SOME MATHEMATICAL ASPECTS OF CRYPTOGRAPHY[1]

By A. A. Albert

1. Introduction. The idea of connecting cryptography with mathematics is not new, but it has not been exploited in the literature of either subject to the extent of the present paper. Our topic should be a timely one not only because of the present public interest in anything connected with our war effort, but also because of the current ever increasing use by scientists[2] of the concepts of modern abstract algebra.

We shall present here a mathematical formulation of a general theory of cryptology[3] with detailed application to cryptography. In this we shall see that cryptography is more than a subject permitting mathematical formulation, for indeed it would not be an exaggeration to state that abstract cryptography is identical with abstract mathematics.

Our formulation will permit a rapid presentation of the methods of cryptography in common use, and we shall show that all of these methods are very special cases of the so-called algebraic cipher systems. These latter cipher systems are entirely practical in the simple cases, and we hope that our presentation will destroy the belief of many cryptologists that

---

[1] Our title is that of an invited address which the author gave at the Manhattan, Kansas meeting of the American Mathematical Society on November 22, 1941. The presentation here is an amplification of the material of that lecture and includes what we hope is an adequate amount of expository mathematical material.

[2] The concepts of ring, mapping, linear transformation, matrix are being used to an ever increasing extent by psychologists, economists and statisticians, as well as most physical scientists.

[3] We shall define this and other terms of this kind later.

they are "only practical providing a machine is used."[4]

2. Cryptography as a theory of non-singular mappings. The function concept has been described frequently as a unifying concept for collegiate mathematics. Elementary functions are usually given by formulas $y = f(x)$, but this sort of definition is not always possible and only makes sense in an environment in which the necessary additional assumptions are presupposed for all the functions considered. Let us then formulate the concept in complete general terms.

Consider a set $\mathcal{M}$ consisting of any objects whatever and call these objects the quantities of $\mathcal{M}$. (They might be numbers or physical objects or even mathematical concepts!) We let x be a symbol which is permitted, during our discussion, to represent any quantity of $\mathcal{M}$, so that we call x a variable whose range is $\mathcal{M}$. Let $\mathcal{N}$ be a second set of quantities and set up a correspondence

$$x \longrightarrow S(x) \tag{1}$$

(read x goes to $S(x)$) whereby every x in $\mathcal{M}$ determines a unique $S(x)$ in $\mathcal{N}$. Then the symbol $u = S(x)$ is a second variable, with $\mathcal{N}$ as its range, and we are accustomed to say that the correspondence defines u as a function of x.

Thus a function of x really consists of two sets $\mathcal{M}$ and $\mathcal{N}$ and the correspondence S given by (1) of the quantities x of $\mathcal{M}$ on their images $S(x)$ in $\mathcal{N}$. It will be better for our purposes to describe this situation by simply speaking of S rather than

---

[4]This is a quotation from Helen F. Gaines, Elementary Cryptanalysis, Boston, 1939, p. 200.

the function, and we shall call S a mapping of $\mathcal{M}$ on $\mathcal{N}$.

Suppose that there is also a mapping T given by

(2) $$u \longrightarrow T(u)$$

on $\mathcal{N}$ to $\mathcal{M}$, so that every u of $\mathcal{N}$ determines a unique T(u) in $\mathcal{M}$. Then we let T be such that if $u = S(x)$ the quantity $T(u) = x$. In this case the mapping S is called a non-singular mapping, T is called its inverse, and we indicate this by writing $T = S^{-1}$.

Cryptography is the study of all non-singular mappings S on $\mathcal{M}$ to $\mathcal{N}$ where $\mathcal{M}$ is the set of all messages x and $\mathcal{N}$ is the set of all cryptograms S(x). The mappings are called cipher systems. If a message x and a cipher system S are given, the process of the application of S to x, so as to obtain the cryptogram S(x), is called the encipherment of x. When S and S(x) are given the process of the application of S^{-1} to the cryptogram S(x), so as to obtain the message x, is called the decipherment of S(x).

There are many mathematical situations in which it is possible to determine a mapping S on $\mathcal{M}$ to $\mathcal{N}$ from a given list of a finite number of quantities x in $\mathcal{M}$ and their images S(x) in $\mathcal{N}$. However we wish to propose the more difficult problem of determining S (and hence each x) from a given finite set of cryptograms S(x). We use this in the definition of cryptanalysis as the theory of those structural properties of messages, cryptograms, and cipher systems which are required in order to solve all problems (which permit a solution) of the kind above. The solution of such a problem is called the decryptment of its cryptograms, and so cryptanalysis is the study of the methods of

decryptment. Cryptology is the subject comprising both cryptography and cryptanalysis. However we shall be concerned only with the first of these two branches here.

