

Definition 1 *The set C of codewords of the Reed-Solomon code is defined as:
 $C = \{(p(a_1), p(a_2), \dots, p(a_n)) | p \text{ is a polynomial over field } F \text{ of degree } < k\}$.*