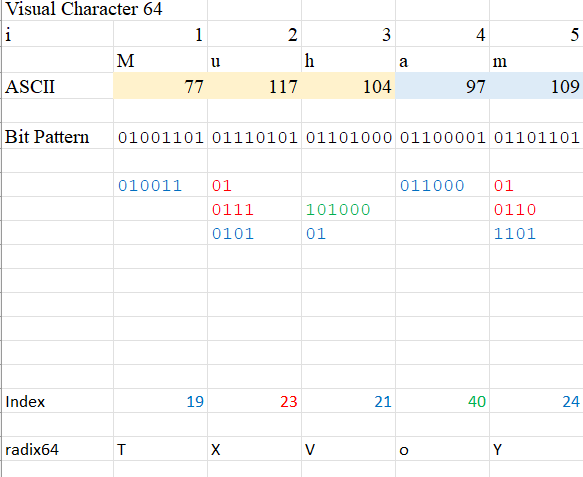
# Radix64

* Base64



# 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 | º | 1 | (mod b) |

# Irreducible Polynomials

Let an irreducible polynomial *m* = 28310 = 256+16+8+2+1=1000110112 = 11B16

In polynomial term, this irreducible polynomial *m*(*x*) = *x*8+ *x*4+ *x*3+ *x* +1.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Euclidean Algorithm | | |  | Extended |  |  |
| *b* = | *a* ⋅ | *q* + | *r* | *u* | *v* | *w*=*u*−*v⋅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* ⋅ *a*-1 ≡ 1 (mod b)

42⋅155 = 6510 = 23⋅283 +1 ≡ 1 (mod 283)

# AES S-Box

*a*-1 = D916 = 110110012 (Inversekan urutan)

*b*(*x*) = *x* 8+ *x*4+ *x*3+*x*+1 = 1000110112 = 11B16

xor-kan nombor yang highlighted

= 00111101 = 3D16