SUPERDES™

There are two very strong realities regarding encryption. The first is that advances in mathematical/statistical theory and computational technology continue to develop special attacks against a particular cryptographic principle, wherein a “special attack” is a cryptanalytic procedure whose expected execution time falls below the time required to exhaust all possible cryptovariables. The second reality is that the installed base of cryptography will require upgrades respecting the results of the first reality. Upgrades can be very disruptive and costly as the scale of implementation may grow to enormous size.

There is therefore a motivation to suggest a cryptoprinciple that meets two objectives. The first objective is the ability to be able to quickly upgrade the strength of the cryptoprinciple without physical replacement of the cryptoengines. . The second objective is to invest the suggested cryptoprinciple with the ability to support its previous cryptoprinciples, in other words, to be backwards compatible.

SUPERDES™ teaches a patented method using a cryptographic algorithm based upon the venerable data encryption standard (DES) promulgated by the National Bureau of Standards in 1976. We chose to build SUPERDES™ on the DES for three reasons. The first is that SUPERDES™ may be straightforwardly cryptographically upgraded in place. Second, SUPERDES™ can be operated so that it will cryptographically communicate with circuits still protected by single DES and triple DES. Third, building around the DES principle made sense as the DES principle has probably been accorded more intense public scrutiny and published study than almost any other cryptographic algorithm and has stood up well admitting only very few special attacks nominally reducing its cryptographic strength.

The patent US7092525 teaches the SUPERDES™ algorithm and enables its method of use. Just a few general observations concerning SUPERDES™ are:

Description

- The patent describes a gigantic family of related cryptographic algorithms where the cryptographic key determines the specific algorithm. Hence a 128 bit key has 2^{128} algorithms and a 256 bit key has 2^{256} algorithms etc.
- Each cryptographic algorithm has a codebook structure
- The security is based upon the fundamental DES architecture which has no known non-nominal cryptographic attacks except for brute force. However, because each secret key determines the algorithm no standard DES attack will work.
- The algorithm was designed so that the algorithm would support a mode that is backward compatible with the DES and TDES. In addition, an implementation of a mode with a longer key length can be made backward compatible with a large fielded implementation of one sub family of the algorithms
- The algorithm has a mode whereby the encryption rounds of the codebook may be a function of an input deterministic stream. This allows security to be scaled up from the DES level. The number of cryptographic keys is essentially unlimited as it depends upon the basic structure keys and the input deterministic stream.
- The cryptographic structure makes use of a controllable permutation such as an omega network or a Benes-Waksman network. These permutations may be readily used in augmenting a DES chip design. These permutations may also be dynamically changed by changing them in real-time with inputs from an outside Boolean source.
- The textbook Cryptography Demystified, published by McGraw-Hill, discusses the algorithm in Module 33, pp. 247-257.
- The algorithm is a symmetric cryptographic algorithm and not subject to quantum computing attacks in the way that asymmetric public cryptographic algorithms are.

Applications

- The modes of the cryptographic algorithm may allow a multiple security level architecture by using the Cipher Feedback Mode with synchronized periodic shifts to an input deterministic stream associated with the higher security level and different from the input stream associated with the lower security level. As all users observe and use the produced ciphertext, there is no wasted overhead in running the multi-level security mode.
- The algorithm could be used to encrypt a streaming service which contains several different levels of access (& payment) for feeds such as financial markets, news , real time research & survey reports and cable content. Various levels of streaming data from monitoring such as from a driverless vehicle could be protected with one basic algorithm but a hierarchy of keys.
- The algorithm may also be used in applications supporting networks of the Internet of Things (IoT).

A Particular Privacy Cryptographic Mode for SUPERDES™

The preferred embodiment for multi-security-level streaming is Cipher Feedback (CFB). This mode is depicted in Figure 1 taken from “Recommendation for Block Cipher Modes of Operation: Methods and Techniques,” by Morris Dworkin, NIST Special Publication 800-38A, 2001 Edition.

