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

BY J. V. BRAWLEY AND JACK LEVINE

This paper is the second part of a two part paper. Part I contained §§1–5 while the present part contains §§6–8. For the relevant notation and terminology we refer the reader to Part I [1].

In Part I we posed a number of questions but essentially solved only the problem of determining for a given $(\alpha, A) \in \mathcal{A} \times GL(n, K)$ those $(\beta, B) \in \mathcal{A} \times GL(n, K)$ equivalent to it [1; §2, Q2.1]. In this part we answer the remaining questions of [1; §2]. In particular we determine (Theorem 6.1) the number of equivalence classes or essentially different linear n-graphic systems which answers Q2.2. We also give in §6 the answers to Q2.3, Q2.4 and Q2.5. In §7 we compute the expected number of alphabets β which must be tried in order to decipher an unknown cryptosystem (α, A) using methods based on a known cipher alphabet (see [4], [5], [6] and [7]). We also give in §7 some related numerical results based on a 25 letter alphabet, $GF(25)$, and $n = 2$. In §8 we consider some group theoretic questions arising in our study.

6. Enumeration of the equivalence classes and cryptographic interpretations. In this section we answer questions Q2.2, Q2.3, Q2.4 and Q2.5 for the case $R = K = GF(p^m)$. We shall find it convenient to partition $\mathcal{A} \times GL(n, K)$ into the four mutually exclusive classes indicated in Theorem 5.3 [1; §5], namely,

$$\bar{C}_1 = \{(\alpha, A) \mid A \text{ is T.1 and not r.s.}\},$$

$$C_1 = \{(\alpha, A) \mid A \text{ is T.1 and r.s.}\},$$

$$\bar{C}_2 = \{(\alpha, A) \mid A \text{ is T.2 and not r.s.}\},$$

$$C_2 = \{(\alpha, A) \mid A \text{ is T.2 and r.s.}\}.$$

(Note that $(\alpha, A) \in C_2$ iff A is a permutation matrix.)

In order to answer Q2.2 we need formulas for the following numbers.

(i) $\bar{\rho}_1(n, t)$ = number of T.1, not r.s. matrices A in $GL(n, K)$ such that the set of elements of A generates the subfield $GF(p^t)$ of K.

(ii) $\rho_1(n, t)$ = number of T.1, r.s. matrices A in $GL(n, K)$ such that the set of elements of A generates the subfield $GF(p^t)$ of K.

(iii) $\bar{\rho}_2(n, r)$ = number of T.2, not r.s. matrices A in $GL(n, K)$ such that the set of nonzero elements of A generates the order r subgroup H_r of K^*.

(iv) $\rho_2(n, r)$ = number of T.2, r.s. matrices A in $GL(n, K)$ such that the set of nonzero elements of A generates the order r subgroup H_r of K^*.

Received October 19, 1971.