A LOW COST IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD ALGORITHM USING 8085A MICROPROCESSOR

Salim M. Wadi[1*], Nasharuddin Zainal[1†],

[1]*Department of Electrical, Electronic and System Engineering , UKM University, Malaysia*

ABSTRACT

The high security communication systems became an urgent need in recent years for both governments and peoples desiring protection from signal interception. The implementation of advanced encryption standard algorithm is important requirement where many researches proposed different items to this purpose. Some papers used microcontrollers as CPU item to implement AES algorithm. A simply item proposed in this paper to speedy, low cost implementation of Rijndael Advanced Encryption Standard (AES) cryptographic algorithm which is 8085A microprocessor. The results prove the implementation is effective through competitive cost, low hardware requirements, and reasonable speeds compared with other implementation methods.

Keywords: AES, 8085 processor, ALP, microcontroller, Rijndael.

1. INTRODUCTION

Transmission of important electronic financial transactions and digital touch applications must be fast and very secure to achieve the requirements for security, integrity, and non reproduction of exchanged information. Cryptography provides a method for securing and authenticating the transmission of information over insecure channels. For these reasons, large number of research were done to developing a high performance encryption system (Daemen and Rijmen 2002; Tran et al 2008) .

Vincent Rijmen and Joan Daeman were innovated new encryption system which referred to as advanced encryption standard (AES) in 2001(Daemen and Rijmen 2002). The Advanced Encryption Standard (AES) was successor alternative algorithm to the Data Encryption Standard (DES) which suffers from theoretical weaknesses in the encryption as well as successful brute force attacks carried out against the algorithm(Orlando et al 2008). The implementations of AES are carryout into two ways, one by FPGA and other by microcontroller.

* Presenter: Email: salimmw@eng.ukm.my

† Presenter: Email: nzainal@hotmail.com

Orlando, J.et al. (Orlando et al 2008) used a bit-serial approach to built their architecture utilizing FPGA with focusing on low cost resulted in a design well-suited for SoC implementations. Proposed implementation give good results in term throughput/slice ratio and cost can be reduced while maintaining a suitable operating speed with minimization of redundancies.

Hyubgun Lee et al. (Hyubgun et al 2009) were presented the sensor network with high security to analyze the communication efficiency through performance evalution of AES ciphering system depending on data length, and cost of operation per hop according to the network scale. The authors concludes that if the scale of the sensor network increased, this lead to doubled the delay as well as increasing in the energy disbursed.

Kai Schramm et al. (Kai and Christ 2004) were design an particularistic lab project in IT security which combines topics of computer architecture, cryptography and software engineering. The professed that undergraduate Students of EE/CS are used the proposed lab to worthily carryout the Advanced Encryption Standard (AES) on a smart card using Atmel ATMega163 Reduced Instruction Set Computer (RISC) microcontroller in assembly.

Gielata et al. (Gielata et al 2008) were proposed special architecture using FPGA to get speedy and flexibility implementation to 128-ASE algorithm. The hardware performance was been evaluated depending on four parameters as, number of used resources, maximum clock frequency, latency measured in number of clocks, throughput measured in bytes per second.

In this paper simply item proposed to low cost implementation of AES algorithm using 8085 microprocessor as processing tool with very effective manner and reasonable speed.

the paper is organized as, in section2 clarify short for AES algorithm. Explain to implementation method show in section3. Results and comparison in section 4 and conclusion in section 5.

2- AES ALGORITHM

AES is based on Rijndael algorithm which is a symmetric block cipher that processes fixed data of 128-bit blocks. It supports key sizes of 128, 192 and 256 bits and consists of 10, 12 or 14 iteration rounds, respectively. In this paper, we will present the 128-bit version of AES with 10 rounds. Each round mixes the data with a round key, which is generated from the encryption key. The AES encryption structure is shown in figure 1 (Orlando et al 2008; Schmidt et al 2009). The cipher maintains an internal, 4×4 matrix of bytes referred to as State, on which the operations are performed. Initially, State is filled with the input data block and XOR-ed with the encryption key. Regular rounds consist of operations called SubBytes, ShiftRows, MixColumns and AddRoundKey. The last round bypasses MixColumns transformation. SubBytes transformation uses 16 identical 256-byte substitution table called S-box as shown in table1(Majithia and Dinesh 2010).

