بسمه تعالی

keeloq code rolling

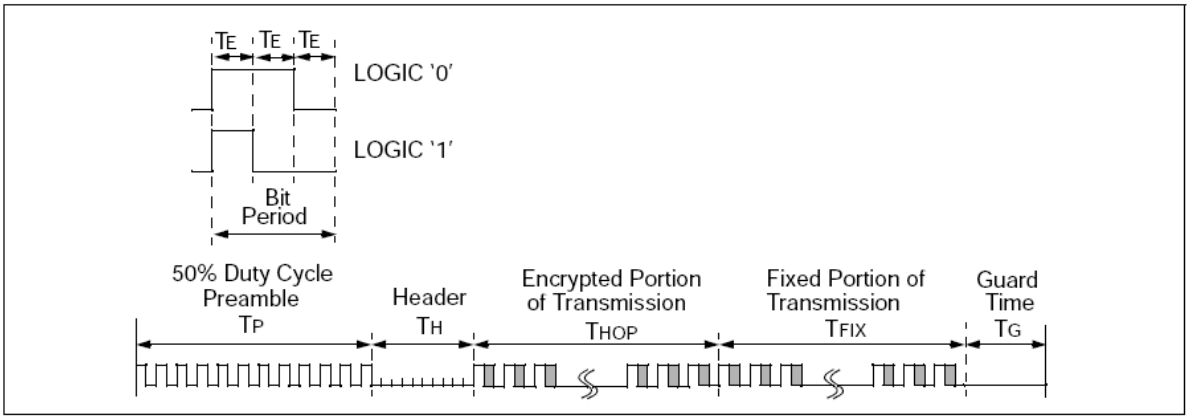
هر کد رولینگ کد هر ۶۵ هزار بار و تحت تنظیمات دیگر که در زمان پروگرم کردن صورت میگیرد هر ۱۹۲ هزار بار کد ارسال تکرار شده.

```
??F433MASKB66C0101001111111110111000010010101100100101101010000000000000010000A00037D170307T142441
??F433MASKB66C1011001001001010011110111011011001001011010100000000000000010000A00038D170307T142442
??F433MASKB66C0010110100000111111011101101100000100101101010000000000000010000A00037D170307T142443
??F433MASKB66C1000110100011001010110010001110100100101101010000000000000010000A00037D170307T142444
```

same button is pushed again. A code word that has been transmitted will not repeat for more than 64K transmissions. This provides more than 18 years of use before a code is repeated; based on 10 operations per day. Overflow information sent from the encoder can be used to extend the number of unique transmissions to more than 192K.

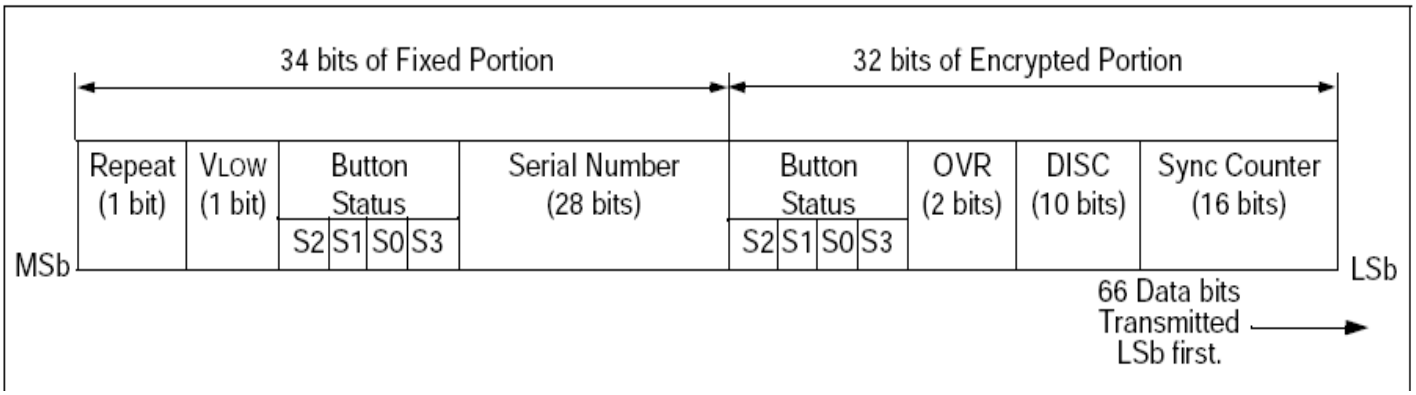
عناصر تشکیل دهنده کد رولینگ:

