Military Technical College
Kobry El-kobbah,
Cairo, Egypt

5th International Conference
on Electrical Engineering
ICEENG 2006

A SURVEY of IFF SYSTEMS

Alaa Fahmy[1] K. H. Moustafa

ABSTRACT

Since Second World War, different military standard modes of Secondary Surveillance Radar (SSR) were developed, namely, Mark X, Mark X IFF Selective Identification Features (SIF), Mode S, and Mark XII. All these modes of operations have different interrogation and reply signals format. This paper review SSR modes of operation. In the mean time, Mark XII is highlighted. An encryption technique based on the use of chaotic map is proposed.

KEYWORDS: IFF, and cryptography

1. Introduction

Cryptographic systems play an important roll for different applications (civilian or military). These cryptosystems can classified into two main categories, private key cryptosystems, and public key cryptosystems [1,2]. Each has its own applications. One of the most important applications of cryptography is the security of the IFF systems. An overview for IFF systems is introduced. The rest of the paper includes the following: section 2 presents motivation and overview of eastern and western IFF systems. Section 3 introduces Mark X (SIF), Mark XII, and a proposed secure mode that can fit for IFF system. Section 4 concludes the paper.

2. Motivation and Overview For Eastern/Western IFF System

In the Eastern IFF system, or Soviet IFF system, the interrogation uses pulses similar to modern IFF systems, but at different frequency, which is equal to 700 MHz (UHF band) for interrogation and reply signal [3]. The interrogation signal format is fixed; but the reply signal pulse impressed by amplitude modulation (AM) tone of twelve possible combinations.

2.1 Interrogation Signal Format For Eastern IFF System

The interrogation signal is a train of RF pulses, at frequency 700 MHz as shown in Fig.1 [3,4,5]. It is composed of three pulses spaced by 4.5 µs. The duration of each pulse is 0.8 ± 0.2 µs.

[1] Assoc. Prof. Dept. of Electrical Engineering, Military Technical College, Cairo, Egypt.

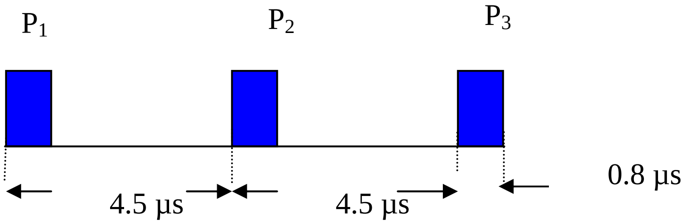


Fig. 1 Eastern IFF interrogation Signal Format

2.2 Reply Signal Format For Eastern IFF System

The reply signal composed of one pulse as shown in Fig.2. The duration of the pulse is 2.5 µs. The reply code is amplitude modulated (AM) by one of 12 different frequencies in the range 1:10 MHz.

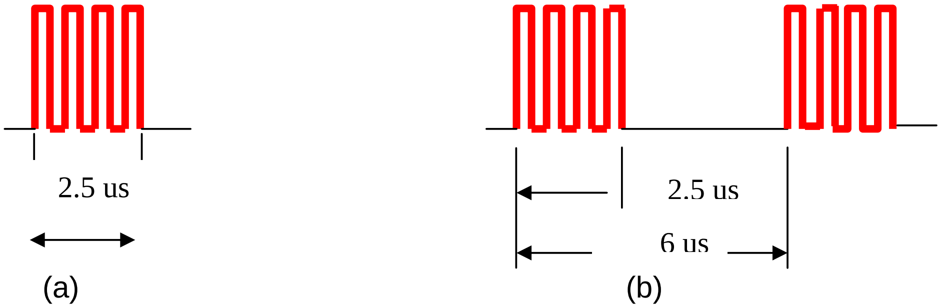


Fig.2 (a) Eastern IFF Reply Signal Format, (b) Eastern IFF Emergency Signal Format

2.3. Interrogation Signal Format For Western IFF System

Mark X is an IFF system developed in the USA [3]. At first “X” denoted an experimental system and after it went into production, it is assigned Mark X (ten) nomenclature. The signal transmitted by the interrogator is conventionally called interrogation. The interrogation signal of Mark X is amplitude-modulated pulses of RF carrier frequency 1030 MHz [3]. Fig.3 shows the characteristic of the interrogation signal.

