Analysis On Encryption Process In Data For Satellite

Hee Jin Bae

Ground System Development Department, Satellite Operations & Applications Division, Space Application Center,
Korea Aerospace Research Institute (KARI)
chelry@kari.re.kr

ABSTRACT ... It is necessary to study encryption for protection and safe transmission of the important information. Specially, the security in satellite data is also getting more and more important. This paper introduces DES and TDES algorithm, studies how to apply to satellite data with those algorithms and process of encryption and decryption for satellite data. Proposed encryption process in this paper will be utilized in satellite data for encryption in many satellites.

KEY WORDS: Encryption, Decryption, DES, TDES, Initialization vector, Key

1. INTRODUCTION

It is necessary to study encryption for protection and safe transmission of important information in computer communication, banking business, electronic card, B2B (Business to business), information war among nations and so on. In addition to, security in satellite data is also getting more and more important. Specially, it is very important to encrypt satellite data because satellite data may be utilized in military intention.

KOMPSAT Program started in 1995 and launched in KOMPSAT-1, KOMPSAT-2 successfully after that. At present, KOMPSAT-2 is operated in normal and KOMPSAT-3 and KOMPSAT-5 are under development. The data from KOMPSAT series also adopts the encryption method.

This paper introduces DES and TDES algorithm, studies how to apply to satellite data with those algorithms and process of encryption and decryption for satellite data.

2. DES AND TDES ALGORITHM

DES is the archetypal block cipher — an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another ciphertext bitstream of the same length. The block size of DES is 64 bits. DES also uses a key to customize the transformation, so that decryption can be performed only by those who know the true key used to encrypt. The key consists of 64 bits; however, only 56 of these are actually used by the algorithm. 8 bits are used only for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits, and it is usually quoted as such.

Like other block ciphers, DES by itself is not a secure means of encryption but must instead be used in a mode of operation.

The algorithm's overall structure is shown in Figure 1: there are 16 identical stages of processing, termed rounds. There is also an initial and final permutation; termed IP and IP-1, which are inverses (IP "undoes" the action of IP-1, and vice versa.) IP and IP-1 have almost no cryptographic significance.

Before the main rounds, the block is divided into two 32-bit halves and processed alternately; this criss-crossing is known as the F-function. The F-function ensures that decryption and encryption are very similar processes — the only difference is that the sub-keys are applied in the reverse order when decrypting. The rest of the algorithm is identical. This greatly simplifies implementation, particularly in hardware, as there is no need for separate encryption and decryption algorithms.

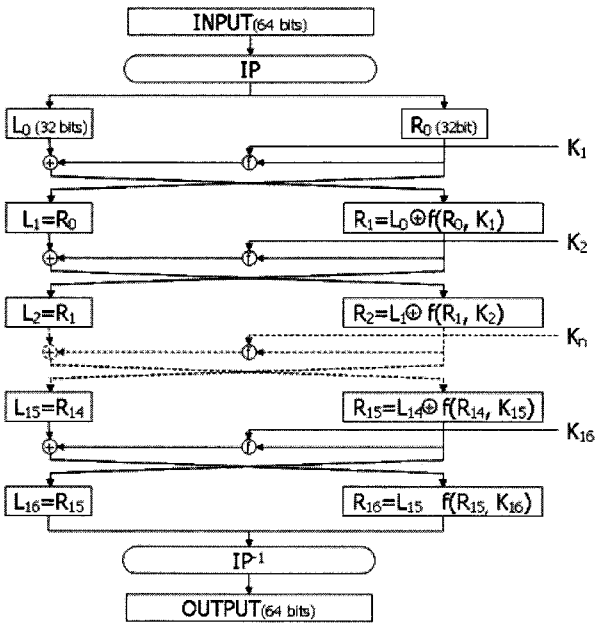

Figure 1. Overall structure of DES

The F-function scrambles half a block together with some of the key. The output from the F-function is then combined with the other half of the block, and the halves are swapped before the next round. After the final round, the halves are not swapped; this is a feature of the F-function which makes encryption and decryption similar processes.

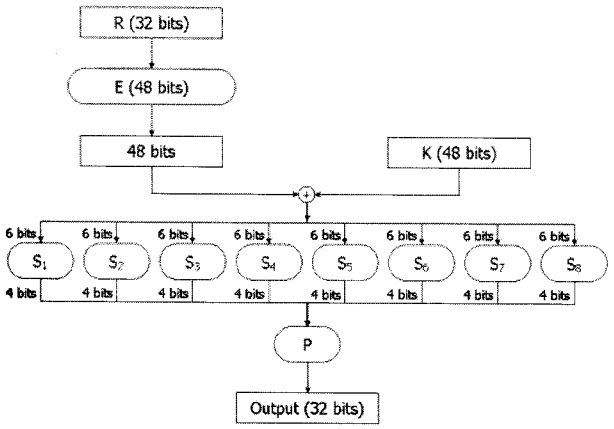

Figure 2. F-function

The F-function, depicted in Figure 2, operates on half a block (32 bits) at a time and consists of four stages:

1. Expansion — the 32-bit half-block is expanded to 48 bits using the expansion permutation, denoted E in the diagram, by duplicating some of the bits.

