**CHAPTER ONE**

**ELEMENTS OF SECURED CODES**

**IV. SECURED CODES AND INFORMATION SIZE**

In order to detect or correct error, we remove some vectors from the natural code. That is, the natural binary code divided into two sets;

* Set of usable vectors (
* Set of forbidden vectors (.

In communication channels, it looks like additional lines were added on a binary natural code of length, K.

For example;

The bits of the lines that are added can be on a fixed place. The code is then set to be systematic. That is, all the added bits are grouped in the same place. In general, it’s not possible to know the number of bits to be added on a natural code to have a systematic code having the desired properties. In general, you have to solve the equation; **n-K= f(K,dmin).**

The best way to approach f is to use the **hamming criteria;**

OR

**Hilbert criteria**

Most of the time, we use specialize tables where having K and dmin, the table recommends **n(K,dmin n)**

**CHAPTER TWO.**

**LINEAR CODES.**

1. **INTRODUCTION.**

The design concept of computer hardware uses group theory which is characterized by decoding functions that are simple to define and implement. Linear codes are based on some aspect of group theory.

1. **GROUP CONCEPT.**

A group is a set of elements in which we define a binary operator that verifies four actions

* Internal rule.

On two different elements, when we apply binary operator, we have an element of the set

* Associativity

The binary operator is associative. That is, for example;

(a b XOR c)=a XOR b XOR c)

* Neutral element€

For example;

A XOR e=a (x=1, +=0)

* Inverse element

Apart from the ne=neutral element, all other elements must be inverse. That is, a XOR b=e where b is the inverse of a

* Addictive element

A group is said to be addictive if the binary operation is addition (+).

A group is said to be abelian if (a+b=b+a) then the operator is communicative

When the number of elements of a group is finite, we say the group is a finite group. In linear code, we use abelian, addictive finite group and the operation is + modulus 2 (+)