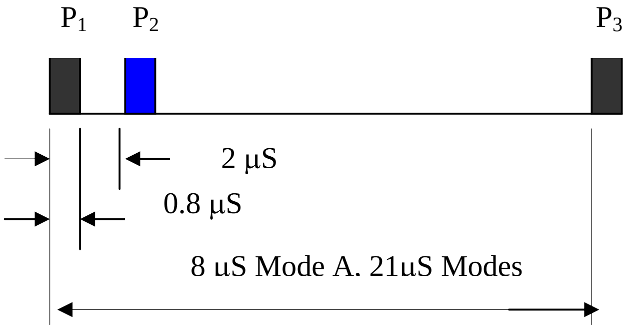


Fig. 3 Mark X Interrogation Signal Format

The two pulses P_1 and P_3 are transmitted via the interrogation beam of the antenna, and the spacing between these two pulses specifies the interrogation mode, and according to this mode, the data contained in the transponder reply is determined. Six different types of interrogation modes are possible. They are shown in Fig.4.

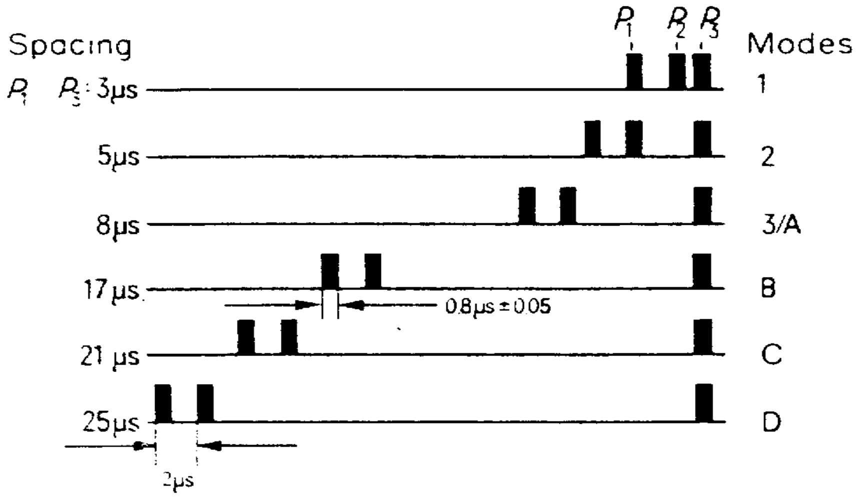


Fig.4. Mark X Interrogation Modes

The significance of the extra pulse P_2 , which is delayed by 2 μs after P_1 declares if the interrogation signal is transmitted via the main beam or via the control beam of the antenna.

In other words, if the strength of P_2 is greater than P_1 or P_3, it means that the interrogation signal is sent via the main beam, otherwise it is sent via the control beam. Therefore, the interrogation signal sent via the control beam can be ignored, since it is transmitted via the side lobe. This can be called Side Lobe Suppression (SLS).

Table 1 gives a synopsis of the characteristics of the six interrogations modes and their applications.

Table 1. Interrogation Modes & Their Applications

Mode	Pulse Spacing (μs)	Use	User
1	3	Identification	Military
2	5	Identification	Military
3/A	8	Identity	Military/Civil
B	17	Not Used	Civil
C	21	Height	Civil
D	25	Not Used	Civil

Mode 1 is not secure, and used by ships to track aircraft and other ships. Mode 2 is used to identify planes such as flight leaders; planes on intercept missions, etc. Its tactical use may vary according to the particular situation. Mode 3 is the standard system which, can be used by commercial aircrafts to indicate their position to ground controllers of Air Traffic Control (ATC) [6].

Besides interrogating in one single mode, it is also possible to interrogate in several interrogation modes in a continuous sequence. A commonly used method of interrogation mode is to ask, alternately, for identification and altitude; i.e. the interrogations follow one another alternately according to the pattern A C A C A C [4].

2.3. Reply Signal Format for Western IFF System

The reply signal is amplitude-modulated RF pulses with carrier frequency 1090 MHz. Mark X reply codes [4] are quite simple, as can be seen in Fig.5. Mode 1 and Mode 3 replies are a single 1-µsec pulse. Mode 2 reply from an airborne transponder is a pair of pulses 16-µsec apart. Mode 2 reply from a ship borne transponder is a single pulse the same as Mode 1.

