SUPPLEMENTARY MATERIALS 2

Title : « Securiting The Light Escaping In a Li-Fi Network Environment »

Author(s) : Dibson Diambeki, Reagan Mandiya, Kyandoghere Kyamakya, Selain Kasereka

According to the studies carried out, Li-Fi presents a better security than its competitor Wi-Fi, by the fact that the Li-Fi connection works only under a light cone, that is to say in Line of sight (LoS). The light waves can not cross obstacles, these waves are confined in a hermetically sealed space. Unlike radio waves that we find everywhere in nature, can be easily listened to by anyone with knowledge of software allowing sniffing. It is in this hypothesis that we affirm the weakness of Wi-Fi.

Nevertheless, the advantage of Li-Fi communication by the fact that light cannot pass through walls, is not a convincing argument to ensure data security, a threat such as eavesdropping can occur when there is a gap between the floor and the door, through windows, light can spread between them and our network could be vulnerable, so to face this problem, we conceived the idea of implementing an AES type cryptographic algorithm to ensure the security of data flow exchanges in the system and set up a captive portal to authenticate users in the network.

« This project is developed in an experimental framework to show the world the benefits of Li-Fi technology and how to secure the light of its bulbs that could spread everywhere and be accessible by anyone. »

1. Overview of the AES algorithm

AES (Advanced Encryption Standard) is a symmetric block cipher algorithm used worldwide to ensure data security. It includes three block cipher algorithms: AES-128, AES-192 and AES-256. Each code encrypts and decrypts data in 128 bit blocks using 128, 192, and 256 bit cryptographic keys, respectively. Symmetric or secret key codes use the same key for encryption and decryption. The sender and the recipient must therefore know and use the same secret key. It is an iterative algorithm and each iteration is called a round. The total number of rounds (Nr) is 10, 12 or 14 when the key length is 128, 192 or 256 bits respectively. Each round in AES, except the last round, consists of four operations : SubBytes, ShiftRows, MixColumns and AddRoundKey. The decryption flow is simply the reverse of the encryption flow, and each operation is the reverse of the corresponding one in the encryption process.

The AES tower transformation and its steps operate on intermediate results, called state, which can be visualized as a rectangular matrix with four rows. The number of columns in this matrix is noted Nb and is equal to the length of the block in bits divided by 32. For a data block of 128 bits (16 bytes), the value of Nb is 4, the state is thus treated as a 4 × 4 matrix. treated as a 4 × 4 matrix and each element of the matrix represents a byte.

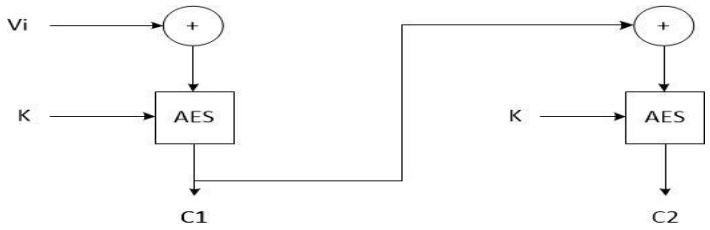
2. Benefits of AES encryption

Here are some key advantages of choosing AES over other encryption standards :

- All three types of keys are long enough, which is the strength of AES
- No cryptographic attack has been proven against AES so far ;
- Does not take up as much memory as other types of encryption (e.g. DES) ;
- Easy to combine with other security protocols and encryption types.

