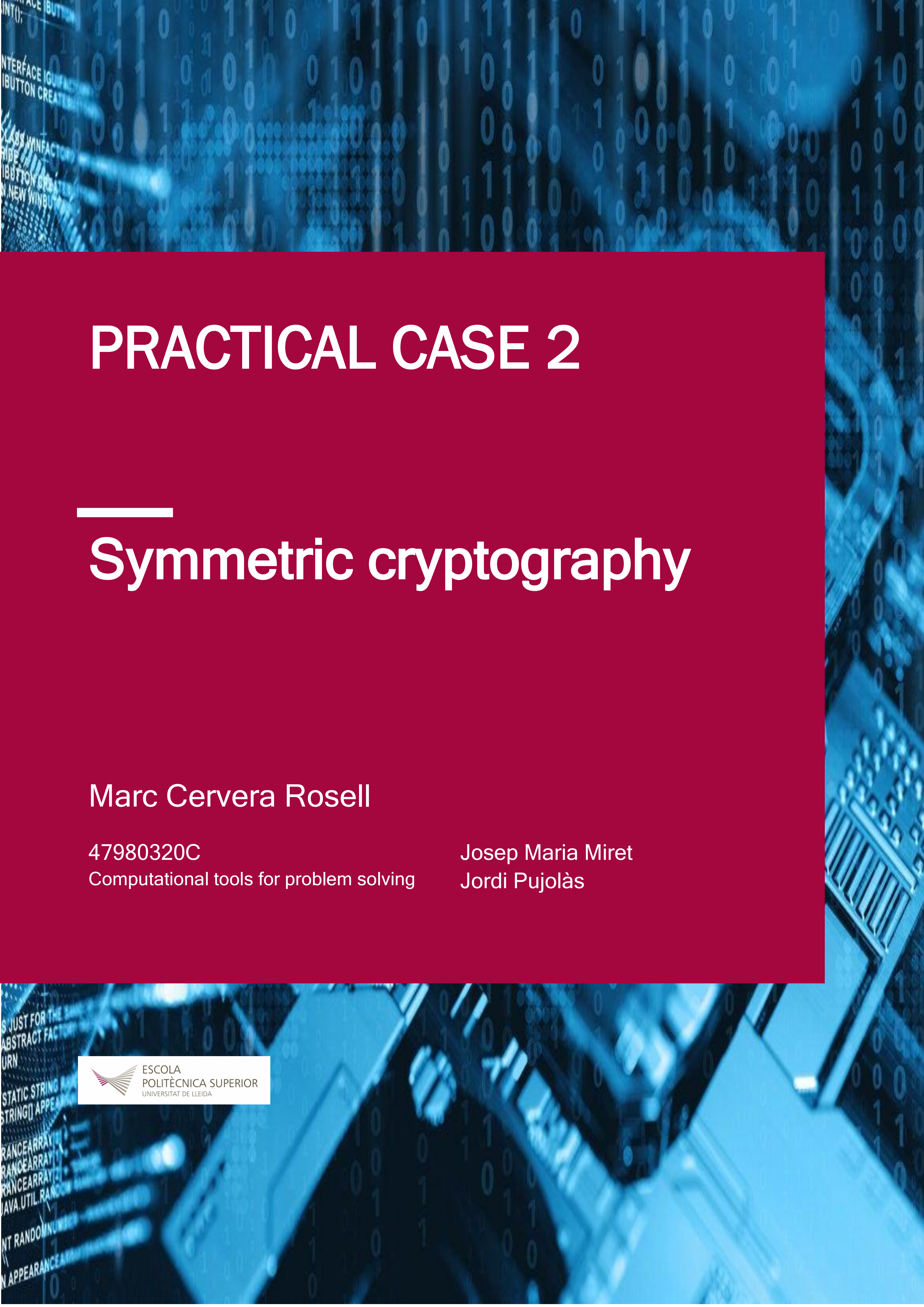


PRACTICAL CASE 2

Symmetric cryptography

Marc Cervera Rosell

47980320C
Computational tools for problem solving

Josep Maria Miret
Jordi Pujolàs

ESCOLA
POLITÈCNICA SUPERIOR
UNIVERSITAT DE LLEIDA

Index

Introduction

This is the second practical case of three.

