Gost Versus DES Encryption Algorithms

Reyadh S. Nauom, Mayada F. Abdul-Halim & Bara'a A. Attea
Department of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq.
Received: 10/8/1998 ***Accepted: 28/8/1999***

Abstract

To translate text to a code is to encrypt it, and to translate it back is to decrypt it. For either operation, we need a general algorithm and a unique key. The Confidence in an algorithm grows as group after group fails to break it. The presented paper discussed two encryption algorithms; DES, the workhorse of cryptography algorithms and GOST, their relation, and the major differences between them.

المستخلص

عملية التشفير هي عملية تحويل المعلومات من صيغتها المفهومة الى صيغة غير واضحة, أما عملية فك الشفرة هى عملية إعا دة المعلومات الى صيغتها الأ صلية. وفي كلا الحالتين, نحتاج الى خوارزميـات بالإضافة الى مفتاح مشترك للتشفير و فك الشفرة. تقاس كفاءة الخوارزمية المستعملة للتشفير بصعوبة فتحها من قبل أشخاص غير مخولين. في هذا البحث نتعامل مع خوارزميتين للتشفير. الطريقة الأولى. باسـتخدام دي- إس- أس و الثانية باستخدام جوست, يوضح البحث أهم العلاقات و الفروقات بين الخوارزميتين.

Introduction

The Data Encryption Standard (DES) was developed by IBM and adopted as a Federal Standard on Nov.23, 1976. Recently, candidates that can be considered serious DES replacements are emerging. The Cryptographic Transformation Algorithm-Gost 28147-89 also known as "GOST "algorithm was published in 1989 by the National Soviet Bureau of Standards. It is a secret-Key Algorithm, similar in construction to DES. However, GOST's designers tried to achieve a balance between efficiency and security by making some modification to the algorithm.

Both DES and GOST are block cipher algorithms, which means that they encrypt a group of plain text symbols as one block. They use a series of iterations of a loop involving arithmetic and logical operations. The following sections describe DES and GOST, relation between them, and outline the major differences between them.

1. Outline of DES and GOST Encryption Algorithm.

Both DES and GOST are Feistel networks; both iterate an encryption algorithm for multiple rounds. The text in both algorithms is first broken up into a left half, L, and a right half, R, of 23-bit each, combine the key with one half, swap the two halves. DES has 16 rounds, while GOST has 23 rounds of this process. A round, i, of either algorithms looks like this: [4]

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} XOR \ \ f(R_{i-1}, k_i)$$

2. Description of DES Round

Figure 1 is a single round of DES [4][1]. First, the right half is expanded from 32 to 48 bits by a fixed permutation (see Table 1). The result is XORed with the *i* th subkey, and then broken it into eight 6-bit chunks. Each chunk becomes the input to a different S-box, the first six bits go in the first S-box, the second six bits go in the second S-box and so on. The outputs of the eight S-boxes are recombined into a 32-bit word, and then the entire word is permuted. Finally the

result is added modulo 2^{32} to the left half to become the new right half, and the right half becomes the new left half [1][2].

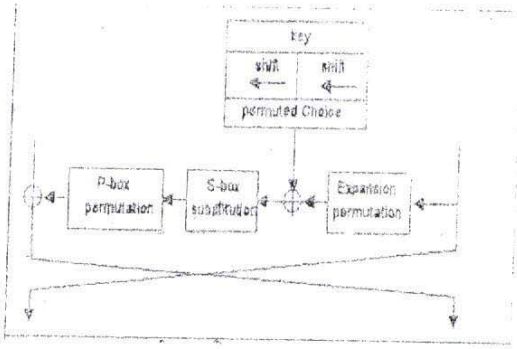

Figure1:One round of DES ($\oplus$)=exclusive-OR

Blt	1	2	3	4	5	6	7	8
Move to	2,48	3	4	5,7	6,8	9	10	11,13
Blt	9	10	11	12	13	14	15	16
Move to	12,14	15	16	17,19	18,2	21	22	23,25
Blt	17	18	19	20	21	22	23	24
Move to	24,26	27	28	29,31	30,32	33	34	35,37
Blt	25	26	27	28	29	30	31	32
Move to	36,38	39	40	41,43	42,44	45	46	47,1