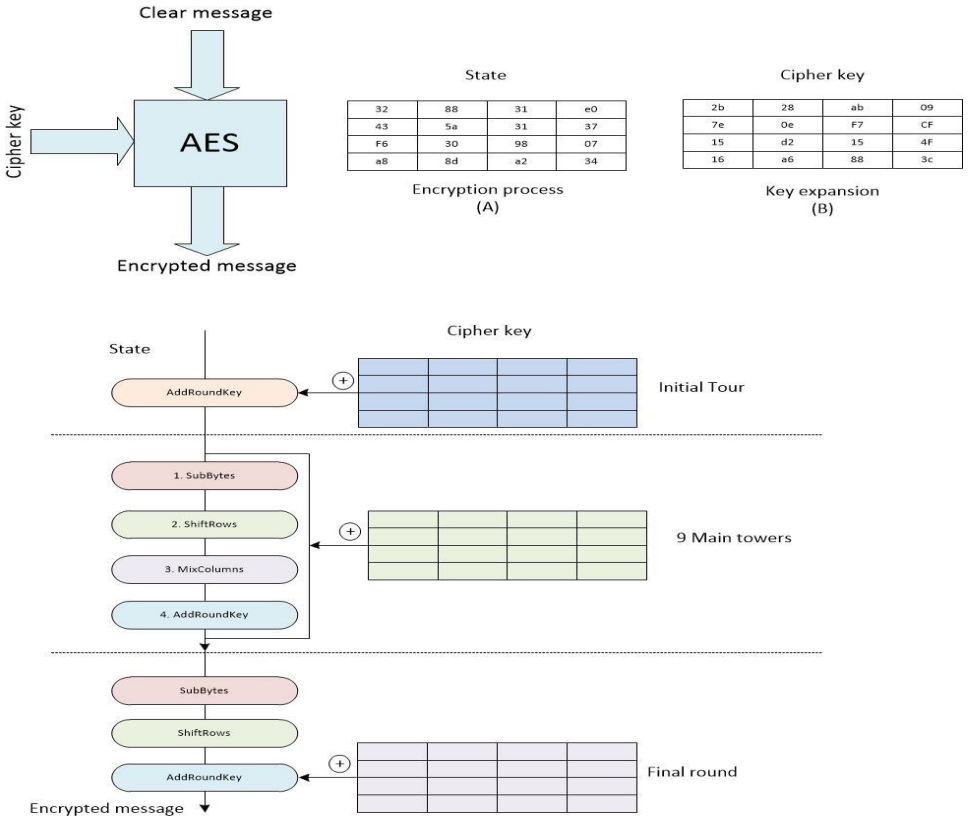
3. Block cipher mode

AES is a block cipher, that is to say the basic message will be divided into different blocks and the blocks will be combined in a certain way to produce the final message. There are several modes of block cipher of which we have : CGM, ECB, CTR, OFB and CBC. CBC for Cipher Block Chaining : the previous block is used to encrypt the next block for example to encrypt M2, the C1 encryption will be combined with the M2 block encryption which is C2. Since the first block has no precedent, we use an initiation vector (Vi) which will be chosen beforehand.



4. How AES works

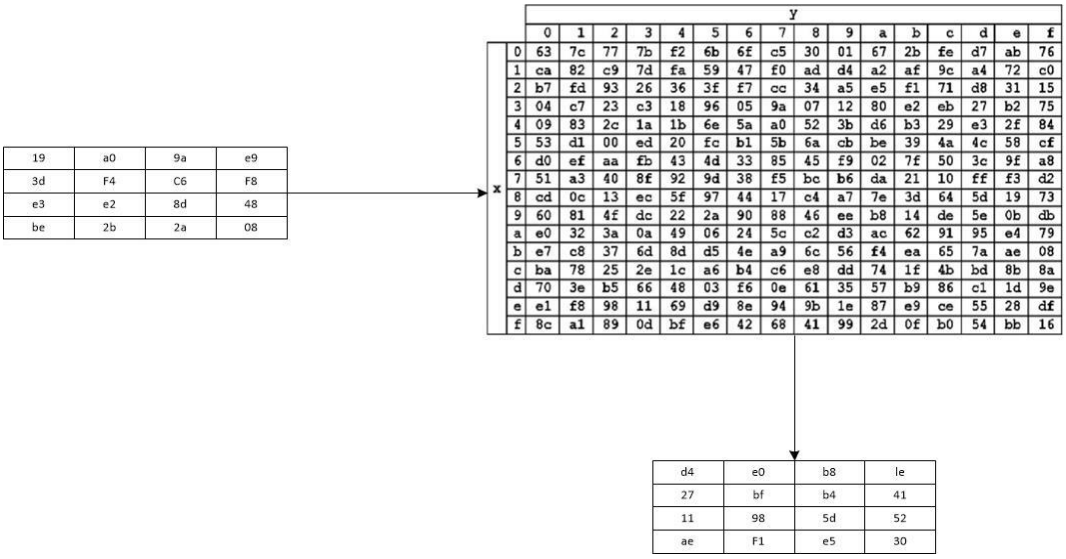
Illustrated in the figure below, AES is a block cipher algorithm, which consists of dividing the message into several blocks of a certain size, encrypting it separately and combining these blocks to form a cipher text.



