

ПЕРЕЛІК ПОСИЛАНЬ

1. Шнайер Брюс Прикладная криптография. – М.: ТРИУМФ, 2003. – 816с.
2. Саломая А. Криптография с открытым ключом. — Москва: Мир, 1995. —318 с.
3. Shamir A. A Polynomial Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem // *Advanced in Cryptology: Proceedings of Crypto 82* — Plenum Press, 1983. — P. 270-288
4. Маховенко Е.Б. Теоретико-числовые методы в криптографии. — Москва: Гелиос АРВ, 2006. — 320 с.
5. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии. — Москва: МЦНМО, 2003.—328 с.
6. A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovasz. Factoring Polynomials with Rational Coefficients. *Mathematische Annalen*. —1982. — P. 515-534.