FIGURE 4-1: CODE WORD FORMAT



- یک سری پالسهای تکرار بنام preamble که حداقل ۱۲ سیکل یکسان است
- یک فاصله زمانی بنام header که تقریبا 15ms است
- ۳۲ بیت کد رمز شده به نام encryptio
- ۳۴ بیت کد فیکس که شامل ۲۸ بیت کد سریال ثابت که برای هر ریموت ثابت و متفاوت است + ۴ بیت مربوط به دکمه یک بیت تعیین کننده کاهش یا نرمال بودن ولتاژ باطری و بیت آخر , تکرار کد را مشخص میکند که اگر کد ۶۶ بیت یکبار بیشتر به طور پیوسته ارسال شد این بیت ۱ میشود.

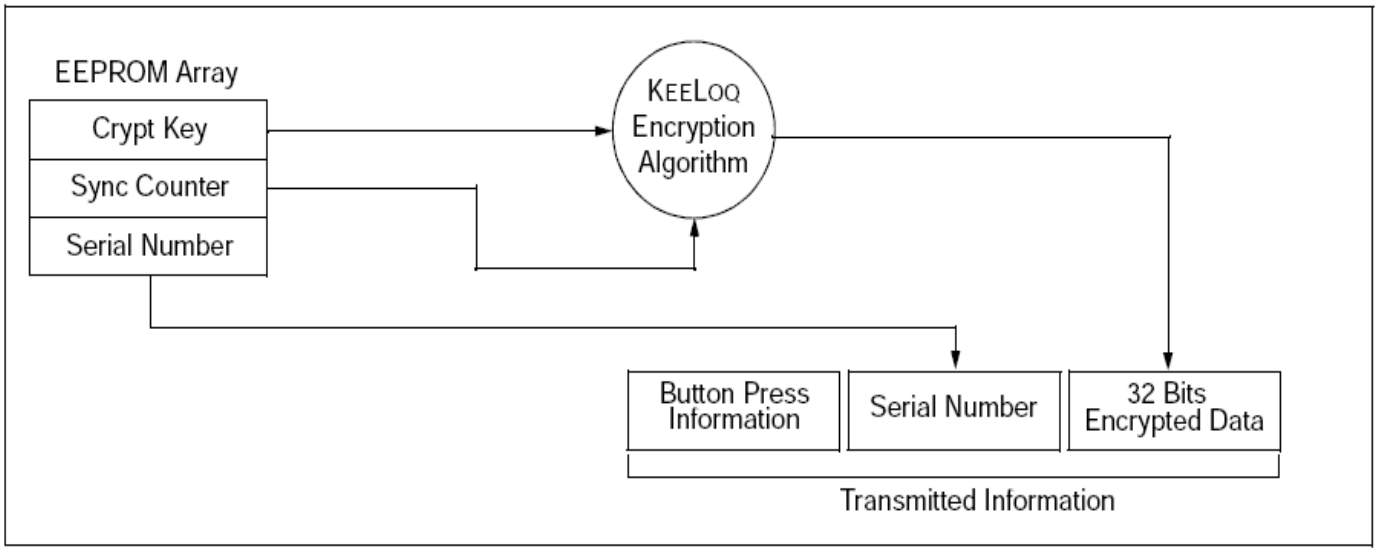
FIGURE 4-2: CODE WORD ORGANIZATION



: Encryption Code

این ۳۲ بیت تشکیل شده از یک کانتر ۱۶ بیتی + ۱۰ بیت کم ارزش کد سریال ریموت + ۲ بیت تعیین کننده اینکه کانتر ۱۶ بیتی باشد یا ۱۸ بیتی و ۴بیت که وضعیت دکمه ها میباشد.مجموع این ۳۲ بیت جهت encrypt شدن میبایست با کدی به نام crypt key ترکیب شود:

FIGURE 1-2: BUILDING THE TRANSMITTED CODE WORD (ENCODER)