SubBytes can be implemented either by computing the substitution or using look-up-table (LUT). ShiftRows is a cyclic left shift of the second, third and fourth row of State by one, two, and three bytes, respectively. MixColumns performs a modular polynomial multiplication on each column.

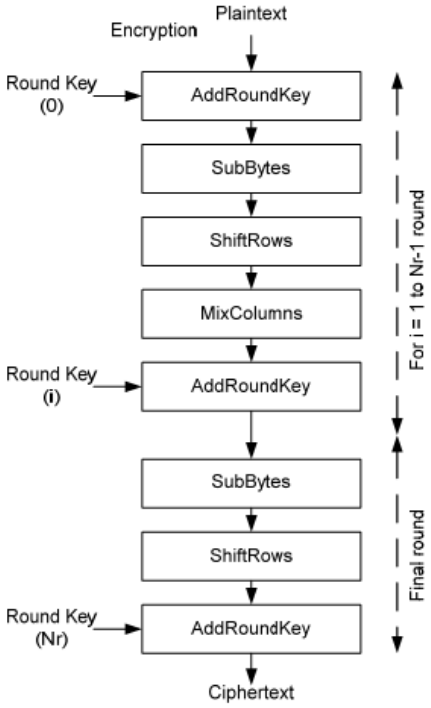

Figure 1: AES Encryption Structure.

During each round, AddRoundKey performs XOR with State and the round key. Round key generation (key expansion) includes S-box substitutions, word rotations, and XOR operations performed on the encryption key. Depending on the security level required for the application, AES uses different key length (Muhammad and Syed 2009; Ming et al 2007).

Table 1: S-Box based on Galois Field GF (2^8)

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

3- PROPOSED IMPEMENTATION:

The best encryption algorithm that is easy to implement in software and in hardware (Orlando et al 2008). Inventors of AES algorithm designed it with an idea in mind of ability for its efficient execution using different platform such as CPU, ASICs, and FPGA. Microprocessor is cheap and easy programmed and has high efficiency. For these reasons, we choose the microprocessor to implement the AES algorithm. A 8085 microprocessor is used to implement AES algorithm in this paper because it compatible with proposed requirements (low cost, good speed, and efficiency). In this implementation, SubBytes transform implemented using lookup table (LUT). MixColumns transform implemented using XOR operations with mod to (11B) because the state in hexadecimal numbers. ShiftRows and AddRoundKey transforms are easily executed using 8085 microprocessor.

A block diagram to proposed implementation shown in figure 2, which consist from:

- 8085A microprocessor: this processor is from Intel family, 8 bit processor, operating frequency is 5MHz.
- EEPROM: about 0.978 Kbyte used to save the operating programs and S Box and inverse S Box.
- RAM: about 0.76Kbyte
- Keyboard and 7-sigment display to input the plaintext and key block as inputs and display the cipher text as outputs.
- I/O ports.