This practical case is about the S-Box in AES. The Advanced Encryption Standard is composed of several rounds where the bits of the key are XORed with those of the plaintext block, and the resulting bits are mixed together in basically three different procedures. The S-Box in AES is one of these steps, and mathematically the S-Box is basically a multiplicative inversion in the finite field F_{2^8} of 256 elements. This means one needs a way to convert the bytes of each block into elements of F_{2^8}. The standard way to do so is to represent the byte as the coefficients of a polynomial of degree at most 7 over F_2.

This practical case has only 1 problem with 3 different sections, but instead of doing section by section, we're going to do the three sections together for every case.

Instructions

After see the method of resolution, the practical case asks for three different things, that are:

i Find the output byte of the following input keys in AES S-Box as described above: 02, cb, 9a.

ii Show the actual computation of the inversions in *i*.

iii Check your results using the AES S-Box lookup table you will find by searching "Rijndael S-Box" in the internet.

Resolutions

Case 02

The first step is to find the input in binary base as a byte ➔ $02_{16)} = 00000010_{2)}$

The second step is to find the polynomial associated to the input as a byte ➔ $00000010_{2)} = 0x^7 + 0x^6 + 0x^5 + 0x^4 + 0x^3 + 0x^2 + 1x + 1$ = X.

Now, we've to find X^{-1}.

To find the invers of the element X, we've to divide the polynomial of the modulus. In this case the modulus will be: $m(x) = x^8 + x^4 + x^3 + x + 1$. So, if we calculate the division, we find:

$$
\begin{array}{l|l}
\quad x^8 + x^4 + x^3 + x + 1 & x \\
\cline{2-2}
+x^8 & x^7+x^3+x^2+1 \\
\cline{1-1}
/ \quad x^4 + x^3 + x + 1 & \\
\quad +x^4 & \\
\cline{1-1}
\quad / \quad x^3 + x + 1 & \\
\quad\quad +x^3 & \\
\cline{1-1}
\quad\quad / \quad x + 1 & \\
\quad\quad\quad +x & \\
\cline{1-1}
\quad\quad\quad / \quad 1/ &
\end{array}
$$

Now, we've to find Bezout's identity to find the inverse of X:

$$x^8+x^4+x^3+x+1=x*(x^7+x^3+x^2+1)+1\Rightarrow 1=(x^8+x^4+x^3+x+1)+x*(x^7+x^3+x^2+1)$$

So, as we can see, the inverse of X is the polynomial of degree 7 ➔ $(x^7+x^3+x^2+1)$

The polynomial of degree 8 is going to be equal to zero because is the modulus.

Finally, we've to compute the matrixial operations specified in the PDF document and convert the result to hexadecimal.

$$\begin{pmatrix} 1&0&0&0&1&1&1&1\\ 1&1&0&0&0&1&1&1\\ 1&1&1&0&0&0&1&1\\ 1&1&1&1&0&0&0&1\\ 1&1&1&1&1&0&0&0\\ 0&1&1&1&1&1&0&0\\ 0&0&1&1&1&1&1&0\\ 0&0&0&1&1&1&1&1 \end{pmatrix} \cdot \begin{pmatrix}1\\0\\1\\1\\0\\0\\0\\1\end{pmatrix} + \begin{pmatrix}1\\1\\0\\0\\0\\1\\1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\\1\\0\\0\\0\end{pmatrix} + \begin{pmatrix}1\\1\\0\\0\\0\\1\\1\\0\end{pmatrix} = \begin{pmatrix}1\\1\\1\\0\\1\\1\\1\\0\end{pmatrix}$$

As we see in the result, the output byte is 01110111 (taken inversely). So, if we convert the bits taken 4 by 4, we obtain $01110111_{\,2)} = 77_{16)}$

So, the final result after inputting $02_{16)}$, we obtain as the output $01110111_{\,2)} = 77_{16)}$.

Case cb

As we've done in the last case, the first step is to convert the input into a byte of binary digits ➔ $cb_{16)} = 11001011_{2)}$.

So, once we've the input as a byte of binary digits, the associated polynomial is ➔ $x^7 + x^6 + x^3 + x + 1$.

Now, we've to search the inverse of this polynomial in F_{2^8}. It's important to remember that $F_{2^8} = \frac{F_2[x]}{x^8+x^4+x^3+x+1}$.