Two addition special Mark X reply codes are shown in Fig.6. In the first one, answer to a radio request from a ground controller, the pilot can control his transponder to reply with two pulses spaced 16 -µsec apart, the same as a normal Mode 2 reply. This mode is termed I/P, or identification of position. The second one is in the case of, turns ON his emergency switch and the transponder replies with 4 pulses spaced 16-µsec apart

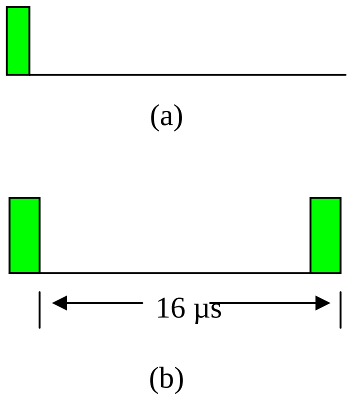
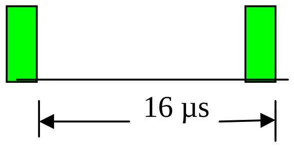
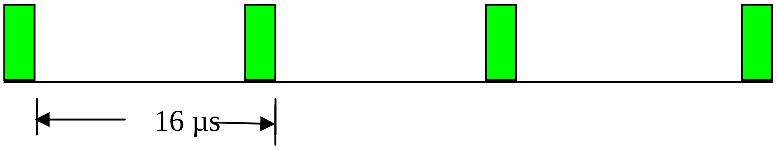


Fig.5. Mark X IFF Reply Code, (a) Mode 1, Mode 3, & Mode 2 (b) Mode 2 Airborne Reply



(a)



(b)

Fig.6. Special Mark X Reply Codes (a) Identification of Position, (b) Emergency Code

3. Mark X (SIF) and Mark XII

3.1 Mark X (SIF)

To satisfy security requirements and problems associated with ATC, an IFF system that could generate many, variably coded IFF replies were needed. To satisfy this requirement, a coder was introduced into the basic Mark X IFF signal path. This coding capability is called SIF, and system nomenclature was changed to Mark X IFF (SIF). The interrogations challenge retained the same form as Mark X. Only the replies were changed.

Fig.7 shows the reply signal transmitted by the aircraft in response to an interrogation. The two pulses F_1 and F_2 are called framing pulses, or brackets, and are always present. The data pulses are designated A, B, C and D with a suffix 1, 2 or 4 to give a total number of 12. The pulse in the middle, the X pulse, is not currently used. Additional SPI pulse (Special position indicator) delayed with respect to F_2, is used occasionally. The 12 pulses that are used give 4096 permutations and communicate the reply data [3]. The data contained in the reply is related to the question being asked through the interrogation mode. Not all of the 4096 reply codes are used on all modes as indicated in table 2.

The standard interrogation mode is Mode 3/A, the common civil/military mode, is used for general identification with the identity number of the aircraft formed from the octal value of the reply pulses in the order ABCD, as an example for the code “3065” is shown in Fig.7.

