

Key is of 3 bits

Possible keys in the key space = {000, 001, 010, 011, 100, 101, 110, 111} = $2^3 = 8$ keys

c -> 000 -> m (correct)

..... 001 ...

... 111 ... m

Advanced Encryption Standard (AES) -> 128 bits key -> 2^{128} operations -> 100 years

Z_p = finite field of prime order $p = \{0, 1, 2, \dots, p-1\}$, under two operations: a) addition modulo p and b) multiplication modulo p

Galois field (GF): $GF(p) = \langle Z_p, +_p, \cdot_p \rangle$

$GF(p)$ -> extended field $GF(p^n)$ [$p = 2$, $GF(2)$ -> $GF(2^n)$, $Z_2 = \{0, 1\}$]

Elements in $GF(2^n)$ > ~~polynomial of degree n-1~~: $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_{n-1} x^{n-1}$, a_i are from Z_2 .

Cardano's Method