Table1: Expansion Permutation

2.2 Description of GOST Round.

Figure 2 is a single round of GOST [4]. First the right half and the i th subkey are added modulo 2^{32}. The result is then broken into eight 4-bit chunks, each of which becomes the input to a different S-box. There are eight different S-box, the first four bits go in the first S-box, the second four bits go in the second S-box, and so on. The outputs of the eight S-boxes are recombined into a 32-bit word to be circularity shifted to the left 11-bits. Finally the result is added modulo 2^{32} to the left half to become the new right half, and the right half becomes the new left half [4].

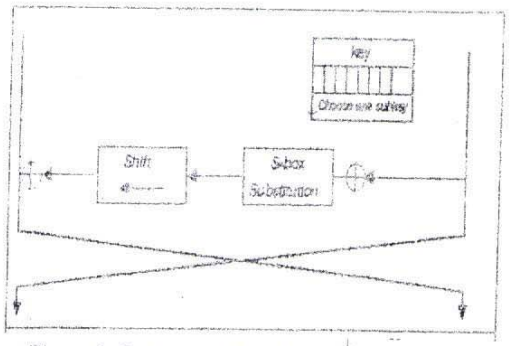

Figure2:One round of GOST($\oplus$ =addition modulo 2^{32})

3. Subkeys Generation

3.1 DES Subkeys Generation

The 64-bit key becomes a 56-bit key by deletion of every eight bit (these bits are assumed to be parity bits that carry no information in the key). Then the56-bit key is first divided in half. Then, each 28-bit half is circularly shift to the left by either one or two digits depending on the round (see Table 2) [1][2]. After the shift, 48-bits are selected by a fixed permutation 9see Table 3) [1].

Table2: number of bits of circular shifts for each cycle

Cycle Number	Bits Shifted
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Table3: Choice permutation to select 48 key bits

Key bit	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Selected for position	5	24	7	16	6	10	20	18	--	12	3	15	23	1
Key bit	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Selected for position	9	19	2	--	14	22	11	--	13	4	--	17	21	8
Key bit	29	30	31	32	33	34	35	36	37	38	39	40	41	42
Selected for position	47	31	27	48	35	41	--	46	28	--	39	32	25	44
Key bit	43	44	45	46	47	48	49	50	51	52	53	54	55	56
Selected for position	--	37	34	43	29	36	38	45	33	26	42	--	30	40

3.2 GOST Subkeys Generation

GOST has a 256-bit key. It is divided into eight 32-bit blocks. The first block is used in the first round, the second block is used in the second round, and so on. At the ninth and at the 17th rounds, the cycle starts again. However, for the 25th through 32nd round, the order is reversed:

the eight blocks is used in the 26th round, and so on [4].

4. Confusion Technique

Both DES and GOST perform a substitution technique that provides confusion by using eight different S-boxes [1].

4.1 DES's and S-boxes Generation

An S-box in DES is a lookup table (see Table 4) by which six bits of data are replaced by four bits [1] [2]. The 48-bit input is divided into eight 6-bit blocks $B_1, B_2, ..., B_8$; block B_i is operated on by S-box as in figure-3 [1]. If the six bits of block B_i are represented as $r_1 c_3 c_2 c_1 c_0 r_0$, then block B_i is transformed into the 4-bit result shown in $r = r_1 r_0$, column $c = c_3 c_2 c_1 c_0$ of section S_i of Table 4.