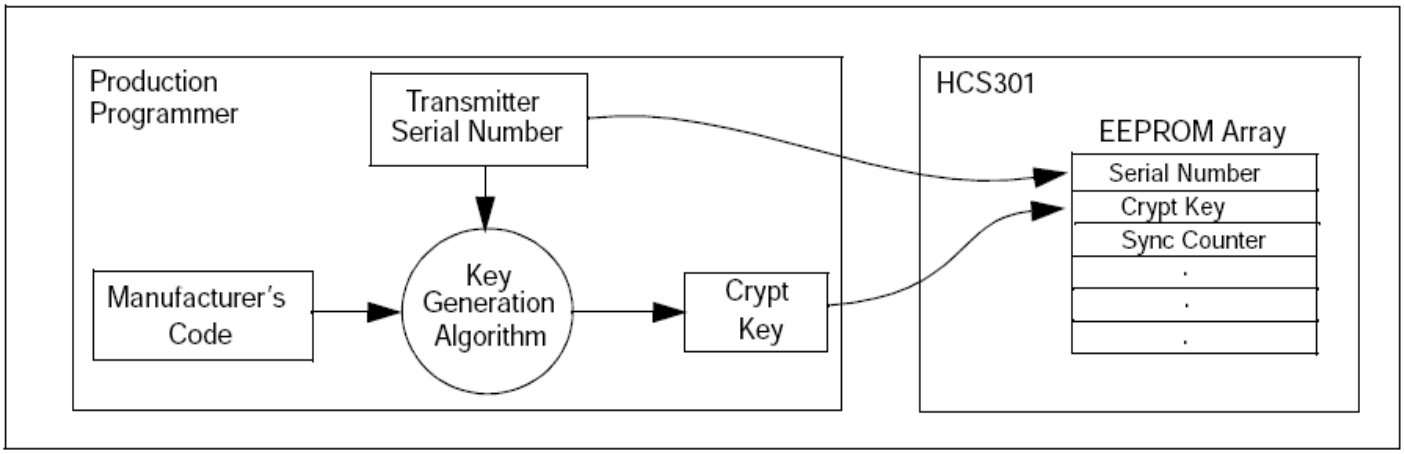


: crypt key

این کد متشکل از دو بخش است که باهم ترکیب شده که شامل :

- کد سریال ۲۸ بیت که برای هر ریموت متفاوت و ثابت است
- کد کارخانه ۶۴ بیت که برای همه ریموتهای یک شرکت هم فرستنده و هم گیرنده ثابت بوده .

FIGURE 1-1: CREATION AND STORAGE OF CRYPT KEY DURING PRODUCTION



:EEPROM

یک ریموت جهت ارسال کد نیاز دارد موارد زیر داخل حافظه eeprom آن یکبار ریخته شود حافظه eeprom

آیسیهای کیلوک قابل خواند نمیباشد .

TABLE 3-1: EEPROM MEMORY MAP

WORD ADDRESS	MNEMONIC	DESCRIPTION
0	KEY_0	64-bit encryption key (word 0) LSb's
1	KEY_1	64-bit encryption key (word 1)
2	KEY_2	64-bit encryption key (word 2)
3	KEY_3	64-bit encryption key (word 3) MSb's
4	SYNC	16-bit synchronization value
5	RESERVED	Set to 0000H
6	SER_0	Device Serial Number (word 0) LSb's
7	SER_1**(Note)**	Device Serial Number (word 1) MSb's
8	SEED_0	Seed Value (word 0)
9	SEED_1	Seed Value (word 1)
10	RESERVED	Set to 0000H
11	CONFIG	Config Word

Note: The MSB of the serial number contains a bit

- کد crypt key که ۶۴ بیت است که از ترکیب کد سریال با کد ۶۴ بیت کارخانه ایجاد شده
- مقدار کانتر که ۱۶ بیتی میباشد
- کد سریال ۲۸ بیت
- مقدار ۳۲ بیت عدد seed جهت حالت **Secure Learn**
- مقدار config که ۱۶ بیتی است که شامل موارد زیر است:

TABLE 3-2: CONFIGURATION WORD

Bit Number	Bit Description
0	Discrimination Bit 0
1	Discrimination Bit 1
2	Discrimination Bit 2
3	Discrimination Bit 3
4	Discrimination Bit 4
5	Discrimination Bit 5
6	Discrimination Bit 6
7	Discrimination Bit 7
8	Discrimination Bit 8
9	Discrimination Bit 9
10	Overflow Bit 0 (OVR0)
11	Overflow Bit 1 (OVR1)
12	Low Voltage Trip Point Select (VLOW SEL)
13	Baud rate Select Bit 0 (BSL0)
14	Baud rate Select Bit 1 (BSL1)
15	Reserved, set to 0

۱۰ بیت اول شامل ۱۰ بیت کم ارزش کد سریال بوده و بیت ۱۰ و ۱۱ میزان ۱۶ بیتی یا ۱۸ بیتی بودن کانتر است.بیت ۱۲ میزان سطح ولتاژ و بیت ۱۳ و ۱۴ آلفای هر بیت وبیت آخر هم رزرو شده میباشد.

