ABSTRACT

Security issue in communication system is a important thing to be consider, altough sometimes it is ignored for convenience purpose. One method to secure important data is by cryptography, scramble the data with known algorithm in order it can only be read by authorized person. AES-128 algorithm is used to secure speech communication on PSTN since it is strong against attack, it would require 2^{127} *of key combination to break it, fast processing speed and it is free or licenced to everyones without fee.*

AES-128 was developed by Rijmen and Demen from Belgia, and was nominated as Advanced Encryption System (AES) by National Institute of Standards and Technology (NIST) in 2001. This AES is considered as symetric block cipher, as both encrypt and decrypt process use same key. The key length could be vary from 128-bit, which is called AES-128, 192-bit (AES-192), and 256-bit (AES-256), but the data block must be 128-bit.

The implementation of the cryptography system requires conversion of analog signal form to digital signal form, and vice versa. Compression is needed in order to preserve communication bandwidth. The AES-128 itself is implemented on 8-bit processor, and the choice was made for MCS-51 microcontroller. After all previous process is done (digitalization, compression, and encryption), the encrypted data is send over PSTN to the receiver.