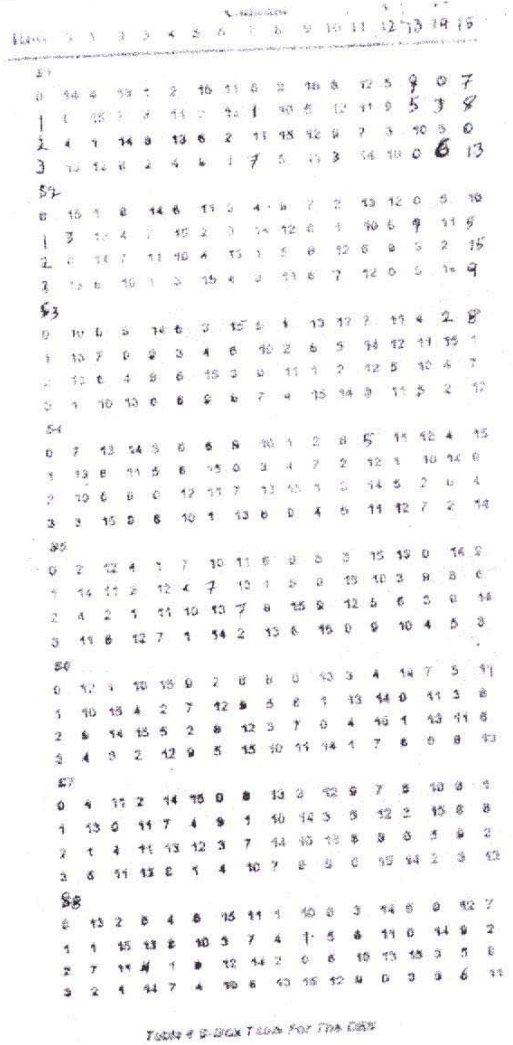

Table 4: S-Box Tables For The DES

4.2 GOST's S-Boxes Generation

GOST has eight different S-boxes. Each S-box is a Permutation of the numbers 0 through 15. For example, an S-box might be: 7,10,2,4,15,9,0,3,6,12,5,13,1,8,11. If the input from a 4-bit chunk (discussed in 3.2) to the S-box is 0,then the output is 7,and so on. All eight S-boxes are different, and they are considered as additional key material.

5. Diffusion Technique

5.1 DES's P-Boxes Generation

DES perform permutation that provides diffusion by reordering the bits resulted from confusion operation, this is designed to increase the avalanche affect; the rate in which a single bit change in the input affects bits in the output[4]. Table 5 shows the position to which bits are moved [1].

Table 5: Permutation box P

Bit	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Goes to position	16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
Bit	17	18	19	20	21	20	22	23	24	25	26	27	28	29	30	32
Goes to position	2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

5.2 GOST Cyclic Shift

The results of confusion operation are recombined into a 32-bit word, undergoes an 11-bit circular shift-left, towards the higher-order bits. The change in one input bit affect one S-box in one round, which then affects two S-boxes in the next round, and so on[4].

6. Exchange left and Right Halves

6.1 DES's XOR operation

The result of diffusion operation in each round is XORed with the left half to become the new right half, and the right half becomes the new left half.

6.2 GOST's Modulo Addition

The result of diffusion operation in each round is added modulo 2^{32} to the left half to become the new right half, and the right half becomes the new left half.

Conclusion

The major differences between DES and GOST are [1] [3] [5]:

1. DES has a complicated procedure for generating the subkeys from the key. GOST has a simple one.

2. DES has a 56-bit key; GOST has a 256-bit key.
3. DES's S-boxes have 6-bit inputs and 4-bit outputs; GOST's S-boxes have 4-bit inputs and outputs.
4. DES's S-boxes are fixed and public; GOST's S-boxes are random and secret.
5. GOST's S-boxes is one fourth the size of a DES's S-box.
6. DES has an irregular permutation "P-Box"; GOST uses an 11-bit left circular shift.
7. DES uses XOR to add the key to the right half and to add the right half to the left half, GOST uses addition modulo 2^{32}.
8. DES has 16 rounds; GOST has 32.
9. From above we conclude that at a reasonable cost, Gost algorithm is better than DES algorithm.

References

1. Charles P. Pfleeger ,(**1989**)"*security In Computing*," Prentice-Hall Inc.,
2. Henry Beker, Fred Piper, (**1982**) "*cipher Systems, The Protection of Communications* ", Northwood publications.
3. Barry Simon, (**1997**) "*Don't Trust Anyone*", PC magazine vol. 16 No. 22 Dec. 16, 1997.
4. Bruce Schneier, (**1995**) "*The GOST Encryption Algorithm*", Dr. Dobb's Journal, Jan. 1995.
5. Bruce Schneier, (**1995**) "*The Blowfish Encryption Algorithm: One Year Later*", Dr. Dobb's Journal.