To do data encryption, the AES algorithm is based on an operation consisting of 4 muni operations.

The four types of operations of the AES algorithm are :

- SubBytes : When the message enters the transformation loop, the AES protocol splits the message into blocks (16-bit blocks), each bit will be replaced by a substitution bit from the substitution matrix called S-Box (Standard Matrix).

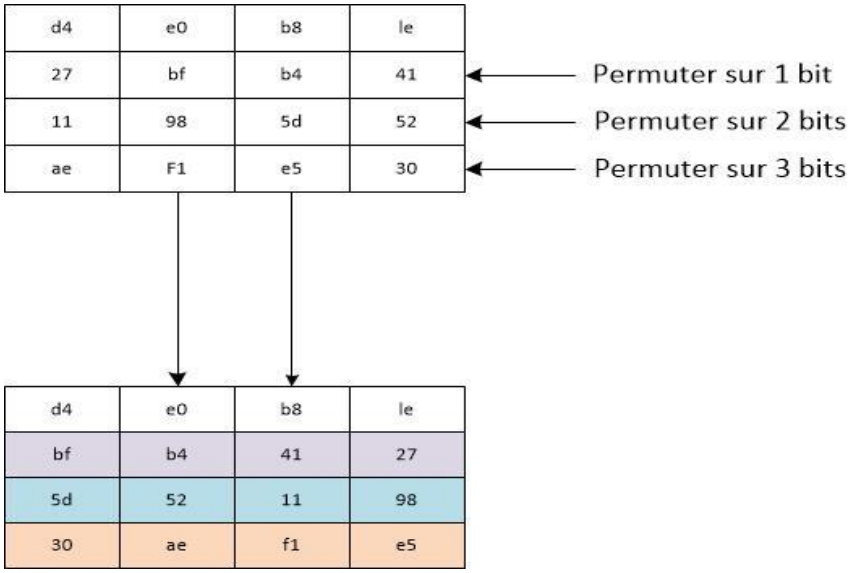


19	a0	9a	e9
3d	F4	C6	F8
e3	e2	8d	48
be	2b	2a	08

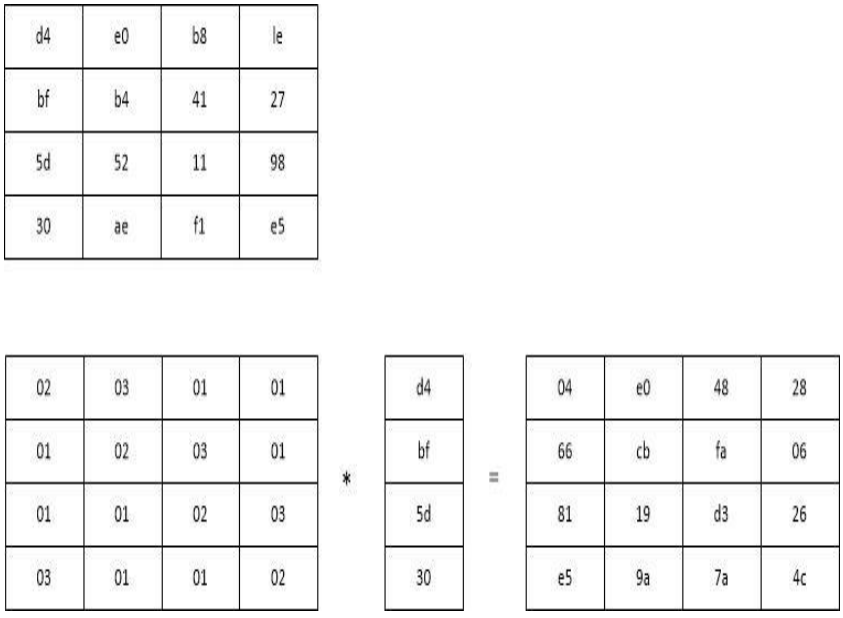
x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	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

d4	e0	b8	1e
27	bf	b4	41
11	98	5d	52
ae	F1	e5	30

- ShiftRows : Performs a circular permutation of the bytes in each cell of the table, except the first row which does not undergo any transformation.



- MixColumns: Each column of the matrix will be multiplied by a standard matrix, already known in advance. An XOR is applied between each of the bytes.

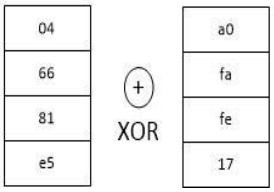


- AddRoundKey : This operation is done column by column. Each bit of the matrix will be associated to a bit of the key matrix to obtain a final matrix using the exclusive or (XOR).

04	e0	48	28
66	cb	fa	06
81	19	d3	26
e5	9a	7a	4c

a0	88	23	2a
fa	54	a3	6c
fe	2c	39	76
17	b1	39	05

Generated key



AES key expansion is used to produce a defined number of key turns from the initial key. In AES, the initial key is used in the initial set of AES as the input to the AddRoundKey operation. We perform the calculation a dozen times, and we get our text simply encrypted. As many rounds as we have in the AES protocol, equals as many keys, 10 for 128 bits.

5. AES algorithm implementation

