



Task 5. «The number of solutions»

Let \mathbb{F}_{256} be the finite field of characteristic 2 with 256 elements. Consider the function

$$F : \mathbb{F}_{256} \rightarrow \mathbb{F}_{256} \text{ such that } F(x) = x^{254}.$$

Since $x^{255} = 1$ for all nonzero $x \in \mathbb{F}_{256}$, we have $F(x) = x^{-1}$ for all nonzero elements of \mathbb{F}_{256} . Further, we have $F(0) = 0$.

Alice is going to use the function F as an S-box (that maps 8 bits to 8 bits) in a new block cipher. But before she wants to find answers to the following questions.

- How many solutions may the equation

$$F(x + a) = F(x) + b \tag{1}$$

have for all different pairs of nonzero parameters a and b , where $a, b \in \mathbb{F}_{256}$?

- How many solutions does the equation (1) have for the function $F(x) = x^{2^n-2}$ over the finite field \mathbb{F}_{2^n} for an arbitrary n ?

Please, help to Alice!