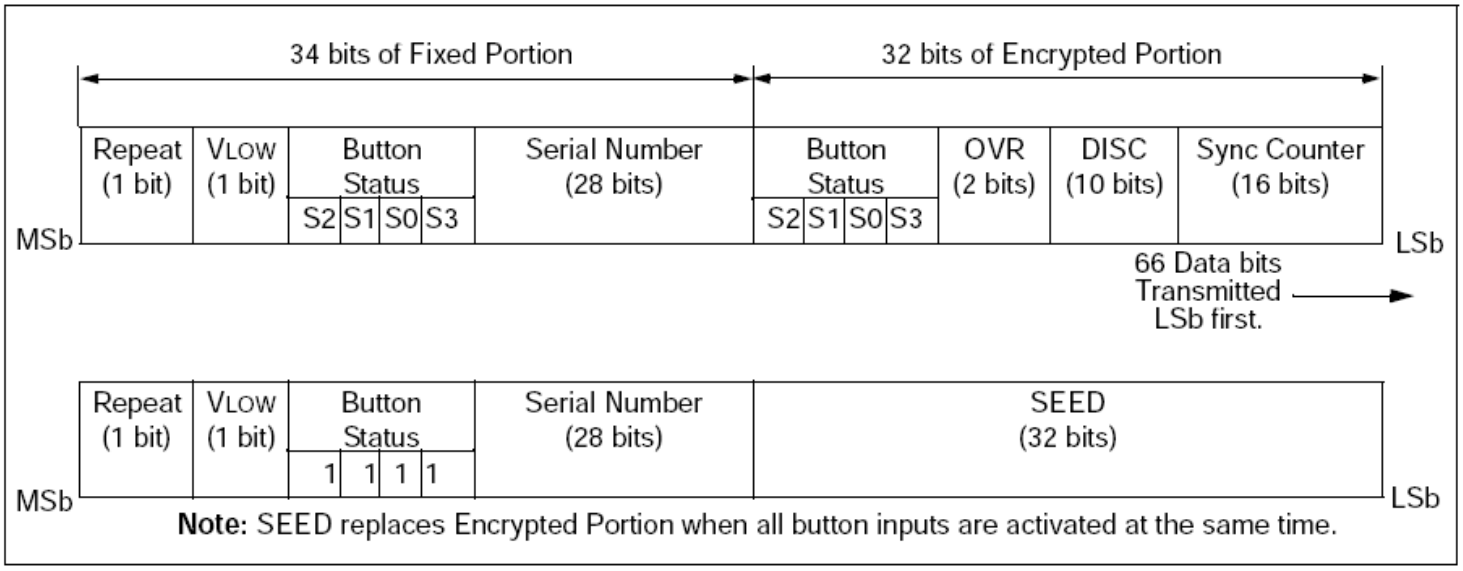
TABLE 3-3: BAUD RATE SELECT

BSL1	BSL0	Basic Pulse Element	Code Words Transmitted
0	0	400 µs	All
0	1	200 µs	1 out of 2
1	0	100 µs	1 out of 2
1	1	100 µs	1 out of 4

لرن کردن

نحوه لرن به سه صورت ساده – نرمال و رمز شده میباشد.در حالت لرن اطلاعات eetprom به گیرنده ارسال شده که در نوع **Secure Learn** اطلاعات رمز شده ارسال میشود و حتما باید تمام کلیدهای ریموت همزمان ابتدا زده شود سپس یکی از دکمه ها زده شود .در زدن همه دکمه ها کد ثابتی به نام seed که ۳۲ بیتی یا ۴۸ بیتی و یا ۶۰ بیتی میباشد جای کد هوپینگ مینشیند که این کد باید در ابتدا به گیرنده ارسال شود.

FIGURE 4-2: CODE WORD ORGANIZATION



Note: SEED replaces Encrypted Portion when all button inputs are activated at the same time.