3. Cipher systems on components, and codes. It is clear from what we have said that the most primitive cipher system would be simply a list of all the messages to be used and an adjacent list of corresponding cryptograms. However some more sophisticated cipher systems are describable, as is the case for some mathematical functions, by formulas. These formulas will express the cryptogram $S(x)$ in terms of the result of applying the cipher system S to what we shall call components of the message x, and we shall formulate this new concept.

The term message has not been interpreted thus far but we now conceive of it as any sequence of a finite number of symbols which are either letters, periods, or commas and the like. We now partition the message into blocks of symbols called components. The message x will then become a sequence of components each consisting of a group of symbols of the message x. These occur in the component in the same order as in x. Also the order of the components themselves is fixed by the order of the symbols in x. The components may be simply the words of x, or its sentences, or simply blocks of a fixed number of letters. In the latter case the final block may not contain enough letters to satisfy the given definition. Then it will be necessary to adjoin letters, called nulls, to bring up the number of letters to the required amount.

Suppose now that a message x has been broken up into n components where n is a positive integer. Let i be any integer

from 1 to n and let the symbol x_i represent the i-th component of x. Then we may represent this situation by writing x in the following notation

$$x = [x_1, x_2, \ldots, x_n]. \tag{3}$$

We wish also to use cipher systems S which replace x by sequences

$$u = S(x) = [u_1, u_2, \ldots, u_m]. \tag{4}$$

Here the cryptogram u has been broken up into m components of some prescribed kind and neither the positive integer m nor the kind of components u_j ($j = 1, \ldots, m$) need be the same as for x.

The most primitive formula for a cipher system in terms of (3) and (4) is given by

$$S(x) = [T(x_1), T(x_2), \ldots, T(x_n)], \tag{5}$$

where T is a non-singular mapping on the set $\mathcal{M}_0$ of components (of a prescribed kind) of messages to the set $\mathcal{N}_0$ of components of cryptograms (also of prescribed kind). The code is such a cipher system. Here the components of x are its words, $\mathcal{M}_0$ is the set of all words in all the messages which will be used, $\mathcal{N}_0$ is the set of all the words in all the resulting cryptograms, T is a non-singular mapping on $\mathcal{M}_0$ to $\mathcal{N}_0$.

In describing cipher systems where more of the cipher system is to be given by the formula and less by auxiliary mapping the nature of the components u_j of the cryptogram (4) may depend both on the nature of x_i in x and also on its position in the message which we have indicated by its subscript i.

But then a formula describing the cipher system would depend upon the length n of the message x, and we are studying formulas independent of x. We may achieve our end, however, by the adjuction of new components, which are nulls, to bring up the number of components to a fixed maximum prescribed in advance. It may also be achieved in a somewhat more practical way by the use of (5) and the fact that each x_i may itself be regarded as being a message, the set of all messages to be considered is now the set $\mathcal{M}_0$ of our components, T is a cipher system. But we may prescribe a partitioning of x. If we then define components for our message so that each component x_i permits a further subdivision into subcomponents $x_{i1}, \ldots, x_{ip}$, the same for each i, the cipher system T will operate on messages all of the same number of components.

We have now seen how to limit our study to cipher systems on messages (3) for a fixed n, and we shall do this.

4. Transposition ciphers. A transposition cipher is simply a cipher system given by (3) and

$$S(x) = [x_{i_1}, x_{i_2}, \ldots, x_{i_n}], \tag{6}$$

where $i_1, \ldots, i_n$ is any permutation (i.e. rearrangement) of the integers 1, 2, ..., n. This may be accomplished most effectively in the general case by simply writing the message and the permutation and then reading off the cryptogram in the form:

$$
\begin{array}{lll}
\text{PLAIN TEXT} & & x_1,\ x_2,\ \ldots,\ x_n, \\
(7) \qquad \text{CIPHER SYSTEM} & & \left\{ \begin{matrix} 1, & 2, & \ldots, & n \\ i_1, & i_2, & \ldots, & i_n \end{matrix} \right\}, \\
\text{CRYPTOGRAM} & & x_{i_1},\ x_{i_2},\ \ldots,\ x_{i_n}.
\end{array}
$$

To decipher such a message we read up in the cipher system to obtain its inverse, and then have:

$$
\begin{array}{lll}
\text{CRYPTOGRAM} & & u_1,\ u_2,\ \ldots,\ u_n, \\
(8) \qquad \text{INVERSE CIPHER} & & \left\{ \begin{matrix} 1, & 2, & \ldots, & n \\ j_1, & j_2, & \ldots, & j_n \end{matrix} \right\}, \\
\text{MESSAGE} & & u_{j_1},\ u_{j_2},\ \ldots,\ u_{j_n}.
\end{array}
$$

