AN ENCRYPTION AND AUTHENTIFICATION PROCEDURE FOR TELESURVEILLANCE SYSTEMS

Odoardo Brugia[*] - *Salvatore Improta*[**] - *William Wolfowicz*[*]

[*] Fondazione Ugo Bordoni - Sede Legale - v. le Trastevere 108 - 00153 Roma

[**] FATME SpA

Work carried out at the Fondazione Ugo Bordoni under the agreement between the Istituto Superiore P.T. and the Fondazione Ugo Bordoni.

T. Beth, N. Cot, and I. Ingemarsson (Eds.): Advances in Cryptology - EUROCRYPT '84, LNCS 209, pp. 437-445, 1985.

ABSTRACT - To perform message authentication in a telesurveillance system, the paper proposes a non linear time varying encryption algorithm, based on key layering in three levels (system key, intermediate key, running key) and on encryption organization into two or more sets of three operations (running key rotation, message digit substitution and transposition). The algorithm was designed to be implemented on an 8-bit microprocessor.

1 - INTRODUCTION

The telesurveillance system we are concerned with includes a control center (CC) and a certain number of environment detection devices (DD) located in the places to be kept under surveillance. The CC asks the remote DD's ciclically about the parameters they are detecting and each DD sends the appropriate answer back taking it from a finite set. The CC and DD's can be linked either by a private network or by leased channels.

To prevent modifications or imitations of the messages interchanged between the CC and the DD's, an effective authentication procedure is needed. Encryption is one of the most effective methods to perform authentication; for this purpose, the encryption algorithm must meet two fundamental requirements: non linearity of the relation between plaintext and cyphertext; time variability of the algorithm parameters. If the former requirement is met, any intruder attempting message modifications without

knowing the secret key would be unable to make the appropriate changes in the encrypted signature required for his modification to escape disclosure. The latter requirement is necessary to avoid that an intruder can record properly encrypted messages and sabotage the system playing them back later.

The encryption algorithm proposed in this paper meets these requirements and can be implemented on an 8-bit microprocessor. It is based on the layering of the key in three levels: system key, intermediate key and running key (sec.2), and on encryption organization into two or more sets of three operation: running key rotation, message digit substitution and transposition (sec.4). The running key consists of segments of the binary sequence generated by a non linear pseudorandom generator whose parameters are functions of both the intermediate and the system key (sec.2). The binary message to be encrypted consists of three fields containing telesurveillance, key changing and authentication information respectively (sec.3). Authentication and telesurveillance procedures are described in sec.5.

2 - KEY GENERATOR

Whenever an encryption or decryption operation has to be performed in the system, a running key request signal starts the key generator shown in fig.1, where M denotes a buffer memory and $G_1, G_2, G_3, G'_1, G'_2, G'_3$ are linear feedback shift registers (LFSR). The first three LFSR's have primitive characteristic polynomials of degree N_1, N_2, N_3 respectively and form a Geffe generator [1], whose output sequence has [2]: equally likely 1's

and 0's; a period equal to lcm $(2^{N_1}-1, 2^{N_2}-1, 2^{N_3}-1)$ and a complexity equal to $N_1N_2+(N_2+1)N_3$. After each running key request, 8 digits of this sequence are generated and written into M to update its content.

The second three LFSR's, together with the 8-digit delayer D, form a modified Geffe generator; the characteristic polynomial of G_2' is primitive, while the feedback connections of G_1' and G_3' and the initial states of G_1', G_2', G_3' are determined as functions of the content of M under the constraints that: the three characteristic polynomials have an odd number of terms and fixed degrees N_1', N_2', N_3' the initial state of each LFSR has at least one digit set to 1. If the polynomial coefficients of G_1' and G_3' and the initial states of G_1', G_2', G_3' were constant (so as the polynomial coefficients of G_2' are), the modified Geffe generator would generate a binary sequence having a period P and a complexity C such that: $3(2^{N_2'}-1) \leq P \leq \text{lcm}(2^{N_1'}-1, 2^{N_2'}-1, 2^{N_3'}-1)$ and $2+N_2' \leq C \leq N_1'N_2'+(N_2'+1)N_3'+N_2'$; the lowest and highest values of P and C are taken respectively with probabilities $2^{8-N_1'-N_3'}$ and $\varphi(2^{N_2'}-1)\varphi(2^{N_3'}-1)/N_2'N_3' \; 2^{N_2'+N_3'-4}$, where φ indicates the Euler totient function. After each running key request, 64 digits of this sequence are generated.

The time varying parameters of the modified Geffe generator are changed according to the content of M whenever a given number of digits randomly generated in the CC coincides with the content of an equal number of fixed memory cells.

The system key, which provides the coefficients of the characteristic polynomial of G_1, G_2, G_3, G_2' and the initial states of G_1, G_2, G_3, is generated by a program fulfilling the requirements that the aforesaid poly

nomials are primitive and each initial state vector contains at least a 1. The intermediate key, which provides the coefficients of the characteristic polynomials of G'_1, G'_3 and the initial states of G'_1, G'_2, G'_3, is taken from M. The running key consists of the 64 digits generated by the modified Geffe generator.

