ПЕРЕЛІК ПОСИЛАНЬ

1. Задірака В.К., Олексюк О.С. Комп'ютерна арифметика багаторозрядних чисел. //Київ - 2003
2. Карацуба А.А., Офман Ю.П. Умножение многорозрядных чисел на автоматах //ДАН СССР. — 1962. т.145. — С. 293-294.
3. Шенхаге А., Штрассен В. Быстрое умножение больших чисел // Кибернет. сб. — 1973. — вып. 10. — С. 87-98.
4. Cook S. A., Aanderaa S. O. On the minimum computation time of functions, Thesis, Harvard University, 1966. — P. 26-50.
5. Березовский А.И., Задирака В.К., Шевчук Л.Б. О тестировании быстродействия алгоритмов и программ вычисления основных операций ассиметричной криптографии /Кибернетика и системный анализ № 5, 1999. - С. 61-68.
6. Кнут Д.Е. Искусство программирования для ЭВМ. Т.2.- М.: Издательский дом "Вильямс", 2001. - 828 с.
7. Качко Е.Г., Свинарёв А.В., Горбенко И.Д., Мельникова О.А. Программирование операций многократной точности //Безопасность информации, №1,1995, с. 18-21.
8. Comba P.G. Exponention cryptosystems on the IBM PC //IBM Systems J. B 1990. - 29. - № 4. - P. - 526-538.
9. I Pollard J. M. The fast Fourier transform in a finite field. Mathematics of Computation, 25,1971.- P. 365 - 374.
10. Riesel H. Prime Numbers and Computer Methods for Factorization. Boston, MA: BirkMnser, 1985.
11. Egecioglu 0. and K09 Q. K. Exponentiation using canonical recording. Theoretical Computer Science, 129 (2), 1994. — P. 407 — 417.
12. U. Задирака В.К., Мельникова С.С. Цифровая обработка сигналов. - К.: Наукова думка, 1993. - 294с. 9

13. Lipson J. D. Elements of Algebra and Algebraic Computing. Reading, MA: Addison-Wesley, 1981.
14. Шеннон К.Э. Теория связи, в секретных системах. В работах по теории информации и кибернетики.-г М.:И.Л., 1963. Г
15. Brickel! E.F. Survey of Hardware Implementation of RSA; //Proc. of CRYPTO'89. Lecture Notes in Comp. Sci. Springer-Verlag, 1990, v. 435.-P. 368-370.
16. Lacy J.B., Mitchell D.P., Schell W.M. Cryptolib: Cryptography in Software. //Proc. of UNIX Security Symposium IV. USENIX Association, 1993-P. 1-
17. CCITT. Recommendation X.509: The Directory. - Authentication Framework. 1988.
18. Balenson D. Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes and Identifiers. //RFC 1423, Feb. 1993.
19. PKCS#1: RSA Encryption Standard. Version 2.0. RSA Data Security Inc. 1997.
20. ElGamal T. A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. //Proc. of CRYPTO'84. Lecture Notes in Comp. Sci. Springer-Verlag, 1985, V.196.-P. 10-18.
21. Heilman V.S. Patent № 4.200.770,29 Apr 1980.
22. Bert den Boer. Diffie-Hellman is a strong as Discrete Log for certain primes. In CRYPTO'88 Proc. Springer-Verlag, 1990. Lecture Notes in Computer Science, v.403. - P. 530-539.
23. Brickell E. F. and McCarley K. S. An interactive identification scheme based on discrete logarithms and factoring, J. Cryptology, №5(1), 1992.-P. 29-39.
24. Chaum D. On line cast checks. //Proc. EUROCRYPT'89, Lecture j Notes in Comput. Sci., v.434, 1990.1P. 288-293.

25. Миренков Н. Н. Параллельное программирование для многомодульных вычислительных систем. - М.: 1989.-320 с; 10
26. Shor P. Algorithms for Quantum Computation: Discrete!! Logarithms and Foundations of Computer Science. IEEE Computer! Society Press, 1999. P. 124-134.
27. Boneh D., Lipton R. J. Quantum cryptanalysis of hidden linear я functions // Lect. Notes Comput. Sci № 963,1995. - P. 424-437