For example we may write:

$$
\begin{array}{lll}
\text{PLAIN TEXT} & & \text{I N T H A T P R E C E D I N G,} \\
\text{CIPHER SYSTEM} & & \left\{ \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 7 & 11 & 5 & 1 & 8 & 13 & 14 & 9 & 15 & 2 & 6 & 10 & 12 & 4 & 3 \end{matrix} \right\}, \\
\text{CRYPTOGRAM} & & \text{P E A I R I N E G N T C D H T,} \\
\text{INVERSE SYSTEM} & & \left\{ \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 4 & 10 & 15 & 14 & 3 & 11 & 1 & 5 & 8 & 12 & 2 & 13 & 6 & 7 & 9 \end{matrix} \right\},
\end{array}
$$

which we apply to obtain the original message.

There are many devices for accomplishing transformations of this kind but none of them can do more than what we have indicated above. They may need to be studied in cryptanalysis but surely are not worth while additions to cryptography. It would seem that their only possible value in this latter subject is that they may be relatively easy to remember. However the most primitive of them are worthless, and the more

complicated ones are not as easy to remember as the following device.

Let us memorize any sentence and write it with a number below each letter from 1 to the number n of letters in the sentence. We then put numbers below those according to the alphabetical order of the letters, giving repeated letters consecutive numbers. The transposition cipher system obtained in this way may be written down rapidly and is usually much more general in its structure than those special systems in common use. For example we have

KEY:	A	N	E	F	F	O	R	T	S	H	O	U	L	D	B	E	M	A	D	E
CIPHER	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
	1	14	6	9	10	15	17	19	18	11	16	20	12	4	3	7	13	2	5	8

5. Products of cipher systems. If S is a non-singular mapping $x \longrightarrow u = S(x)$ on $\mathcal{M}$ to a set $\mathcal{N}$ and T is a non-singular mapping $u \longrightarrow T(u)$ on $\mathcal{N}$ to a set $\mathcal{L}$ the correspondence

$$x \longrightarrow V(x) = T[S(x)] \tag{9}$$

is a non-singular mapping V on $\mathcal{M}$ to $\mathcal{L}$. However, it may be more convenient to compute V(x) by first computing $u = S(x)$, and then T(u), rather than V(x) directly. We shall call V the product ST of the mappings S and T.

In cryptography it is frequently possible to think of cryptograms themselves as being messages, and thus study cipher systems which are non-singular mappings on $\mathcal{M}$ to $\mathcal{M}$. But then the product ST of a cipher system S by a cipher system T is another cipher system.

It is also possible frequently to break down a cipher system into a product of simpler ones. This is usually done in analyzing cipher systems, and much of our discussion will be concerned with a description of these simpler systems rather than the more complicated systems derivable from them by the product operation described above.

It should be observed that the operation of product of mappings is associative, that is, $(ST)U = S(TU)$ for any three mappings S, T, U. Indeed both of these mappings are the same correspondences $x \longrightarrow U\{T[S(x)]\}$. However the operation is not commutative and indeed TS may not even be defined. But even if S and T are mappings on $\mathcal{M}$ to $\mathcal{M}$, so that ST and TS are also mappings on $\mathcal{M}$ to $\mathcal{M}$, they may be different. For example, let $\mathcal{M}$ consist of the symbols 1, 2, 3; S be the correspondence $1 \longrightarrow 2$, $2 \longrightarrow 3$, $3 \longrightarrow 1$; T be the correspondence $1 \longrightarrow 2$, $2 \longrightarrow 1$, $3 \longrightarrow 3$. Then ST is given by $1 \longrightarrow 1$, $2 \longrightarrow 3$, $3 \longrightarrow 2$, and TS by $1 \longrightarrow 3$, $2 \longrightarrow 2$, $3 \longrightarrow 1$.

6. The role of the ring in a cipher alphabet. It is frequently desirable in cryptography to use an intermediate set $\mathcal{N}$ and so construct a cipher system S as the product TUT^{-1}, where T is a non-singular mapping on the set $\mathcal{M}$ of all messages to the intermediate set $\mathcal{N}$, U is a non-singular mapping on $\mathcal{N}$ to $\mathcal{N}$. Let us then write

$$x = [x_1, \ldots, x_n],$$

for components x_i of our messages x, and suppose that T is such that

(10) $$u = T(x) = [u_1, \ldots, u_n], \quad u_i = T_0(x_i).$$

Here T_0 is a non-singular mapping on the set $\mathcal{M}_0$ of all components of messages, to a set $\mathcal{N}_0$ whose quantities are at our choice. Then u is formed as the sequence above and we have

(11) $$T^{-1}(u) = [T_0^{-1}(u_1), \ldots, T_0^{-1}(u_n)].$$

We apply a second transformation U on $\mathcal{N}$ to $\mathcal{N}$ and have

(12) $$U(u) = [v_1, \ldots, v_n],$$

so that

(13) $$S(x) = [T_0^{-1}(v_1), \ldots, T_0^{-1}(v_n)].$$

Let us call the set $\mathcal{N}_0$, together with the mapping T_0, a <u>cipher alphabet</u>.

