ByMySelf(BMS) Encryption Algorithm

Marusic, Diana

Savva, Emilia

Cyber Security is a matter that influences both big companies and individuals. Current services and software products do provide the user security to a certain extent with the help of encryption, but with emerging modern fields, newer mathematical discoveries and increasing computational power algorithms considered secure today will be vulnerable to cyber attacks in the future. Therefore the need of newer, more secure and efficient algorithms always persists. The point of start was Background Research: analysis of encryption algorithms, protocols and instruments like AES, SSL, RSA, PGP. The next step was developing several concepts of the algorithm, and through the process of evolution that included the following phases: Algorithm Development, Implementation, Testing, Results and Analysis, Improvements resulted the current version. After each iteration the algorithm was tested and compared by using cyber attack simulations, cryptanalysis and complexity calculations. The resulted algorithm compared to AES has advantages in terms of having a shorter key and block size with the same brute force complexity, faster encryption and decryption and the possibility to set manually the key length and block size (thus a potential attacker needs to brute force not only the information itself but the key and block size as well). The obtained algorithm having these advantages can be used for the following purposes: data storage services, personal data protection, car security, copyrighted products, financial and banking security, smart home systems. By further improving the algorithm it could be extended to other cybersecurity or data protection areas.