Abstract

In this thesis, a new block cipher algorithm (HANK-1) is presented for the purpose of voice privacy in GSM mobile phone Networks.

The name HANK-1 is an acronym of the first letter of the contributing team first names. HANK-1 is intended to replace the weak and broken A5/1 and A5/2 cipher algorithms and significantly increase the confidentiality and security of the GSM network. The algorithm is 128-bit balanced Feistel structure cipher algorithm with eight rounds and working in cipher block chaining mode of operation.

The work starts by studying the confidentiality algorithms employed in GSM mobile phone network and their weakness. Following this the proposed algorithm in details is introduced. The introduction includes the design strategy, the general structure and the detailed description of the algorithm building blocks.

Following this, the security assessment of the algorithm is presented. The assessment includes the cryptographic evaluation of the building blocks of the algorithm (Substitution boxes – Diffusion matrices), the statistical tests, the avalanche effect criterion, the linear approximation table, and the histogram comparison between the plaintext and the ciphertext.

Finally, the implementation and the experimental results are presented along with the performance evaluation (memory-speed) .The MicroBlaze soft-core microprocessor has been chosen as a target platform and emulator to implement HANK-1 and evaluate its efficiency and suitability to operate on a constrained device like the Mobile Handset.