2. Key mixing — the result is combined with a sub-key using an XOR operation. Sixteen 48-bit sub-keys — one for each round — are derived from the main key using the key schedule (described below).

3. Substitution — after mixing in the sub-key, the block is divided into eight 6-bit pieces before processing by the S-boxes, or substitution boxes. Each of the eight S-boxes replaces its six input bits with four output bits according to a non-linear transformation, provided in the form of a lookup table. The S-boxes provide the core of the security of DES — without them, the cipher would be linear, and trivially breakable.

4. Permutation — finally, the 32 outputs from the S-boxes is rearranged according to a fixed permutation, the P-box.

The alternation of substitution from the S-boxes, and permutation of bits from the P-box and E-expansion provides so-called "confusion and diffusion" respectively, a concept identified by Claude Shannon as a necessary condition for a secure yet practical cipher.

Figure 3 illustrates the key schedule for encryption — the algorithm which generates the sub-keys.

Initially, 56 bits of the key are selected from the initial 64 by Permuted Choice 1 (PC-1) — the remaining 8 bits are either discarded or used as parity check bits. The 56 bits are then divided into two 28-bit halves; each half is thereafter treated separately. In successive rounds, both halves are rotated left by 1 or 2 bits (specified for each round), and then 48 sub-key bits are selected by Permuted Choice 2 (PC-2) — 24 bits from the left half, and 24 from the right.

The key schedule for decryption is similar — the sub-keys are in reverse order compared to encryption. Apart from that change, the process is the same as for encryption.

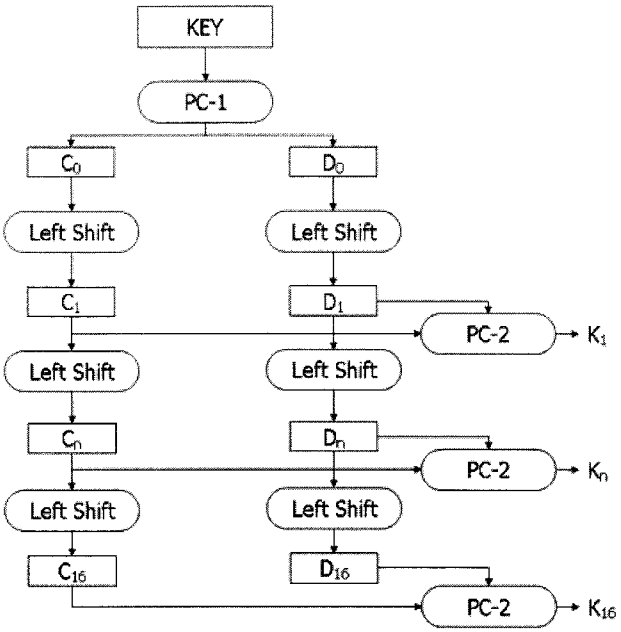

Figure 3. Key Schedule for Encryption

When it was found that a 56-bit key of DES is not enough to guard against brute force attacks, TDES was chosen as a simple way to enlarge the key space without a need to switch to a new algorithm. The use of three steps is essential to prevent meet-in-the-middle attacks that are effective against double DES encryption. Note that DES is not a group; if it were one; the TDES construction would be equivalent to a single DES operation and no more secure.

The simplest variant of TDES operates as follows: DES (K3; DES (K2; DES (K1; M))), where M is the message block to be encrypted and K1, K2, and K3 are DES keys. This variant is commonly known as EEE because all three DES operations are encryptions. In order to simplify interoperability between DES and TDES the middle step is usually replaced with decryption (EDE mode): DES (K3; DES-1(K2; DES (K1; M))) and so a single DES encryption with key K can be represented as TDES-EDE with K1 = K2 = K3 = K. The choice of decryption for the middle step does not affect the security of the algorithm.

In general TDES with three different keys (3-key TDES) has a key length of 168 bits: three 56-bit DES keys (with parity bits 3-key TDES has the total storage length of 192 bits), but due to the meet-in-the-middle attack the effective security it provides is only 112 bits. A variant, called two-key TDES (2-key TDES), uses K1 = K3, thus reducing the key size to 112 bits and the storage

length to 128 bits. However, this mode is susceptible to certain chosen-plaintext or known-plaintext attacks and thus it is designated by NIST to have only 80 bits of security.