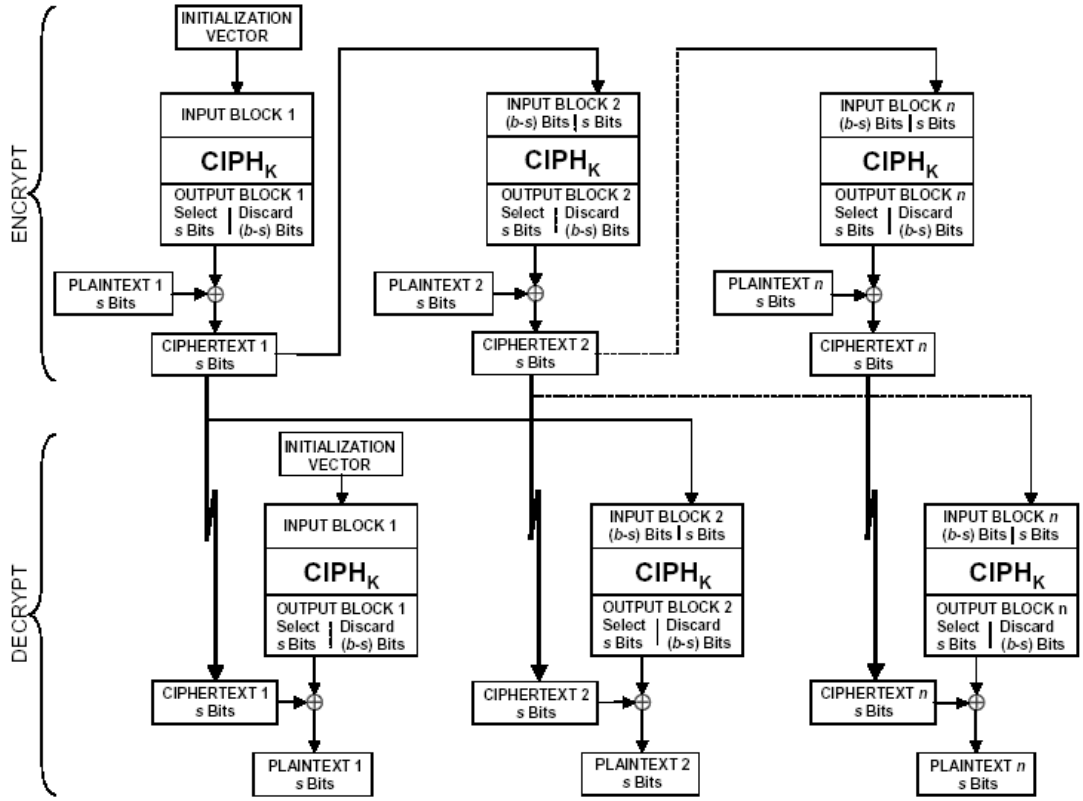

Figure 1 - The CFB Mode

The CFB mode has a number of advantages for a network wherein there a plurality of groups that wish to be cryptographically unique. The CFB mode is self-synchronous and what the preferred embodiment teaches is a way in which all of the groups can choose to start receiving and decrypting at different times.

The mode may be implemented in a number of ways. The following description is for illustration and is not intended to be exclusive of other implementations that will occur to those skilled in the art.

There is established a rota during which the basic 56-bit keying variable remains in effect but the P* keying variable changes for the different groups. The number of k-bit blocks per rota element may be different and the rota schedule and makeup may be dynamically changed should this technique be used in a dynamic bandwidth allocation

scheme. The examples below are proffered for instruction and are not exhaustive as other implementations will occur to those skilled in the art

Let R be the rate at which cryptographic traffic is sent. In Figure 2 we illustrate the case in which grouping A & B have a secure circuit delivering data at a rate 7/8 R.

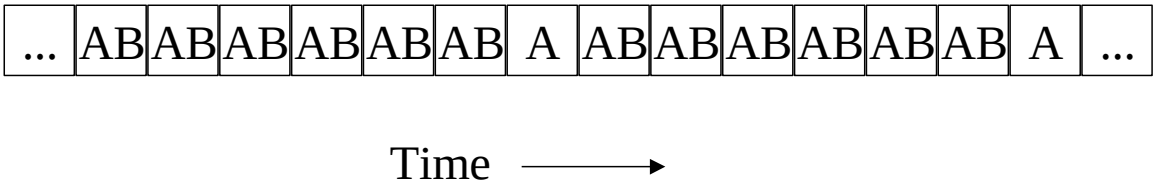

Figure 2 - Grouping A&B Receiving at Rate = 7/8 R; Group A Alone Receiving at Rate = 1/8 R

In Figure 3 we illustrate the case in which the seven possible groupings of three different groups are provided privacy traffic with each distinct grouping receiving traffic at a rate 1/7 R.

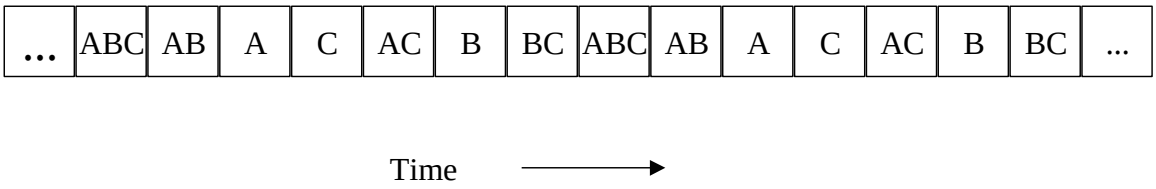

Figure 3 - Each Distinct Grouping Formable from Three Distinct Groups Receiving at Rate = 1/7 R