



R-E-System

Cryptoalgorithm RFC

RFC – Introduction

RFC is a [symmetric crypto algorithm](#) (secret keys) allowing a secure and rapid encrypting and decrypting of messages.

RFC has been designed particularly for:

- Communications in military applications;
- To combine a high security level over a long period of time
- To be implemented on multiple platforms.

RFC – The Method

It is an **Stream Cipher Algorithm**, designed for military and e-commerce applications being small in complexity it is simple to implement and has a small footprint in software as well as hardware. (*)
In the stream cipher phase the algorithm process a group of bytes. (**)

RFC is based on sub-keys allowing a simultaneous permutation and substitution of bytes: RFC works on single byte.

The key has a length that varies from a minimum size of 64 bit to a maximum of 4096 bit. In all phases of stream cipher, calculation will always use different sub-keys (use 512 bit per group of bytes)

RFC – Mathematical functions

RFC use a “**Non linear cross substitution method**” (use two table) combined with the “**Modified Pseudo-Hadamard Transform**” combined with a particular function named “**Group Bytes Intersection**”.

The “Modified Pseudo-Hadamard Transform” creating a superposition of effects and completes the process of diffusion and confusion in the bit of the message.

Synergies between of this function result in producing a very high level of security.

The max size of table (used in RAM memory) is equal to 2048 bytes; (AES, for example has need up to 4400 bytes)

(*) **Simplicity of algorithm simplifies the task of cryptanalysis to assess its robustness.**

(**) **The group is generally a multiple of 16 byte.**