:** Cryptography algorithm in **Field 2:** All Fields

**Select years**

1976 to present [full-text]

|  |
| --- |
| C. Результаты поиска: |

*Searching US Patent Collection...*

**Results of Search in US Patent Collection db for:  
IN/"Rivest Ronald" AND "Cryptographic algorithm"**: 11 patents.   
*Hits****1****through****11****out of****11***

Документы, относящиеся к предмету поиска:

|  |  |  |  |
| --- | --- | --- | --- |
|  | **PAT. NO.** |  | **Title** |
| 1 | [7,502,467](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=1&f=G&l=50&co1=AND&d=PTXT&s1=%22Rivest%3B+Ronald%22.INNM.&OS=IN/%22Rivest;+Ronald%22&RS=IN/%22Rivest;+Ronald%22) | Full-Text | [System and method for authentication seed distribution](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=1&f=G&l=50&co1=AND&d=PTXT&s1=%22Rivest%3B+Ronald%22.INNM.&OS=IN/%22Rivest;+Ronald%22&RS=IN/%22Rivest;+Ronald%22) |
| 2 | [7,363,494](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=2&f=G&l=50&co1=AND&d=PTXT&s1=%22Rivest%3B+Ronald%22.INNM.&OS=IN/%22Rivest;+Ronald%22&RS=IN/%22Rivest;+Ronald%22) | Full-Text | [Method and apparatus for performing enhanced time-based authentication](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=2&f=G&l=50&co1=AND&d=PTXT&s1=%22Rivest%3B+Ronald%22.INNM.&OS=IN/%22Rivest;+Ronald%22&RS=IN/%22Rivest;+Ronald%22) |
| 3 | [6,985,583](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=3&f=G&l=50&co1=AND&d=PTXT&s1=%22Rivest%3B+Ronald%22.INNM.&OS=IN/%22Rivest;+Ronald%22&RS=IN/%22Rivest;+Ronald%22) | Full-Text | [System and method for authentication seed distribution](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=3&f=G&l=50&co1=AND&d=PTXT&s1=%22Rivest%3B+Ronald%22.INNM.&OS=IN/%22Rivest;+Ronald%22&RS=IN/%22Rivest;+Ronald%22) |
| 4 | [6,970,070](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=4&f=G&l=50&co1=AND&d=PTXT&s1=%22Rivest%3B+Ronald%22.INNM.&OS=IN/%22Rivest;+Ronald%22&RS=IN/%22Rivest;+Ronald%22) | Full-Text | [Method and apparatus for selective blocking of radio frequency identification devices](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=4&f=G&l=50&co1=AND&d=PTXT&s1=%22Rivest%3B+Ronald%22.INNM.&OS=IN/%22Rivest;+Ronald%22&RS=IN/%22Rivest;+Ronald%22) |
| 5 | [6,269,163](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=5&f=G&l=50&co1=AND&d=PTXT&s1=%22Rivest%3B+Ronald%22.INNM.&OS=IN/%22Rivest;+Ronald%22&RS=IN/%22Rivest;+Ronald%22) | Full-Text | [Enhanced block ciphers with data-dependent rotations](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=5&f=G&l=50&co1=AND&d=PTXT&s1=%22Rivest%3B+Ronald%22.INNM.&OS=IN/%22Rivest;+Ronald%22&RS=IN/%22Rivest;+Ronald%22) |
| 6 | [5,835,600](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=6&f=G&l=50&co1=AND&d=PTXT&s1=%22Rivest%3B+Ronald%22.INNM.&OS=IN/%22Rivest;+Ronald%22&RS=IN/%22Rivest;+Ronald%22) | Full-Text | [Block encryption algorithm with data-dependent rotations](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=6&f=G&l=50&co1=AND&d=PTXT&s1=%22Rivest%3B+Ronald%22.INNM.&OS=IN/%22Rivest;+Ronald%22&RS=IN/%22Rivest;+Ronald%22) |
| 7 | [5,724,428](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=7&f=G&l=50&co1=AND&d=PTXT&s1=%22Rivest%3B+Ronald%22.INNM.&OS=IN/%22Rivest;+Ronald%22&RS=IN/%22Rivest;+Ronald%22) | Full-Text | [Block encryption algorithm with data-dependent rotations](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=7&f=G&l=50&co1=AND&d=PTXT&s1=%22Rivest%3B+Ronald%22.INNM.&OS=IN/%22Rivest;+Ronald%22&RS=IN/%22Rivest;+Ronald%22) |
| 8 | [5,144,667](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=8&f=G&l=50&co1=AND&d=PTXT&s1=%22Rivest%3B+Ronald%22.INNM.&OS=IN/%22Rivest;+Ronald%22&RS=IN/%22Rivest;+Ronald%22) | Full-Text | [Method of secure remote access](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=8&f=G&l=50&co1=AND&d=PTXT&s1=%22Rivest%3B+Ronald%22.INNM.&OS=IN/%22Rivest;+Ronald%22&RS=IN/%22Rivest;+Ronald%22) |
| 9 | [4,691,299](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=9&f=G&l=50&co1=AND&d=PTXT&s1=%22Rivest%3B+Ronald%22.INNM.&OS=IN/%22Rivest;+Ronald%22&RS=IN/%22Rivest;+Ronald%22) | Full-Text | [Method and apparatus for reusing non-erasable memory media](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=9&f=G&l=50&co1=AND&d=PTXT&s1=%22Rivest%3B+Ronald%22.INNM.&OS=IN/%22Rivest;+Ronald%22&RS=IN/%22Rivest;+Ronald%22) |
| 10 | [4,405,829](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=10&f=G&l=50&co1=AND&d=PTXT&s1=%22Rivest%3B+Ronald%22.INNM.&OS=IN/%22Rivest;+Ronald%22&RS=IN/%22Rivest;+Ronald%22) | Full-Text | [Cryptographic communications system and method](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=10&f=G&l=50&co1=AND&d=PTXT&s1=%22Rivest%3B+Ronald%22.INNM.&OS=IN/%22Rivest;+Ronald%22&RS=IN/%22Rivest;+Ronald%22) |
| 11 | [4,376,299](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=11&f=G&l=50&co1=AND&d=PTXT&s1=%22Rivest%3B+Ronald%22.INNM.&OS=IN/%22Rivest;+Ronald%22&RS=IN/%22Rivest;+Ronald%22) | Full-Text | [Data center for remote postage meter recharging system having physically secure encrypting apparatus and employing encrypted seed number signals](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=11&f=G&l=50&co1=AND&d=PTXT&s1=%22Rivest%3B+Ronald%22.INNM.&OS=IN/%22Rivest;+Ronald%22&RS=IN/%22Rivest;+Ronald%22) |