Then, the next step is to compute the division. In this case, we will see that with one only division is not enough. We're going to need 2 divisions.

$$\begin{array}{rl|l} & x^8+0x^7+0x^6+0x^5+x^4+x^3+0x^2+x+1 & x^7+x^6+x^3+x+1 \\ \hline + & x^8+x^7+0x^6+0x^5+x^4+0x^3+x^2+x+0 & x+1 \\ \hline / & x^7+0x^6+0x^5+0x^4+x^3+x^2+0x+1 & \\ + & x^7+x^6+0x^5+0x^4+x^3+0x^2+x+1 & \\ \hline / & x^6+0x^5+0x^4+0x^3+x^2+x+0\,/ & \end{array}$$

As we don't have as residue 1, we've to divide another time. In this occasion, we've to divide the polynomial of degree 7 between the residue.

$$
\begin{array}{rl}
x^7+x^6+0x^5+0x^4+x^3+0x^2+x+1 & \underline{\lfloor x^6+x^2+x} \\
\underline{+\,x^7+0x^6+0x^5+0x^4+x^3+x^2+0x+0} & x+1 \\
/\quad x^6+0x^5+0x^4+0x^3+x^2+x+1 & \\
\underline{+x^6+0x^5+0x^4+0x^3+x^2+x+0} & \\
/\quad 0x^5+0x^4+0x^3+0x^2+0x+1\,/ &
\end{array}
$$

Once we’ve as residue 1, we’ve to find the Bezout’s identity.

$$1=(x^7+x^6+x^3+x+1)+(x+1)*(x^6+x^2+x)\Rightarrow$$

$$\Rightarrow 1=(x^7+x^6+x^3+x+1)+(x+1)*[(x^8+x^4+x^3+x+1)+$$

$$(x+1)*(x^7+x^6+x^3+x+1)]\Rightarrow 1=(x+1)*(x^8+x^4+x^3+x+1)+$$

$$[(x+1)^2+1]*(x^7+x^6+x^3+x+1)$$

The polynomial of degree 8 is going to be equal to zero because is the modulus, so the inverse of the polynomial is $(x+1)^2+1=\ x^2 \ => \ 00000100_{2)}$.

The final step is to calculate the matrixial operations.

$$
\begin{pmatrix}
1&0&0&0&1&1&1&1\\
1&1&0&0&0&1&1&1\\
1&1&1&0&0&0&1&1\\
1&1&1&1&0&0&0&1\\
1&1&1&1&1&0&0&0\\
0&1&1&1&1&1&0&0\\
0&0&1&1&1&1&1&0\\
0&0&0&1&1&1&1&1
\end{pmatrix}
\cdot
\begin{pmatrix}0\\0\\1\\0\\0\\0\\0\\0\end{pmatrix}
+
\begin{pmatrix}1\\1\\0\\0\\0\\1\\1\\0\end{pmatrix}
=
\begin{pmatrix}0\\0\\1\\1\\1\\1\\1\\0\end{pmatrix}
+
\begin{pmatrix}0\\0\\1\\0\\0\\0\\0\\0\end{pmatrix}
=
\begin{pmatrix}1\\1\\1\\1\\1\\0\\0\\0\end{pmatrix}
$$

The result vector is ➔ $00011111_{2)}$ and if we make the conversion to hexadecimal we obtain 1F. So, the final result after inputting $cb_{16)}$, we obtain as the output $00011111_{2)}=1F_{16)}$.

Case 9a

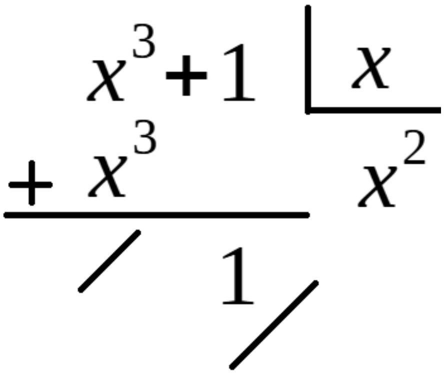
As we've in the two first examples, the first step is to convert the input, expressed in hexadecimal, into a byte of binary digits. So, $9a_{16)} = 10011010_{2)}$, and the associated polynomial is: $x^7 + x^4 + x^3 + x$

The next step is to find, again, the inverse of this polynomial.

$$
\begin{array}{r|l}
x^8+0x^7+0x^6+0x^5+x^4+x^3+0x^2+x+1 & \underline{x^7+x^4+x^3+x} \\
\underline{+x^8+0x^7+0x^6+x^5+x^4+0x^3+x^2+0x+0} & x \\
/ \qquad x^5+0x^4+x^3+x^2+x+1 \, / &
\end{array}
$$

$$
\begin{array}{r|l}
x^7+0x^6+0x^5+x^4+x^3+0x^2+x+0 & \underline{x^5+x^3+x^2+x+1} \\
\underline{+x^7+0x^6+x^5+x^4+x^3+x^2+0x+0} & x^2+1 \\
/ \qquad x^5+0x^4+0x^3+x^2+x+0 & \\
\underline{+x^5+0x^4+x^3+x^2+x+1} & \\
/ \qquad x^3+0x^2+0x+1 \, / &
\end{array}
$$

$$
\begin{array}{r|l}
x^5+x^3+x^2+x+1 & \underline{x^3+1} \\
\underline{+x^5 \qquad x^2 \qquad\quad} & x^2+1 \\
/ \quad x^3 \quad / \quad +x+1 & \\
\underline{+x^3 \qquad\quad +1} & \\
/ \qquad x \quad / \; / &
\end{array}
$$



As in the last two examples, now we've to find the Bezout's identity.

$$1=(x^3+1)+x^2*x\Rightarrow 1=(x^3+1)+x^2*[(x^5+x^3+x^2+x+1)+(x^2+1)*(x^3+1)]$$

$$1=(x^2*(x^2+1)+1)*(x^3+1)+x^2*(x^5+x^3+x^2+x+1)\Rightarrow$$

$$\Rightarrow 1=(x^4+x^2+1)*(x^7+x^4+x^3+x+(x^5+x^3+x^2+x+1)*(x^2+1))+x^2*(x^5+x^3+x^2+x+1)\Rightarrow$$

$$\Rightarrow 1=(x^4+x^2+1)*(x^7+x^4+x^3+x)+((x^4+x^2+1)*(x^2+1)+x^2\boxtimes(x^5+x^3+x^2+x+1))\Rightarrow$$

$$\Rightarrow 1=(x^4+x^2+1)*(x^7+x^4+x^3+x)+(x^6+x^4+x^4+x^2+x^2+1+x^2)*(x^5+x^3+x^2+x+1)\Rightarrow$$

$$\Rightarrow 1=(x^4+x^2+1)*(x^7+x^4+x^3+x)+(x^6+x^2+1)*(x^5+x^3+x^2+x+1)\Rightarrow$$

$$\Rightarrow 1=(x^4+x^2+1)*(x^7+x^4+x^3+x)+(x^6+x^2+1)*((x^8+x^4+x^3+x+1)+x*(x^7+x^4+x^3+x))\Rightarrow$$

$$\Rightarrow 1=(x^4+x^2+1+x*(x^6+x^2+1))*(x^7+x^4+x^3+x)+(x^6+x^2+1)*(x^8+x^4+^3+x+1x)\Rightarrow$$

$$\Rightarrow 1=(x^7+x^4+x^3+x^2+x+1)*(x^7+x^4+x^3+x)$$

As we can see in the previous calculations, the inverse of the polynomial is $x^7+x^4+x^3+x^2+x+1 => \ 10011111_{2)}$.