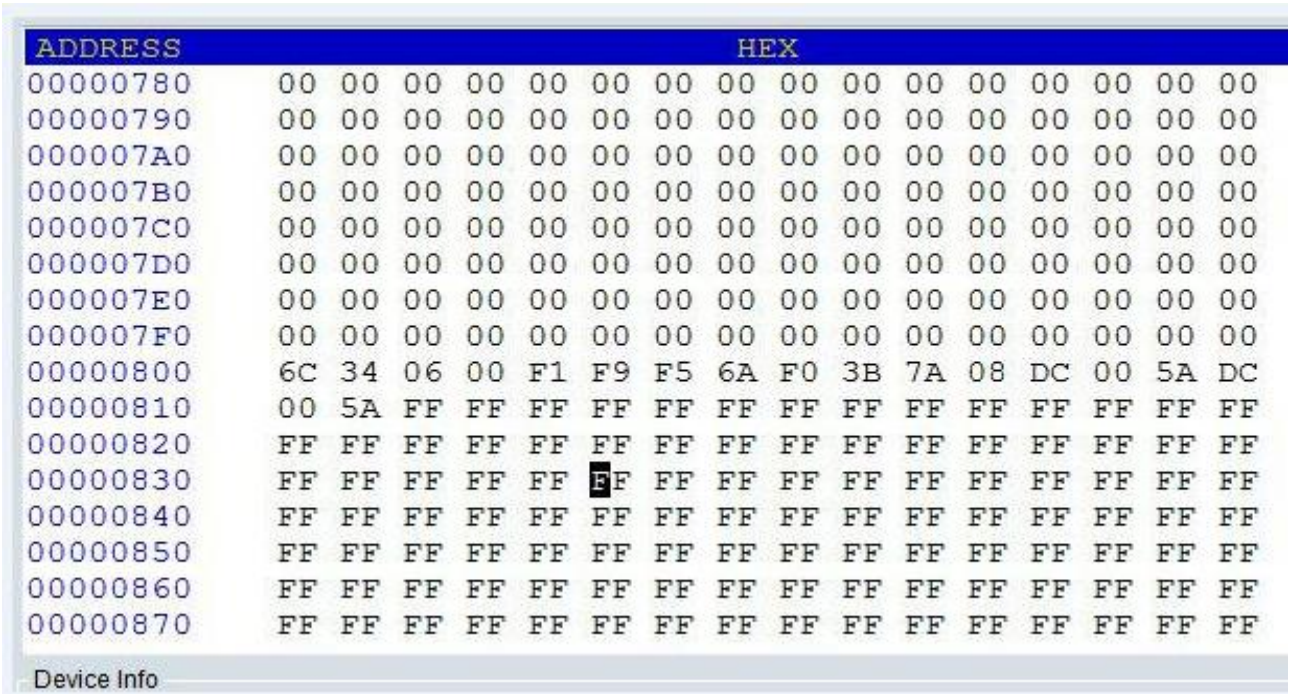
3.5 SEED_0, SEED_1 (Seed Word)

The 2-word (32-bit) seed code will be transmitted when all three buttons are pressed at the same time (see Figure 4-2). This allows the system designer to implement the secure learn feature or use this fixed code word as part of a different key generation/tracking process.

TABLE 5-1: PIN ACTIVATION TABLE

	Function	S3	S2	S1	S0
Standby	0	0	0	0	0
Hopping Code	1	0	0	0	1
	2	0	0	1	0
	-	-	-	-	-
	13	1	1	0	1
	14	1	1	1	0
Seed Code	15	1	1	1	1

نمونه کد eetprom میکرو bft :



ADDRESS	HEX															
00000780	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000790	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000007A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000007B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000007C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000007D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000007E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000007F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000800	6C	34	06	00	F1	F9	F5	6A	F0	3B	7A	08	DC	00	5A	DC
00000810	00	5A	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00000820	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00000830	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00000840	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00000850	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00000860	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00000870	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF

Device Info

پروگرم کردن hcs301:

جهت پروگرم باید موارد زیر ریخته شود :

- Crypt key که از ترکیب ۲۸ بیت کد سریال با ۶۴ بیت کد کارخانه ایجاد شده که اگر فرستنده و گیرنده را خودمان پروگرم کنیم میتوانیم یک کد توافقی تعیین کنیم و با قرار دادن در فرمول یا برنامه از پیش آماده کد crypt key را بدست آوریم.نمونه ای از برنامه های آماده که کد crypt key و کد دیکود هوپینگ ۳۲ بیت را با توجه مقادیر KEY بدست آمده به ما میدهد در زیر آمده .