To allow a good encryption and decryption of the data, a sequence of steps has been has been programmed.

5.1. Encryption

Here are the main steps of the cryptographic algorithm used for the encryption. It will be executed at the Li-Fi transmitter level.

Algorithm 1 : Encryption

```
Begin
    Calcul size of the text
    Add padding bit
    State = plainText
    AES-CBC encryption
    { KeyExpansion
    AddRoundKey (State, ExpandedKey[0])
    for r ← 1 to (Nr - 1)
            { SubBytes (State, S-box)
            ShiftRows (State)
            MixColumns (State)
            AddRoundKey (State, ExpandedKey[r])}
    end for
        SubBytes (State, S-box)
        ShiftRows (State)
        AddRoundKey (State, ExpandedKey[Nr])
        XOR_block (iv, State)}
```

```
        Out = CipherText
    End
```

5.2. Decryption

Here are the main steps of the cryptographic algorithm used for decryption. It will be executed at the Li-Fi receiver.

Algorithm 2 : Decryption

```
    Begin
        Calcul size of the ciphertext
        State = CipherText
        AES-CBC decryption
        { XOR_block (plain, iv)
        KeyExpansion
        AddRoundKey (State, ExpandedKey[0])
        for r ← (Nr - 1) to 1
            { InverseShiftRows (State)
            InverseSubBytes (State, S-box)
            AddRoundKey (State, ExpandedKey[r])
            InverseMixColumns (State) }
        end for
            InverseSubBytes (State, S-box)
            InverseShiftRows (State)
            AddRoundKey (State, ExpandedKey[Nr])}
            Delete padding bits
        out = PlainText
    End
```

Even with a multitude of super-powered computers, cracking a 256-bit AES key would take much longer.