Since the intermediate key is changed at random, the sequence generated by the modified Geffe generator is usually aperiodic and it is meaningless to define its complexity.

3 - MESSAGE STRUCTURE

Every message consists of 64 binary digits subdivided in three fields: a 40-digit information field, reserved to the telesurveillance information; an 8-digit signalling field, devoted to the transmission of key-changing information; a 16-digit authentication field, for transmission of authentication information. The information field is subdivided in two sectors, devoted respectively to the transmission of CC's interrogations and DD's answers; the CC uses the second sector too, to transmit a replica of the interrogation; the DD's use the first sector too, to transmit a replica of the received interrogation. In the signalling field the CC inserts the key-changing signal and the DD inserts a replica of the received key-changing signal. The sequence to be inserted in the authentication field can be get either by taking the remainder of the modulo 2 division of the d-transform [3] of the information and signalling field contents by a 16 degree polynomial, or as the result of 16 parity checks. The

probability that intentional or unintentional message modifications can elude the controls is greatly reduced owing to the high message redundancy and check number.

4 - ENCRYPTION

Encryption consists of two or more iterations of three operations: running key rotation; plaintext digit substitution; transposition of the digits resulting from the preceding operation. Substitution is performed by adding modulo 2 each plaintext digit to the corresponding digit of the running key (without rotation in the first iteration, and after suitable running key shifts in the following iterations); the substituted sequence is segmented in eight 8-digit blocks which are arranged in an 8x8 matrix, while the running key is segmented in sixteen 3-digit blocks. Transposition is performed by shifting each row and then each column of the matrix ciclically by a number of positions given by the decimal value of the appropriate key block.

5 - TELESURVEILLANCE PROCEDURE

The CC shares individual system keys with the DD's: the key generators sharing the same system key evolve synchronously at 64-digit steps, generate the same running key and change the intermediate key on the initiative of the CC.

To interrogate each DD about its state, the CC sends a message encrypted with the specific running key.

The DD decrypts the message and either verifies that the 16 authentication digits coincide with the remainder of the modulo 2 division of the d-transform of the information and signalling field contents by the prefixed 16 degree polynomial or performs 16 parity checks according to the authentication approach used in transmission.

If the message authenticity is recognized, the DD reads the information and signalling field contents. If a key-changing signal is present in the signalling field, the DD gets ready to change the intermediate key at the next running key request. Moreover, the DD prepares a message containing: the replica of the received interrogation and the corresponding answer, in the information field; the replica of the received key-changing signal, in the signalling field; and the authentication sequence, in the authentication field. This message is encrypted with a new running key.

Failure of authentication check can be due, or not, to the reception of a cleartext by which the CC communicates it did not recognize the authenticity of the message previously sent by the same DD. In the former case the DD changes the intermediate key and encrypts the preceding message with the new running key. In the latter case, the DD sends a non authentication message in clear, keeps its key generator up with the corresponding CC's one by letting it run by 64 digits, and gets it ready to change the intermediate key. Both non authentication messages consist of 64 digits obtained by repeating the DD address a certain number of times.

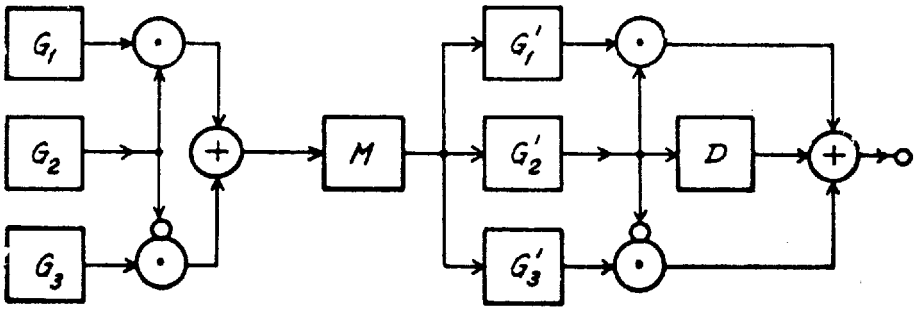
An alarm is given in the CC whenever one of the following events occurs: lack of DD answer within a prefixed time interval; non authentication of three consecutive messages coming from a same DD; alarm indication and consective alarm confirmation from the part of a same DD; a combination of non authentication and alarm messages.

REFERENCES

[1] P.R. GEFFE: "How to protect data with ciphers that are really hard to break" Electronics, jan.4, 1973, p.99-101.

[2] E.L. KEY: "An analysis of the structure and complexity of non linear binary sequence generators" IEEE Trans. on Inf.Th., v.IT-22, n.6, nov.1976, p.732-6.

[3] A. GILL: "Linear sequential circuits" Mc.Graw Hill, 1967.



⊙ = Modulo 2 multiplier

⊕ = Modulo 2 adder

$G_1, G_2, G_3, G_1', G_2', G_3'$ = Linear feedback shift registers

M = Buffer memory

D = Delayer

Fig. 1 - Key generator