Using Fake Dictionaries in Cryptology to Develop a More Secure Cipher (Fake Synonyms Encryption Cipher)

Aloui, Tarek

Due to daily development, actual ciphers became insecure, for instance AES-256 (Advanced Encryption Standard) which is the most used Symmetric Block cipher (version of AES that inputs a 256 key length), seems to be insecure against the Related Keys Attack that reduces the time for cryptanalysis which would endanger data encrypted using AES-256 which means that other versions can be broken in the future evolutions in cryptanalysis techniques. My project's role is to suggest a new technique inspired from human languages that are improving since 5000 years ago. This technique aims at evolving the security of the cipher every data we transmit, so that we make use of the previous information to produce a more secure one. With this cipher the cryptanalyst will have to decrypt all the previous messages to have a chance to decrypt the actual one which will take so much time to decipher the content. By concatenating this technique with mathematical models we may get more secure ciphers that would lead cryptography to the next level.

Awards Won: