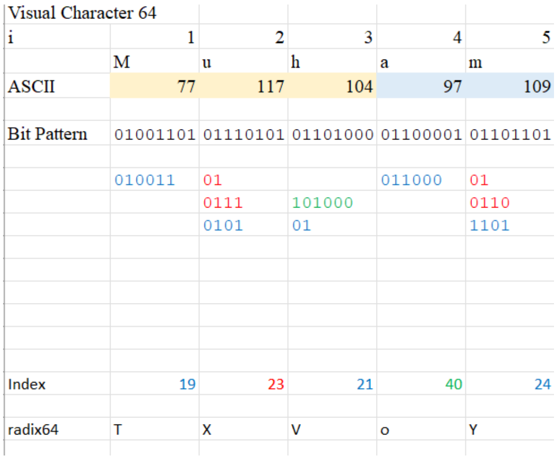
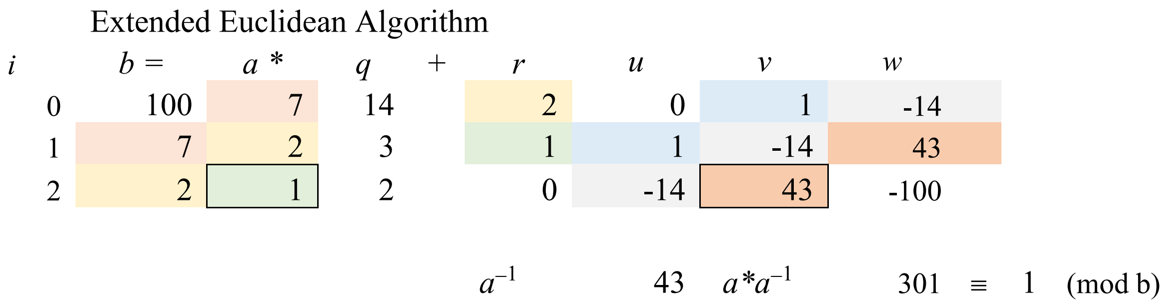
Radix64

- Base64



Visual Character 64					
i	1	2	3	4	5
	M	u	h	a	m
ASCII	77	117	104	97	109
Bit Pattern	01001101	01110101	01101000	01100001	01101101
	010011	01		011000	01
		0111	101000		0110
		0101	01		1101
Index	19	23	21	40	24
radix64	T	X	V	o	Y

Extended Euclidean Algorithm (EEA)



Extended Euclidean Algorithm

i	$b =$	a *	q	+	r	u	v	w
0	100	7	14		2	0	1	-14
1	7	2	3		1	1	-14	43
2	2	1	2		0	-14	43	-100

a^{-1} 43 $a*a^{-1}$ 301 ≡ 1 (mod b)

Irreducible Polynomials

Let an irreducible polynomial $m = 283_{10} = 256+16+8+2+1 = 100011011_2 = 11B_{16}$
In polynomial term, this irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$.

Euclidean Algorithm				Extended		
$b =$	$a \cdot$	$q +$	r	u	v	$w{=}u{-}v{\cdot}q$
283	42	6	31	0	1	-6
42	31	1	11	1	-6	7
31	11	2	9	-6	7	-20
11	9	1	2	7	-20	27
9	2	4	1	-20	27	-128
2	1	2	0	27	-128	283

a^{-1} mod b = –128 +283 = 155.
We always check $a \cdot a^{-1} \equiv 1$ (mod b)

$$42{\cdot}155 = 6510 = 23{\cdot}283 + 1 \equiv 1 \pmod{283}$$

AES S-Box

$a^{-1} = D9_{16} = 11011001_2$ (Inversekan urutan)

$b(x) = x^8 + x^4 + x^3 + x + 1 = 100011011_2 = 11B_{16}$

$$\begin{bmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

xor-kan nombor yang highlighted

$= 00111101 = 3D_{16}$