Данные ссылки начинаем проверять с конца списка, т.к. сортируются документы в порядке убывания даты, т.е. наиболее свежие патенты будут первыми в списке.

Уже вторая ссылка является тем, что мы искали. [Cryptographic communications system and method](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=10&f=G&l=50&co1=AND&d=PTXT&s1=%22Rivest%3B+Ronald%22.INNM.&OS=IN/%22Rivest;+Ronald%22&RS=IN/%22Rivest;+Ronald%22)

D. Метаданные патента:

|  |  |
| --- | --- |
| **United States Patent** | **4,405,829** |
| **Rivest ,   et al.** | **September 20, 1983** |

Cryptographic communications system and method 

**Abstract**

A cryptographic communications system and method. The system includes a communications channel coupled to at least one terminal having an encoding device and to at least one terminal having a decoding device. A message-to-be-transferred is enciphered to ciphertext at the encoding terminal by first encoding the message as a number M in a predetermined set, and then raising that number to a first predetermined power (associated with the intended receiver) and finally computing the remainder, or residue, C, when the exponentiated number is divided by the product of two predetermined prime numbers (associated with the intended receiver). The residue C is the ciphertext. The ciphertext is deciphered to the original message at the decoding terminal in a similar manner by raising the ciphertext to a second predetermined power (associated with the intended receiver), and then computing the residue, M', when the exponentiated ciphertext is divided by the product of the two predetermined prime numbers associated with the intended receiver. The residue M' corresponds to the original encoded message M.

|  |  |
| --- | --- |
| **Inventors:** | **Rivest; Ronald L.** (Belmont, MA)**, Shamir; Adi** (Cambridge, MA)**, Adleman; Leonard M.** (Arlington, MA) |
| **Assignee:** | **Massachusetts Institute of Technology** (Cambridge, MA) |
| **Appl. No.:** | **05/860,586** |
| **Filed:** | **December 14, 1977** |

|  |  |
| --- | --- |
| **Current U.S. Class:** | **380/30** ; 380/255; 713/150; 713/151; G9B/20.002 |
| **Current International Class:** | H04L 9/30 (20060101); H04L 9/28 (20060101); G11B 20/00 (20060101); G06F 1/00 (20060101); H04K 001/00 (); H04I 009/04 () |
| **Field of Search:** | 178/22,22.1,22.11,22.14,22.15 |

**References Cited [[Referenced By]](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2Fsearch-adv.htm&r=0&f=S&l=50&d=PALL&Query=ref/4405829)**

**U.S. Patent Documents**

|  |  |  |
| --- | --- | --- |
|  |  |  |
| [3657476](http://patft.uspto.gov/netacgi/nph-Parser?Sect2=PTO1&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=1&f=G&l=50&d=PALL&RefSrch=yes&Query=PN%2F3657476) | April 1972 | Aiken |
|  |  |  |

**Other References**

|  |
| --- |
| "New Directions in Cryptography", Diffie et al., IEEE Transactions on Information Theory, vol. IT-22, No. 6, Nov. 1976, pp. 644-654. . "Theory of Numbers" Stewart, MacMillan Co., 1952, pp. 133-135. . "Diffie et al., Multi-User Cryptographic Techniques", AFIPS. Conference Proceedings, vol. 45, pp. 109-112, Jun. 8, 1976.. |

*Primary Examiner:* Cangialosi; Sal   
*Attorney, Agent or Firm:* Smith, Jr.; Arthur A. Horn, Jr.; Robert J.

***Description***

BACKGROUND OF THE DISCLOSURE   
  
This invention relates to communications, and more particularly to cryptographic communications systems and methods.   
  
With the development of computer technology, the transfer of information in digital form has rapidly increased. There are many applications, including electronic mail systems, bank systems and data processing systems, where the transferred information must pass over communications channels which may be monitored by electronic eavesdroppers. While the degree of security required may vary for various applications, it is generally important for all of these examples that the substance of particular communications pass directly from a sender to an intended receiver without intermediate parties being able to interpret the transferred message. In addition, there are further instances where information in computer memory banks must be protected from snoopers who have access to the memory through data processing networks.

…

Настоящий отчет состоит 4 л.

Дата завершения поиска: Подпись уполномоченного лица

26.11.2012