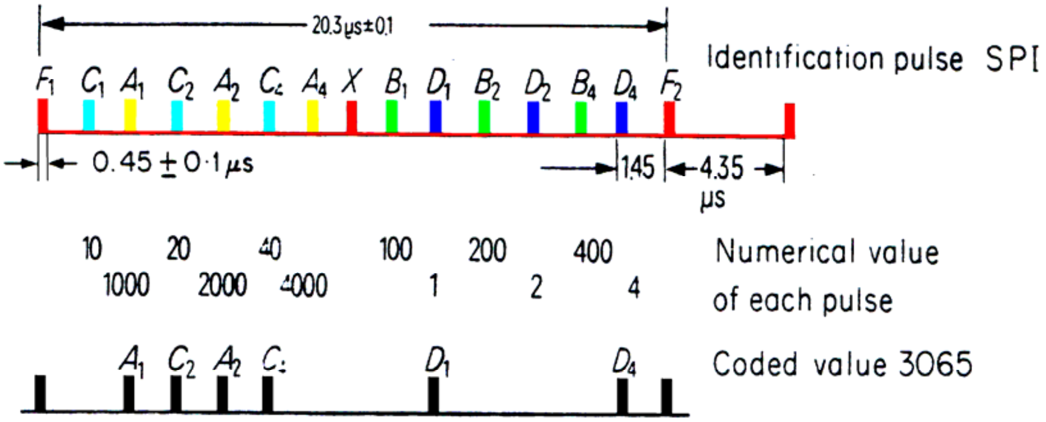


Fig.7. Mark X IFF (SIF) Reply Signal Formats

Table 2 Reply Codes for Each Interrogation Mode

Mode	Number of Possible codes
1	32 codes (B4, all C and D pulse not used)
2	4096 codes
3/A	4096 codes
C	2048 codes (D1 pulse not used)

Table 3 Special Reply Codes

Reply code	Meaning
7700	Emergency
7600	Radio failure
7500	Hijack

Through an international agreement, specific sets of identity numbers can indicate the type of flight, the destination, or the origin of the aircraft. Three particular codes are universally used to indicate emergency conditions (Table 3). These special codes are of great value for indicating particular difficulties to the ground authority in circumstances when the pilot may be unable to communicate using the normal voice channels.

3.2 Mark XII and Proposed Secure Mode

3.2.1 Mark XII

Mark X (SIF) did not provide real a security. Its interrogation pulses are not coded. There was always a possibility that an enemy might use Mark X (SIF) interrogation pulses to let aircraft to identify themselves and then use the aircraft's IFF system as a homing beacon for missiles. By 1956, an American group had been formed to implement what has now become the Mark XII system; it uses a Mode 4 (Secure Mode), which is a fully cryptographic mode [7].

The secure mode is used exclusively for military purposes. This mode uses a very long challenge telling the transponder that it is about to receive a secured message. The challenge itself is encrypted at the interrogator by a separate device that uses various complex mathematical algorithms to put it in a secure form. The transponder routes the ensuing challenge to a separate device that uses the inverse algorithms to decode the challenge.

In effect, each challenge is telling the transponder to respond in a certain way. If the transponder cannot decipher the challenge, it will not be able to respond in the proper way and thus will not be identified as a friend. A complete description of IFF equipment is in reference [3, 6]. To prevent unauthorized use of either the interrogation equipment or the transponders if they should fall into hostile hands, a key code must be periodically entered into each device.

To eliminate the chance of a random guess for the proper response by a hostile target, identification consists of a rapid series of challenges each requiring a different response that must be correct before the target is confirmed as a friend. A very high degree of security to the identification system is achieved through the use of key codes and powerful cryptographic techniques. Fig.8 illustrates Mark XII interrogation and reply codes. Meanwhile Fig.9 shows the interrogation and reply codes for different modes.

The **interrogation challenge for mode 4** is amplitude-modulated pulses, 0.5 µs pulse width, and 2 µs spacing. The interrogation contains the following bits:
Five Digit Sync: five pulse positions, first pulse occupied always, fifth pulse always missing (used for ISLS). Thirty-two-digit word: The composition of the thirty-two bits challenge before ciphering is shown in Fig.10. Random bits for crypto (20 bits), reply bits to indicate reply position (4 bits), authentication bits to reject unauthorized challenge, minimize attempts at exploitation, and verifies that interrogator and transponder share the same key (8 bits).

For mode 4-reply code, there are three pulses 0.5 µs pulse width, and 1.8 µs spacing. The group is time coded to occupy any one of sixteen positions (4 bits), 4 µs spacing, and continuously changing as dedicated in Fig.8. Since, Mark XII is a fully cryptographic system used to identify friendly aircraft in hostile situations by employing complex enciphered signal; a proposed cryptosystem will be presented.

