

## Перелік посилань

1. Roel Peeters , Svetla Nikova and Bart Preneel. Practical RSA Threshold Decryption for Things That Think, 2008.
2. Victor Shoup. Practical Threshold Signatures.2000р., 207–220.
3. Theodore M. Wong, Chenxi Wang, Jeannette M. Wing. Verifiable Secret Redistribution for Archive Systems, 2003.
4. Yvo Desmedt . Redistributing secret shares to new access structures and its applications, 1997
5. Schnorr C.P. Efficient Signature Generation by Smart Cards. — J. Cryptology, 1991.
6. Meet Android Studio [Електронний ресурс] - [https://developer.android.com/studio/intro/index.html#project\\_structure](https://developer.android.com/studio/intro/index.html#project_structure)
7. Алгоритм шифрування AES [Електронний ресурс]- <http://www.opengsm.ru/blog/algorithm-shifrovaniya-aes/>
8. Б. А. Погорелов and Б. Н. Сачков, Eds., Словарь криптографических терминов. М, 2006.
9. J. Gallian, Contemporary Abstract Algebra. Cengage Learning, 2012.
10. W. Мао, Modern Cryptography: Theory and Practice. Prentice Hall PTR, 2004.
11. D. R. Stinson, Cryptography: Theory and Practice, Third Edition. CRC Press, 2005.
12. H. C. A. van Tilborg and S. Jajodia, Encyclopedia of Cryptography and Security. Springer Science & Business Media, 2011.
13. H. C. A. van Tilborg and S. Jajodia, Encyclopedia of Cryptography and Security. Springer Science & Business Media, 2011.
14. R. Canetti, “Universally composable security: A new paradigm for cryptographic protocols,” in Foundations of Computer Science, 2001. Proceedings. 42nd IEEE Symposium on, 2001, pp. 136–145.
15. D. Chaum and T. P. Pedersen, “Wallet databases with observers,” in Advances in Cryptology—CRYPTO’92, 1992, pp. 89–105.

16. P. Feldman, "A practical scheme for non-interactive verifiable secret sharing," in Foundations of Computer Science, 1987., 28th Annual Symposium on, 1987, pp. 427–438.
17. T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," 1998.
18. ISO/IEC 9797-1:1999 Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher.