EQUIVALENCE CLASSES OF LINEAR MAPPINGS WITH APPLICATIONS TO ALGEBRAIC CRYPTOGRAPHY, I

BY J. V. BRAWLEY AND JACK LEVINE

1. Introduction. The application of algebraic methods in constructing cryptographic systems of a highly effective nature was demonstrated by Hill in [1] and [2]. Later, Levine [4], [5] and [6] and Levine and Brawley [7] and [8] continued with these applications as applied to the cryptanalysis of various special problems based on Hill's matrix multiplication encipherment method. We refer to this method as *linear cryptography* (see §2) and use the term *algebraic cryptography* to refer to any method of secret message writing which utilizes an algebraic system such as a group, ring, or field to encipher a message (called a *plain-text*). The enciphered form of the message is called a *cipher-text* or *cryptogram.*

The general method in an algebraic cryptographic system is to first establish a correspondence between the letters of the alphabet being used and some algebraic system. The operations of that system are then used to convert a plain-text to a cryptogram. This process must be reversible so that the plain-text can be recovered uniquely.

From the point of view of the cryptanalyst, both the letters of the alphabet and the algebraic system may be known and yet a correspondence between the two (the so-called *cipher-alphabet*) may be either known or unknown. The basis of several papers by the present authors [5], [6], [7] and [8] was, in fact, precisely the assumption that the cipher-alphabet was known.

This paper is presented in two parts. One of its objects is to determine if a linear cryptographic system using an unknown cipher-alphabet can always be replaced by an equivalent system using a known cipher-alphabet (in the sense defined in §2). An affirmative answer would, of course, be of great importance to the cryptanalyst. However in Part II it is shown that for linear systems over a finite field the answer is in general "no". Various other related questions will also be considered. These are formulated in §2 which also contains a precise description of the cryptographic system in which we shall be interested. In §3 these questions are converted into a purely algebraic form and in §§4, 5 and in Part II solutions are given when the cryptographic system is based on a finite field. Part II also contains solutions to certain probability questions and a section devoted to a study of certain groups related to the questions of §2.

Although the basic cryptographic system of this paper utilizes a finite ring with identity and the questions posed concern such a system, our results are obtained by restricting the ring to be a field. In a later paper it is planned to consider more general rings and other algebraic systems.

Received October 5, 1971.