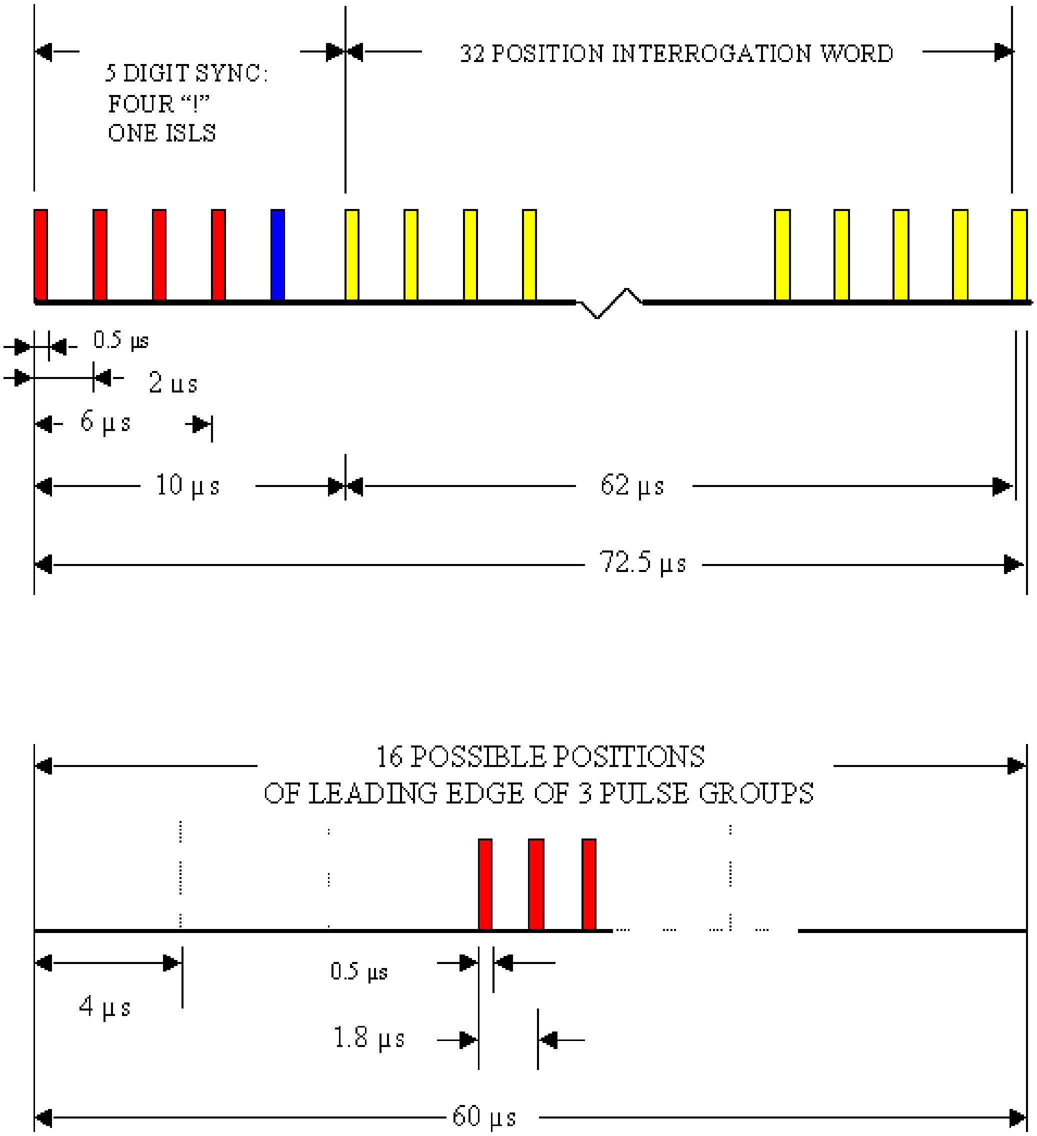


Fig. 8 Mark XII Interrogation & Reply Code

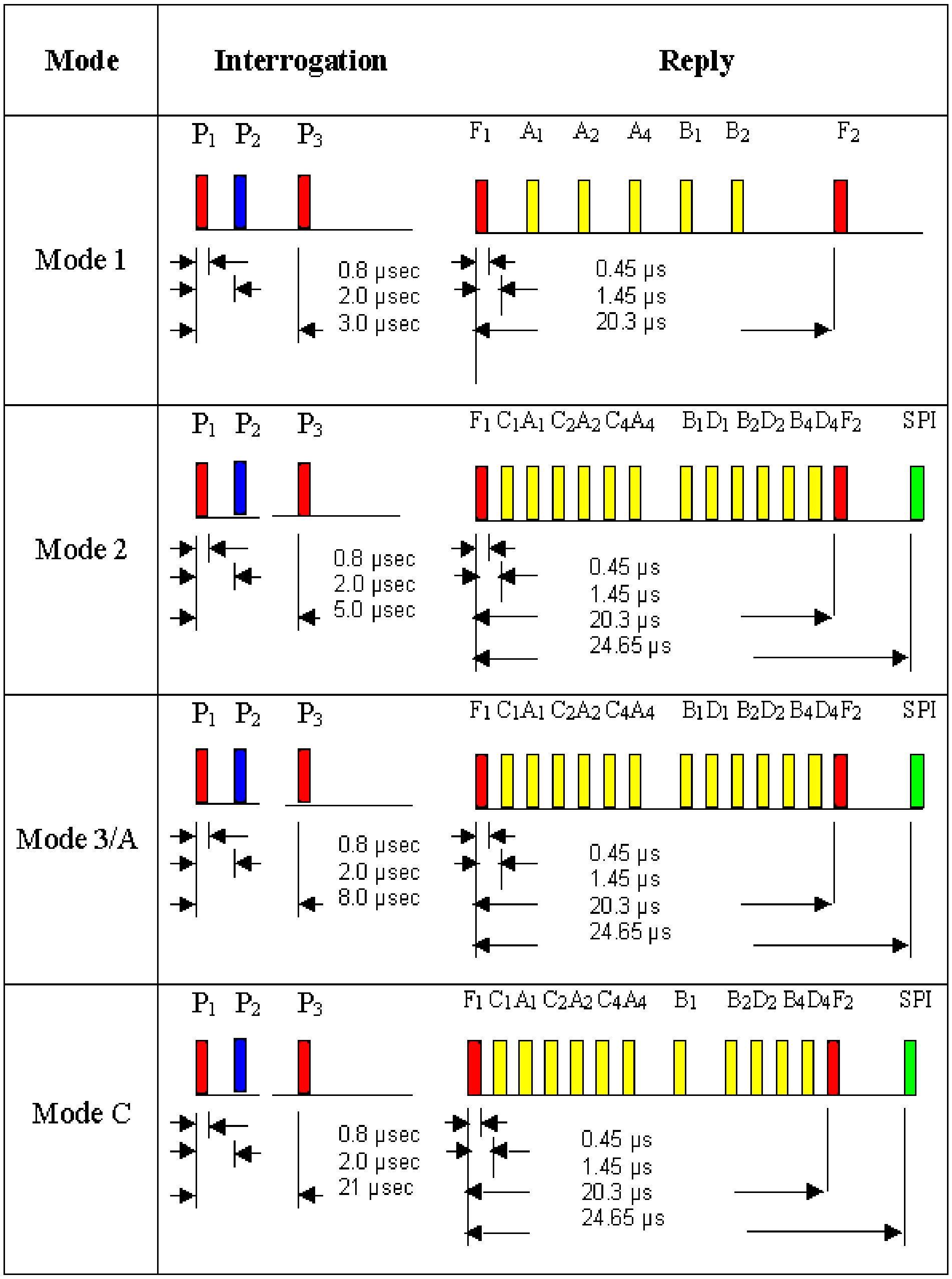


Fig.9 Mark X (SIF) Interrogations & Reply Codes For Different Modes

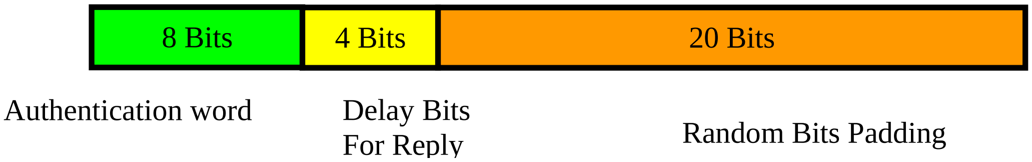


Fig.10.Mark XII Challenge Format

3.2.2 Proposed Secure Mode

The proposed system is based on transmitted interrogation /reply signal, which contain information about the transponder and the required code to be used in the reply. In addition, some of random bits should be added to change the nature of the interrogation signal. The basic block diagram of the proposed secure mode is shown in Fig.11. It starts it operation by coding/decoding the interrogation/reply signal. The coded/decoded signal is then subjected to substitution and permutation tables.

