

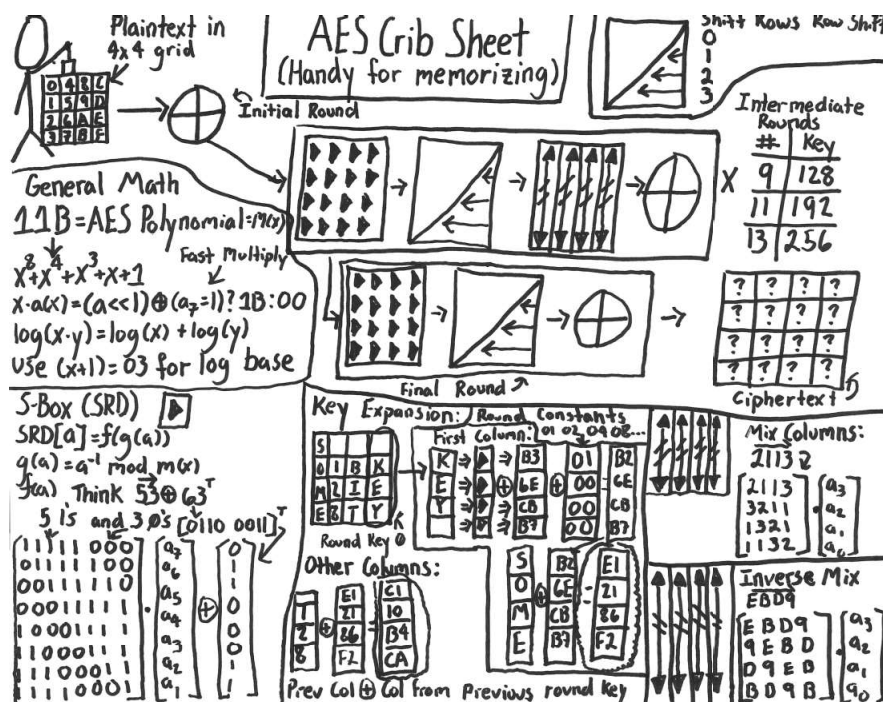


## Problem 2. «Zerosum at AES»

Let  $AES_0$  be a mapping that represents the algorithm AES-256 with the all-zero key. Let  $X_1, \dots, X_{128} \in \mathbb{F}_2^{128}$  be pairwise different vectors such that

$$\bigoplus_{i=1}^{128} X_i = \bigoplus_{i=1}^{128} AES_0(X_i).$$

1. Propose an effective algorithm to find an example of such vectors  $X_1, \dots, X_{128}$ .
2. Provide an example of  $X_1, \dots, X_{128}$ .



The picture is from the [page](#) of Jeff Moser.