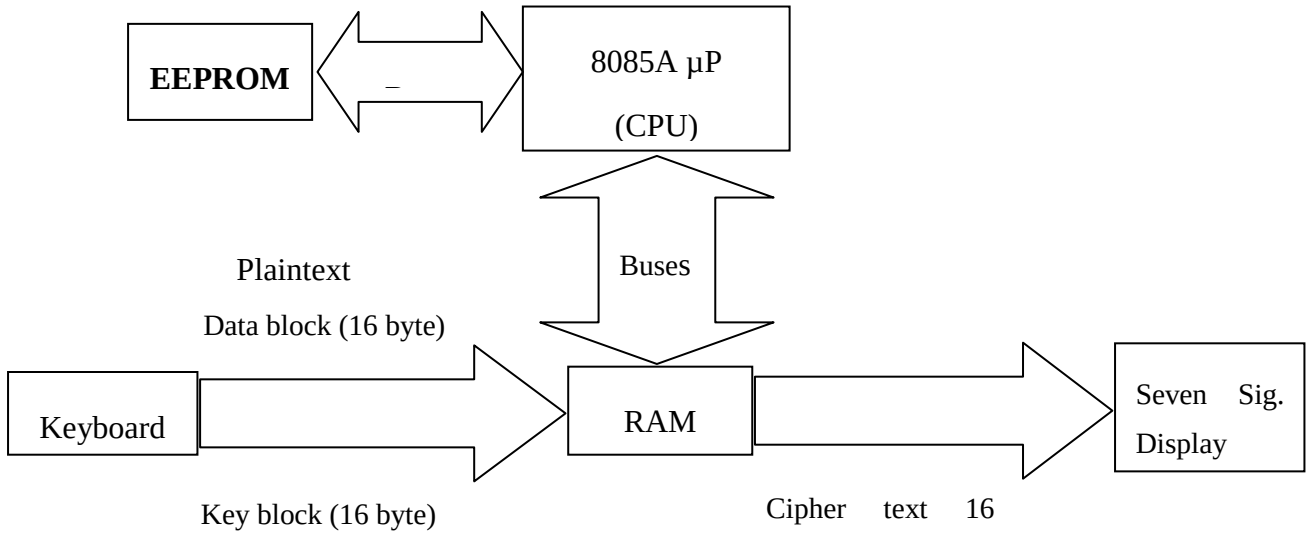

Figure 2: Block diagram of device.

4- RESULT:

Performance of the proposed implementation was evaluated according to the below parameters:

Simplicity: the proposed implementation is very simple as hardware see fig.2 as well as the programming requirements is very easy where assembly language used to write the essential programs to employment the microprocessor.

Cost: As known to all, the price of 8085 microprocessor IC is very low about 1-1.5 $ which is the mean part of the proposed circuit and this is true for other parts, therefore we think that the cost of the complete circuit is very low compared with other implementation using FPGA or microcontrollers.

Speedy: Table 2 shown the implementation results to the circuit. From this table we see that the speed of complete implementation is reasonable and compatible most applications as example to researches purpose.

Table 2: The implementation results

Implementation of AES	Suggested implement.
Type of processor	8085A µP
Frequency	5 MHz
Time of encryption	17.66ms
No. of CPU Cycle (for one block data)	4500
EEPROM needed	0.978 Kbyte (contain the program memory)
Volatile memory	0.76Kbyte
Internal registers	7(8-bit),1 (16-bit)

To demonstrate the effectiveness of proposed method , we compare the proposed implementation with other two implementations, which used the microcontroller. We don't find implementation using any type of microprocessor especially 8085 microprocessor. Table 3 shown the comparison.

From table 3, we see that the consumption time in proposed method near of the proposed method in (Kai and Christ 2004) but the memory required is little in proposed method and is cheaper. In compare with implementation that proposed in (Hyubgun et al 2009) the difference in terms of time carryout and memory required is very high. Therefore, we conclude that the proposed method is effective in terms of cost, time consumption, simplicity, and required peripherals such as memory.

Table 3:Comparison of Suggested Implementation Results with Proposed Implementation in [4, 5]

Implementation of AES	Suggested implement.	Prop. imp. in [4]	Prop. imp. in [5]
Type of processor	8085A µP	ATmega644p µC	ATMega163 µC
Frequency	5 MHz	12 MHz	3.57 MHz
Time of encryption	17.66ms	449 ms	22.50 ms
EEPROM needed	0.978 Kbyte (contain the program memory)	8 Kbyte	32 byte
Volatile memory	0.76Kbyte	Not found	2.234 Kbyte
Internal registers	7(8-bit),1 (16-bit)	Not found	32 (8-bit)

5-CONCLUSION:

In this paper we proposed the novel implementation to AES algorithm using 8085 microprocessor. The 8085 microprocessor is low cost and effectiveness with reasonable speed. the performance of proposed implementation is evaluated in terms of cost and time required to carry out the AES algorithm. As a result the time and cost of the proposed implementation is good in compare with other implementation.

6-ACKNOWLEDGEMENT

The authors would like to thank staff of Department of Electrical, Electronic and Systems Engineering in Faculty of Engineering and Built Environment, Universiti Kebangsaan Malaysia for assist in the completion of this work and also UKM for UKM-GUP-2011-060 fund.