These tables can be generated from a chaotic source, which is based on the logistic map [8]. In addition the chaotic generator generates random bits, which are required to form the interrogation signal. The signal generated from the substitution and permutation tables is converted to a set of initial conditions. These initial conditions are then assigned to the cryptosystem with other logic circuits to start the encryption process. This can be repeated to N-rounds set by the cryptographer, to get the cipher interrogation signal.

The proposed cryptosystem has many advantages:

- It has the main features for strong cryptosystems.
- It has the main source of randomness (chaotic map).
- It has strong relation ships between blocks.
- It can resist the analytical and statistical attacks.

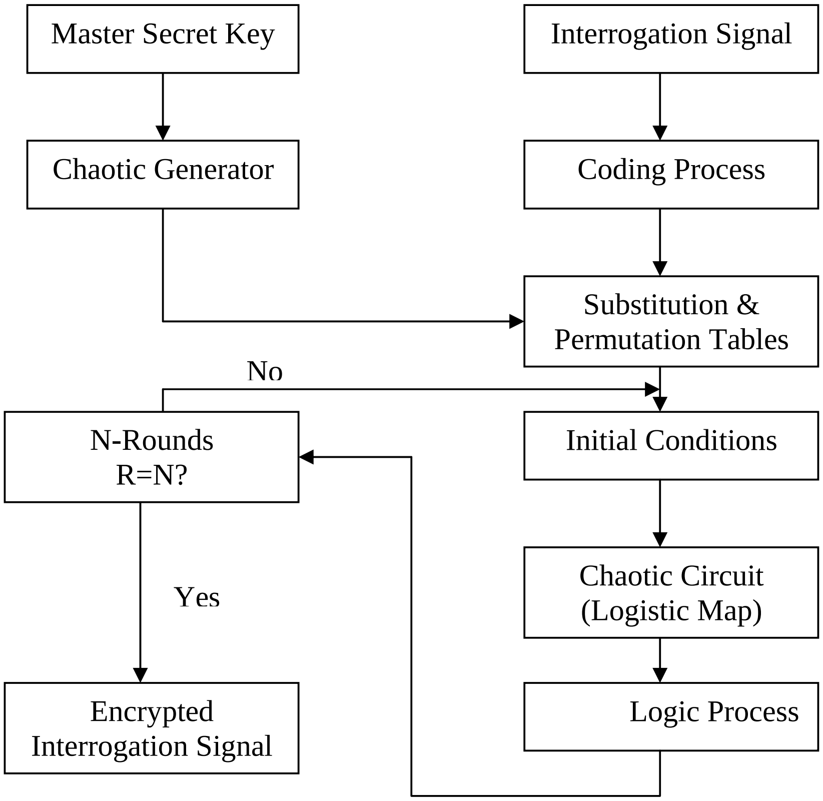


Fig.11 Proposed Cryptosystem for IFF Applications

4. Conclusion

The SSR have been evolved since the Second World War. An overview of eastern and western IFF systems has been introduced. The paper concentrates on the interrogation and reply signal formats, for different mode of operation. It also introduces a proposed cryptosystem to fit the IFF system. Most of electrical engineers are welling to get rid of chaos, but in this paper we introduce how to make use of chaos in the field of secondary surveillance radar. The proposed technique is based on the use of chaotic map, namely, logistic map, which has been already discussed and it is has been proven its security.

REFERENCES

[1] IEEE Standard Specifications for public key cryptography, IEEE std 1363-2000.
[2] Donglasr Stinson," Cryptography Theory and Practice", 2nd edition, Chapman & Hall/CRC, 2002.
[3] C. Michael Stevens," Secondary Surveillance Radar", Artech House Inc., Norwood, 1988.
[4] P. Honold, "Secondary Radar Fundamentals and Instrumentation", Heyden & Son Ltd., London, 1976.
[5] M. Scanlan, "Modern Radar Techniques", William Collins Sons & Co. Ltd., Chap. 6, p241-281, 1987.
[6] S. M. Weinstein, "An Electronic Scan Antenna for ATC Scan Acquisition", Journal of ATC, July-Sept., 1976.
[7] http://www.littongcs.com/products/3iff/iffqa.html
[8] G.L. Baker and J.P. Gollub, Chaotic Dynamics, An Introduction, Cambridge: C.U.P, 1990.