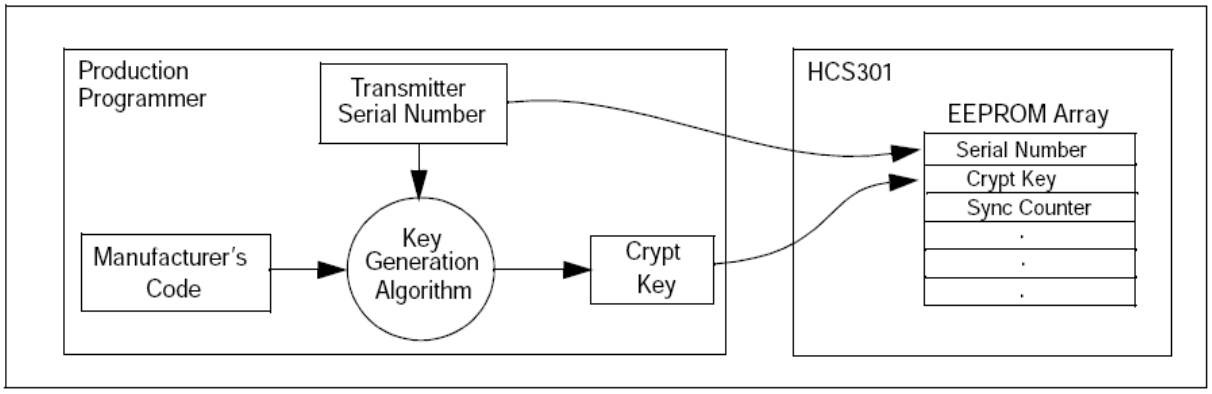
- کانتر ۱۶ بیتی که مقدار عدد شروع آن اختیاری است.
- ۲۸ بیت کد سریال ریموت
- Config ۱۶ بیتی

نحوه clone ریموت bft :

اگر کد hex حافظه فلش و eetprom یک bft قفل شکسته را در یک bft خام کپی کنیم عین ریموت اول ایجاد شده .ولی اگر بخواهیم با اطلاعات eetprom یک ریموت bft کل ریموتهای این شرکت را clone کنیم باید ابتدا موارد زیر انجام شود.ابتدا" هر ریموتی که قرار است clone شود باید یک بار وقتی شخص مخاطب دکمه ارسال میزند کد ۶۶ بیت آن را capture کنیم تا کد سریال و کد هوپینگ و کد دکمه ها از آن استخراج شودسپس مراحل زیر انجام شود :

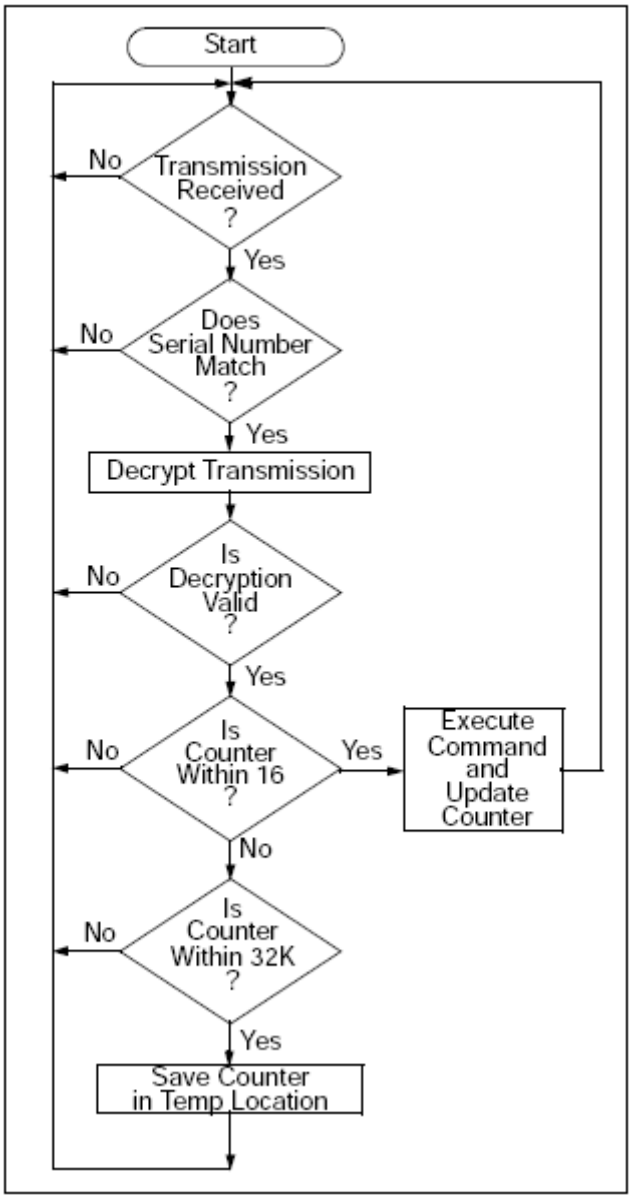
- استخراج کد ۶۴ بیت کارخانه از crypt key موجود در eetprom ریموت حک شده اولیه و ترکیب آن با کد سریال ریموت جدید که قرار است clone شود جهت ایجاد کد crypt key جدید و قرار دادن آن در eetprom میکرو bft خام.