References:

Daemen J and Rijmen V (2002). The design of AES-The Advance Encryption Standard, Springer-Verlag.

Tran M. T., Bui DK and Duong AD (2008) Gray S-Box for Advanced Encryption Standard. In Proceeding of International Conference on Computational Intelligence and Security, Vol. 1, pp. 253-258.

Orlando J., Hernandez T., Sodon MA and Numan K (2008). A Low Cost Advanced Encryption Standard (AES) Co-Processor Implementation. JCS&T, Vol.8 No.1 pp 8-14.

Hyubgun L., Kyounghwa L., and Young-Tae S (2009). AES Implementation and Performance Evaluation on 8-bit Microcontrollers. International Journal of Computer Science and Information Security, Vol. 6, No. 1.

Kai S and Christ P (2004) IT Security Project: Implementation of the Advanced Encryption Standard (AES) on a Smart Card. in Proceedings of the International Conference on Information Technology: Coding and Computing IEEE.

Gielata A., Russek P., and Wiatr K. (2008). AES hardware implementation in FPGA for algorithm acceleration purpose. in Proceeding of International Conference on Signals and Electronic Systems, pp. 137-140.

Schmidt JM, Hutter M, and Plos T (2009) Optical Fault Attacks on AES: A Threat in Violet. in Workshop on Fault Diagnosis and Tolerance in Cryptography, pp. 13-22.

Majithia S and Dinesh K (2010). Implementation and Analysis of AES, DES and Triple DES on GSM Network. IJCSNS, VOL.10 No.1, pp 298-300.

Muhammad HR, and Syed MQ (2009) A Novel FPGA Implementation of AES-128 using Reduced Residue of Prime Numbers based S-Box. IJCSNS, VOL.9 No.9, pp.305 -309.

Ming-Haw J, Chen JH, and Chen ZH (2007) Diversified Mixcolumn Transformation of AES. IEEE.

