

REFERENCES

- [1] L. Gu, L. Wang, K. Ota, M. Dong, Z. Cao and Y. Yang, New public key cryptosystems based on non-abelian factorization problems, *Secur. Commun. Netw.* Vol 6, 2013, no. 7, pp. 912–922.
- [2] J.-M. Bohli, B. Glas and R. Steinwandt, Towards provable secure group key agreement building on group theory, *Cryptology ePrint Archive: Report 2006/079*, 2006.
- [3] L. Gu and S. Zheng, Conjugacy systems based on nonabelian factorization problems and their applications cryptography, *J. Appl. Math.* 2014 (2014), Article ID 630607.
- [4] I. Raievska M. Raievska, Y. P. Sysak. Finite local nearrings with split metacyclic additive group. *Algebra Discrete Math.*, 22, no. 1, 2016, pp. 129-152.
- [5] G. A. Miller “Groups which contain an abelian subgroup of prime index” National academy of sciences. *Biographical memoirs*. 1936. pp. 21-32.
- [6] R. V. Skuratovskii, Employment of Minimal Generating Sets and Structure of Sylow 2-Subgroups Alternating Groups in Block Ciphers. Springer, *Advances in Computer Communication and Computational Sciences*, 2019, pp. 351-364.
- [7] A. Otmani, J. P. Tillich, I Dallot. Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes, *Math.Comput.Sci.*3, 2010, pp. 129–140.
- [8] Vladimir Shpilrain And Alexander Ushakov. The conjugacy search problem in public key cryptography: unnecessary and insufficient
- [9] Barrett, P. Implementing the Rivest Shamir and Adleman Public Key Encryption Algorithm on a Standard Digital Signal Processor. *Advances in Cryptology — CRYPTO' 86. Lecture Notes in Computer Science* (1986). volume 263, pp. 311–323.
- [10] Hasenplaugh, W.; Gaubatz, G.; Gopal, V. "Fast Modular Reduction" (PDF). 18th IEEE Symposium on Computer Arithmetic (ARITH'07). (2007). pp. 225–229.
- [11] R. V. Skuratovskii, Involutive irreducible generating sets and structure of sylow 2-subgroups of alternating groups. *ROMAI J.*, 13, Issue 1, (2017), pp. 117-139.
- [12] R. Skuratovskii, "Corepresentation of a Sylow p -subgroup of a group S_n ". *Cybernetics and systems analysis*, (2009), N. 1, pp. 27-41.
- [13] Runovski, K., Schmeisser, H.-J. On the convergence of Fourier means and interpolation means. *J Comput. Analysis Applic.* 2004, 6, pp. 211-227.