FIGURE 1-1: CREATION AND STORAGE OF CRYPT KEY DURING PRODUCTION



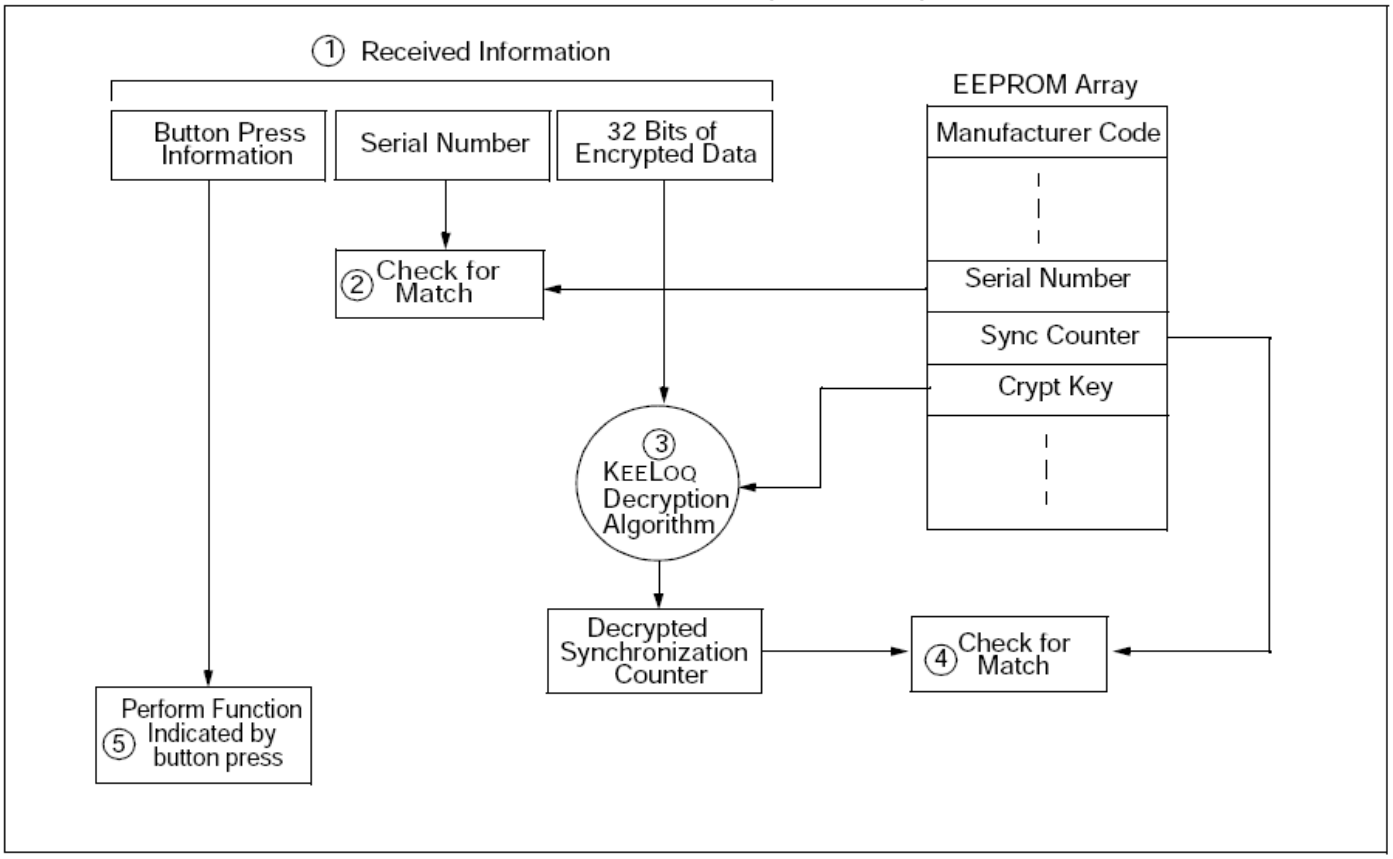
- استخراج مقدار کانتر (مقدار عدد کانتر باید با نمونه ای که قرار است clone شود یکی باشد .عقبتر نباشد ولی اگر تعدای جلوتر باشد موردی پیش نمیاید در بعضی مواقع اگر عدد کانتر کمی زیادتر از حد مشخص شده جلو باشد با دوبار زدن دکمه ارسال کد مشکل حل میشود و مقدار کانتر جدید جایگزین مقدار قبلی میشود)