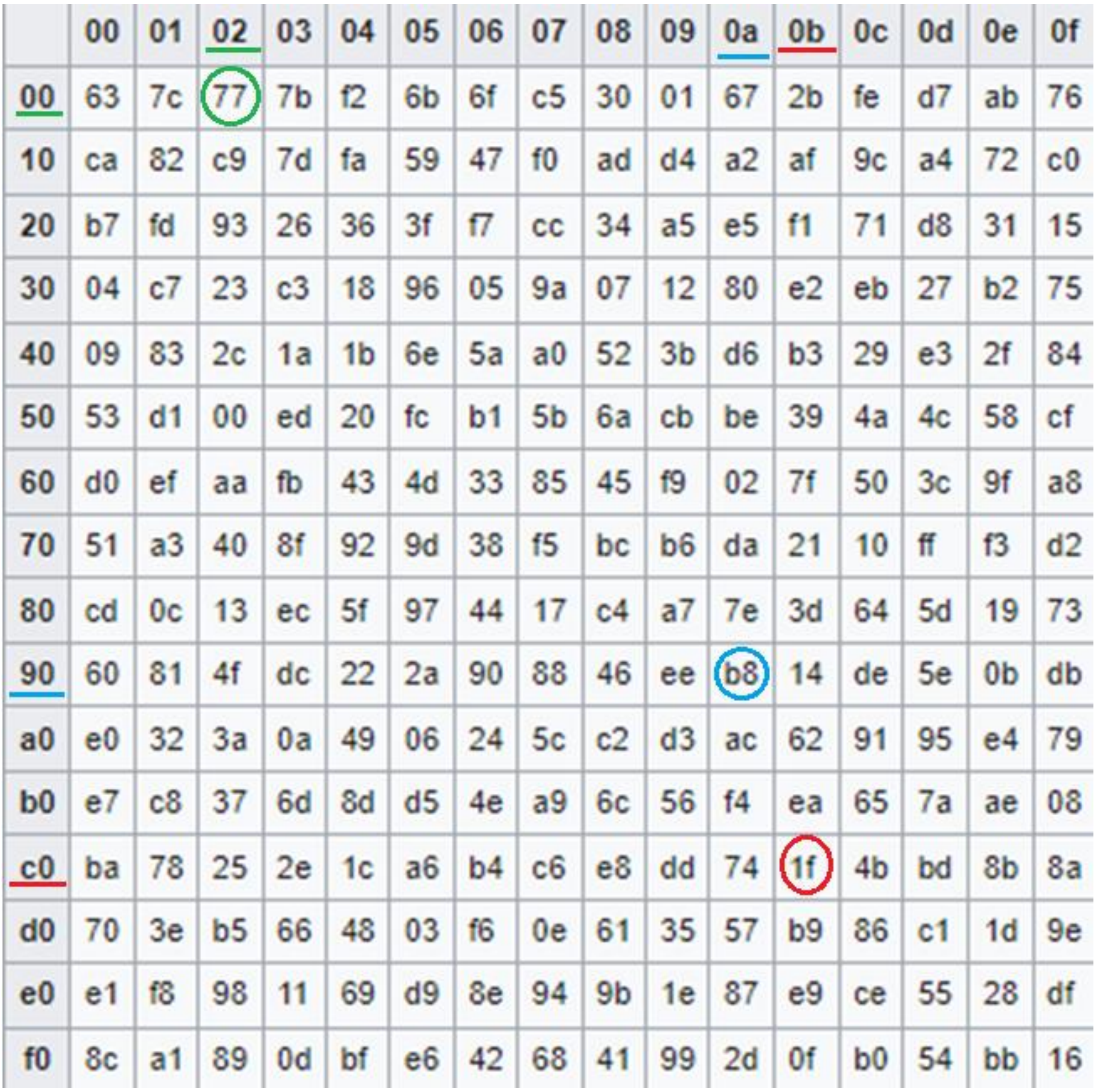
And the last step is to compute the matrixial calculations, as in the following cases.

$$\begin{pmatrix} 1&0&0&0&1&1&1&1\\ 1&1&0&0&0&1&1&1\\ 1&1&1&0&0&0&1&1\\ 1&1&1&1&0&0&0&1\\ 1&1&1&1&1&0&0&0\\ 0&1&1&1&1&1&0&0\\ 0&0&1&1&1&1&1&0\\ 0&0&0&1&1&1&1&1 \end{pmatrix}\cdot\begin{pmatrix}1\\1\\1\\1\\1\\0\\0\\1\end{pmatrix}+\begin{pmatrix}1\\1\\0\\0\\0\\1\\1\\0\end{pmatrix}=\begin{pmatrix}1\\1\\0\\1\\1\\0\\1\\1\end{pmatrix}+\begin{pmatrix}1\\1\\0\\0\\0\\1\\1\\0\end{pmatrix}=\begin{pmatrix}0\\0\\0\\1\\1\\1\\0\\1\end{pmatrix}$$

And finally, now yes, we've to transform the result into a hexadecimal number ➔$10111000_{2)} = B8_{16)}$

Table check

If we take a look on the different results of the practical case, as we can see in the following table, the results are totally valid.



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