Appendix A Example of AES Encryption

Table1: key expansion example

Key words	Auxiliary function
W0=0f 15 71 c9 W1=47 d9 e8 59 W2=0c b7 ad d6 W3=af 7f 67 98	Rot word (W3)= 7f 67 98 af =x1 Sub word (x1) =d2 85 46 79 =y1 R con (1) = 01 00 00 00 Y1 ⊕ Rcon(1) = d3 85 46 79 = z1
W4 = W0 ⊕ Z1 = dc 90 37 b0 W5= W4 ⊕ W1= 9b 49 df e9 W6= W5 ⊕ W2= 97 fe 72 3f W7= W6 ⊕ W3= 38 81 15 a7	Rot word (W7)= 81 15 a7 38 =x2 Sub word (x2) = 0c 59 5c 07 =y2 R con (2) = 02 00 00 00 Y2 ⊕ Rcon(2) = d3 85 46 79 = z2
W8 = W4 ⊕ Z2 = d2 c9 6b b7 W9= W8 ⊕ W5 = 49 80 b4 5e W10= W9 ⊕ W6 = de 7e c6 61 W11= W10 ⊕ W7 =e6 ff d3 c6	Rot word (W11)= ff d3 c6 e6 =x3 Sub word (x3) = 16 66 b4 8e =y3 R con (3) = 04 00 00 00 Y3 ⊕ Rcon(3) = 12 66 b4 8e = z3
W12= W8 ⊕ Z3 = c0 af df 39 W13= W12 ⊕ W9 = 89 2f 6b 67 W14= W13 ⊕ W10= 57 51 ad 06 W15= W14 ⊕ W11= b1 ae 7e c0	Rot word (W15)= ae 7e c0 b1 = x4 Sub word (x4) = e4 f3 ba c8 =y4 R con (4) = 08 00 00 00 Y4 ⊕ Rcon(4) = ec f3 ba c8 = z4
W16= w12 ⊕ Z4 = 2c 5c 65 f1 W17= w16 ⊕ W13 = a5 73 0e 96 W18= w17 ⊕ W14 = f2 22 a3 90 W19= w18 ⊕ W15 = 43 8c dd 50	Rot word (W19)= 8c dd 50 43 = x5 Sub word (x5) = 64 c1 53 1a =y5 R con (5) = 10 00 00 00 Y5 ⊕ Rcon(5) = 74 c1 53 1a = z5
W20= W16 ⊕ Z5 = 58 9d 36 eb W21= W20 ⊕ W17 = fd ee 38 7d W22= W21 ⊕ W18 = 0f cc 9b ed W23= W22 ⊕ W19 = 4c 40 46 bd	Rot word (W23)= 40 46 bd 4c = x6 Sub word (x6) = 09 5a 7a 29 =y6 R con (6) = 20 00 00 00 Y6 ⊕ Rcon(6) = 29 5a 7a 29 = z6
W24= W20 ⊕ Z6 = 71 c7 4c c2 W25= W24 ⊕ W21 = 8c 29 74 bf W26= W25 ⊕ W22 = 83 e5 ef 52 W27= W26 ⊕ W23 = cf a5 a9 ef	Rot word (W27) = a5 a9 ef cf = x7 Sub word (x7) = 06 d3 df 8a = y7 R con (7) = 40 00 00 00 Y7 ⊕ Rcon(7) = 46 d3 df 8a = z7
W28= W24 ⊕ Z7 = 37 14 93 48 W29= W28 ⊕ W25 = bb 3d e7 f7 W30= W29 ⊕ W26 = 38 d8 08 a5 W31= W30 ⊕ W27 = f7 7d a1 4a	Rot word (W31) = 7d a1 4a f7 = x8 Sub word (x8) = ff 32 d6 68 = y8 R con (8) = 80 00 00 00 Y8 ⊕ Rcon(8) = 7f 32 d6 68 = z8
W32= W28 ⊕ Z8 = 48 26 45 20 W33= W32 ⊕ W29 = f3 1b a2 d7 W34= W33 ⊕ W30 = cb c3 aa 72 W35= W34 ⊕ W31 = 3c be 0b 38	Rot word (W35) = be 0b 38 3c = x9 Sub word (x9) = ae 2b 07 eb = y9 R con (9) = 1b 00 00 00 Y9 ⊕ Rcon(9) = b5 2b 07 eb = z9
W36= W32 ⊕ Z9 = fd 0d 42 cb W37= W36 ⊕ W33 = 0e 16 e0 1c W38= W37 ⊕ W34 = c5 d5 4a 6e W39= W38 ⊕ W35 = f9 6b 41 56	Rot word (W39) = 6b 41 56 f9 = x10 Sub word (x10) = 7f 83 b1 99 = y10 R con (10) = 36 00 00 00 Y10 ⊕ Rcon(10) = 7f 83 b1 99 = z10

W40= W36 ⊕ Z10 = b4 8e f3 52 W41= W40 ⊕ W37 = ba 98 13 4e W42= W41 ⊕ W38 = 7f 4d 59 20 W43= W42 ⊕ W39 = 86 26 18 76	