3. ENCRYPTION PROCESS FOR SATELLITE DATA

For the implementation of encryption and decryption of satellite data, following items shall be defined:

- Encryption method
- Operation mode
- Input Data Block Size
- Number of encryption key(s) (only for TDES)
- Length of encryption key(s) (only for TDES)
- Length of Initialization Vector
- Encryption key(s)
- Initialization Vector

Generally, encryption strategy of satellite data is desirable to adopt all options and to choose one method in need. Task and command of choice of method may be performed by ground segment.

Operation mode of DES is 4 types as ECB, CBC, CFB and OFB. At first, ECB (Electronic CodeBook) is the simplest method but has the weakest of DES mode, because the ciphertext is the same result in the same plaintext Secondly, there is CBC (Cipher Block Chaining) which output ciphertext impact on input plaintext. Error in operation impacts on next cipher text in this mode. Thirdly, there is CFB (Cipher FeedBack) which performs encryption for initialization vector at first. Finally, there is OFB (Output FeedBack) which does not impact on the next encryption in error. That is, OFB is modified method with ECB which has defect of the same ciphertext for the same plaintext and CBC (or CFB) which has defect of error propagation. Therefore, one mode of 3mode except for ECB is desirable to b adopted because satellite data required for high security.

Initialization vector and encryption key(s) may be made by ground segment or onboard. In case of being made by ground segment, initialization vector and (or) encryption key(s) may be transmitted by telecommand information or separate information. In case of being made on board, ground segment shall receive not only the satellite data but also encryption key(s) and (or) initialization vector. Specially, although the Initialization vector and encryption key(s) are not made on board but selected in dedicated storage on board, the ground segment shall receive not only the satellite data but also encryption key(s) and (or) initialization vector. In this case, encryption key(s) and (or) initialization vector are made in ground segment not on board. That is, dedicated storage on board has the function only to store. Also, ground segment shall update encryption key(s) and (or) initialization vector for dedicated storage on board periodically. The period may be decided according to discussed strategy in advance.

Most of satellite data is transferred as CCSDS format. Therefore, in transmission of some information data from ground segment to satellite, some part of header of CCSDS frame may be encryption key(s) and (or) initialization vector. In this case, ground segment shall transmit the exact position information (pointer) of header used for encryption key(s) and (or) initialization vector to satellite.

Consequently, all information concerning with encryption for satellite data is decided by ground segment. In addition to, ground segment shall know all information concerning with encryption for satellite data because ground segment performs decryption for processing after receiving of satellite data.

Encryption and decryption process for satellite are as below.

1. Ground segment decides which encryption method: DES, TDES.
2. Ground segment decides which encryption key(s).
   1) Made by ground segment
   2) Made on board
   3) Choose in dedicated storage on board
   4) Some part of CCSDS frame
3. Ground segment decides which initialization vector
   1) Made by ground segment
   2) Made on board
   3) Choose in dedicated storage on board
   4) Some part of CCSDS frame
4. Ground segment transmits the information of decision from 1, 2, and 3 to satellite. In case of 1), ground segment transmits the encryption key(s) and (or) initialization vector.
5. Satellite data is encrypted according to information from ground segment and transmitted to ground segment.
6. Satellite data is received from satellite.
7. Satellite data is decrypted with the information concerning encryption strategy.
8. Satellite data is processed at ground segment.

4. CONCLUSTIONS

For the implementation of encryption and decryption of satellite data, some items shall be decided.

Most information concerning with encryption for satellite data is decided by ground segment. In addition to, ground segment shall know all information concerning with encryption for satellite data because ground segment performs decryption for processing after receiving of satellite data. Specially, it is important for ground segment to decide encryption method, mode, encryption key(s) and (or) initialization vector.

Because ground segment decide most information of encryption strategy, ground segment shall transmit the decided information to satellite for performing encryption

process. And the information may be encrypted for high security.

Many satellite needs to protect their data for security. Therefore, it is necessary to plan and decide encryption strategy logically.

The logic of proposed encryption process in this paper will be utilized satellite data for encryption in many satellites.

5. REFERENCES

[1] Data Encryption Standard, FIPS PUB 46-3, 25 Oct, 1999

[2]Don Coppersmith. (1994). The data encryption standard (DES) and its strength against attacks. IBM Journal of Research and Development, 38(3), 243–250.

[3] Eli Biham, Adi Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer Verlag, 1993. ISBN 0-387-97930-1, ISBN 3-540-97930-1.

[4]Eli Biham, Alex Biryukov: An Improvement of Davies' Attack on DES. J. Cryptology 10(3): 195–206 (1997)

[5] NIST SP 800-20 NIST Special Publication 800-20 April 2000