FIGURE 7-2: TYPICAL DECODER OPERATION



استخراج مقدار کانتر از کد هوپینگ نمونه clone شده و کد crypt key جدید برای این ریموت که در مرحله قبل ایجاد شده.

FIGURE 1-3: BASIC OPERATION OF RECEIVER (DECODER)



- حال مقدار crypt key - کد سریال -کانتر – config و seed را در eetprom میکرو bft خام قرار میدهیم .خود میکرو با زدن اولین دکمه کانتر + config را که ۳۲ بیت هست با ۶۴ بیت crypt key در فرمول قرار داده و کد هوپینگ ۳۲ بیت جدید را ایجاد کرده و بقیه موارد را نیز به ترتیب میچیند.

FIGURE 1-2: BUILDING THE TRANSMITTED CODE WORD (ENCODER)

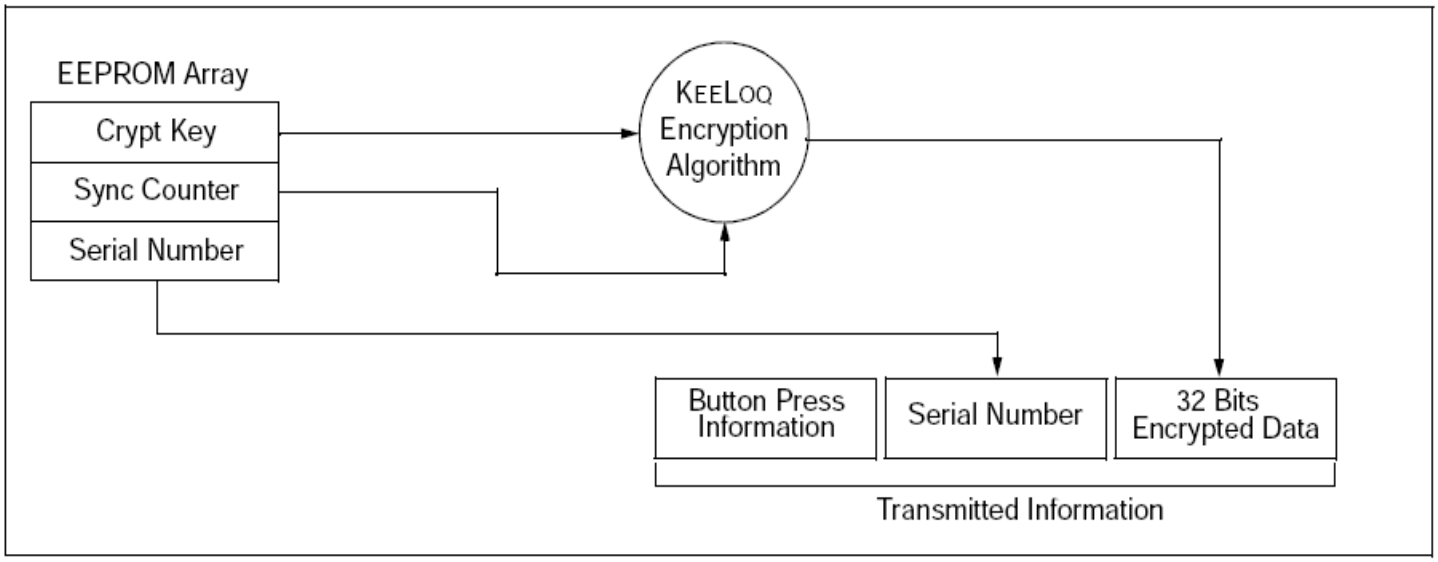


FIGURE 4-2: CODE WORD ORGANIZATION