Table 2: AES encryption example

Start of round	After sub Byte	After Shift Ro.	After Mix col.	Round Key
01 89 fe 76 23 ab dc 54 45 cd ba 32 67 ef 98 10				0f 47 0c af 15 d9 b7 7f 71 e8 ad 67 c9 59 d6 98
0e ce f2 d9 36 72 6b 2b 34 25 17 55 ae b6 4c 88	ab 8b 89 35 05 40 7f f1 18 3f f0 fc e4 4e 2f c4	ab 8b 89 35 40 7f f1 05 f0 fc 18 3f c4 e4 4e 2f	b9 94 57 75 c4 8e 16 51 47 20 9a 3f c5 d6 f5 3b	dc 9b 97 38 90 49 fe 81 37 df 72 15 b0 e9 3f a7
65 0f c0 4d 74 c7 e8 d0 70 ff e8 2a 75 3f ca 9c	4d 76 ba e3 92 c6 9b 70 51 16 9b e5 9d 75 74 de	4d 76 ba e3 c6 9b 70 92 9b e5 51 16 de 9d 75 74	8e 22 db 12 b2 f2 dc 92 df 80 f7 c1 2d c5 1e 52	d2 49 de e6 c9 50 7e ff 6b b4 c6 d3 b7 5e 61 c6
5c 6b 05 f4 7b 72 a2 6d b4 34 31 12 9a 9b 7f 94	4a 7f 6b bf 21 40 3a 3c 8d 81 c7 c9 b8 14 d2 22	4a 7f 6b bf 40 3a 3c 21 c7 c9 8d 81 22 b8 14 d2	b1 c1 0b cc ba f3 8b 07 f9 1f 6a c3 1d 19 24 5c	c0 89 57 b1 af 2f 51 ae df 6b ad 7e 39 67 06 c0
71 48 5c 7d 15 dc da a9 26 74 c7 bd 24 7e 22 9c	a3 52 4a ff 59 86 57 d3 f7 92 c6 7a 36 f3 93 de	a3 52 4a ff 86 57 d3 59 c6 7a f7 92 de 36 f3 93	d4 11 fe 0f 3b 44 06 73 cb ab 62 37 19 b7 07 ec	2c a5 f2 43 5c 73 22 8c 65 0e a3 dd f1 96 90 50
f8 b4 0c 4c 67 37 24 ff ae a5 c1 ea e8 21 97 bc	41 8d fe 29 85 9a 36 16 e4 06 78 87 9b fd 88 65	41 8d fe 29 9a 36 16 85 78 87 e4 06 65 9b fd 88	2a 47 c4 48 83 e8 18 ba 84 18 27 23 eb 10 0a f3	58 fd 0f 4c 9d ee cc 40 36 38 9b 46 eb 7d ed bd
72 ba cb 04 1e 06 d4 fa b2 20 bc 65 00 6d e7 4e	40 f4 1f f2 72 6f 48 2d 37 b7 65 4d 63 3c 94 2f	40 f4 1f f2 6f 48 2d 72 65 4d 37 b7 2f 63 3c 94	7b 05 42 4a 1e d0 20 40 94 83 18 52 94 c4 43 fb	71 8c 83 cf c7 29 e5 a5 4c 74 ef a9 c2 bf 52 ef
0a 89 c1 83 d9 f9 c5 e5 d8 f7 f7 fb 56 7b 11 14	67 a7 78 97 35 99 a6 d9 61 68 68 0f b1 21 82 fa	67 a7 78 97 99 a6 d9 35 68 0f 61 68 fa b1 21 82	ec 1e c0 80 0c 50 53 c7 3b d7 00 ef b7 22 72 e0	37 bb 38 f7 14 3d d8 7d 93 e7 08 a1 48 f7 a5 4a
db a1 f8 77 18 6d 8b ba a8 30 08 4e	b9 32 41 f5 ad 3c 3d f4 c2 04 30 2f	b9 32 41 f5 3c 3d f4 ad 30 2f c2 04	b1 1a 44 17 3d 2f ec b6 0a 6b 2f 42	48 f3 cb 3c 26 1b c3 be 45 a2 aa 0b

ff d5 d7 aa	16 03 0e ac	ac 16 03 0e	9f 68 f3 b1	20 d7 72 38
f9 e9 8f 2b 1b 34 2f 08 4f c9 85 49 bf bf 81 89	99 1e 73 f1 af 18 15 30 84 dd 97 3b 08 08 0c a7	99 1e 73 f1 18 15 30 af 97 3b 84 dd a7 08 08 0c	31 30 3a c2 ac 71 8c c4 46 65 48 eb 6a 1c 31 62	fd 0e c5 f9 0d 16 d5 6b 42 e0 4a 41 cb 1c 6e 56
cc 3e ff 3b a1 67 59 af 04 85 02 aa a1 00 5f 34	4b b2 16 e2 32 85 cb 79 f2 97 77 ac 32 63 cf 18	4b b2 16 e2 85 cb 79 32 77 ac f2 97 18 32 63 cf		b4 8e f3 52 ba 98 13 4e 7f 4d 59 20 86 26 18 76
ff 3c e5 b0 3f 53 6a 7c 08 e1 ab b7 9e 14 7b b9				