The cipher alphabet is introduced to simplify the description of S. In particular we may use a mathematical number system $\mathcal{A}$ for the set $\mathcal{N}_0$ and so have a set $\mathcal{N}_0$ in which addition and multiplication of its quantities are defined. It may then be a very simple matter to give formulas for the mapping U and to give T_0 explicitly. However the consequent description of S in terms of messages alone would usually be extremely complicated.

The only sets $\mathcal{A}$ which we shall use are the sets called <u>commutative rings</u>. A <u>ring</u> $\mathcal{A}$ is a set of quantities for which the sum a + b and the product ab of any a and b in $\mathcal{A}$ are quantities of $\mathcal{A}$ such that

(14) $$a + b = b + a, \quad (a + b) + c = a + (b + c), \quad a(bc) = (ab)c$$

(15) $$a(b + c) = ab + ac, \quad (b + c)a = ba + ca,$$

for every a, b, c of $\mathcal{A}$. Moreover we assume that for every a and b of $\mathcal{A}$ there is a unique solution x in $\mathcal{A}$ of the equation

$$a + x = b. \tag{16}$$

We call $\mathcal{A}$ a commutative ring if it is also true that

$$ab = ba \tag{17}$$

for every a and b of $\mathcal{A}$.

In every ring there is a unique zero quantity 0 such that

$$a + 0 = a, \tag{18}$$

for every a of $\mathcal{A}$, and a unique quantity -a, called the negative of a, such that

$$a + (-a) = 0. \tag{19}$$

Then in (15) we have $x = b + (-a)$. It can be shown that the properties we have assumed imply that $-(-a) = a$, $(-a)b = a(-b) = -(ab)$, $(-a)(-b) = ab$ for all quantities a and b of $\mathcal{A}$.

The familiar number systems consisting of all rational numbers, of all real numbers and of all complex numbers are examples of commutative rings. These rings are all <u>fields</u>, that is, commutative rings $\mathcal{A}$ with the property that if a and b are in $\mathcal{A}$ and a is not zero there is a unique solution x in $\mathcal{A}$ of the equation

$$ax = b. \tag{20}$$

This quotient x has a property like the difference $x = b - a$ which is the solution of (15). First there is a <u>unity quantity</u> 1 in $\mathcal{A}$ such that

(21) $$1a = a1 = a,$$

for every quantity a of $\mathcal{A}$. Also every $a \neq 0$ has a unique inverse a^{-1} such that

(22) $$aa^{-1} = a^{-1}a = 1,$$

and then $x = b\,a^{-1}$.

The set of all integers, and the set of all polynomials $f(\lambda)$ in a symbol λ with rational coefficients, are both commutative rings with a unity quantity. But they are not fields.

7. Residue class rings in cipher alphabets. Let us now suppose that the components x_i of a message x in its representation (3) as a sequence are letters of the alphabet, and perhaps other similar symbols like periods or commas. Then the set $\mathcal{M}_0$ of all possible components is a finite set and we shall wish to map it on a ring $\mathcal{R}_0$ also with a finite number of quantities. Let us then proceed to define certain very simple finite rings.

The quantities of our new rings will not be ordinary integers but classes of integers. The reader is already familiar with the classification of integers into two classes, namely, the class of all even integers, and the class of all odd integers. For these classes we have the rules that even + even = even, even + odd = odd + even = odd, even × odd = odd × even = even, odd × odd = odd. Then we may represent the class of all even integers by 0, the class of all odds by 1, and we have a ring of two elements with the laws

(23) $$0+0=0=1+1,\quad 1+0=0+1=1,\quad 0\cdot 0=0\cdot 1=1\cdot 0=0,\quad 1\cdot 1=1.$$

We shall define similarly a ring

$$\mathfrak{A}_m$$

of m classes of ordinary integers, for every fixed integer $m > 1$. If a is any integer there are integers q and r such that

$$a - qm = r, \tag{24}$$

where the remainder r is one and only one of the integers

$$0, 1, 2, \ldots, m - 1. \tag{25}$$

Let us call two integers a and b congruent and write

$$a \equiv b, \tag{26}$$

if the corresponding remainders are the same. Then $a \equiv 0$ if and only if a is a multiple of m, $a \equiv b$ if and only if $a - b \equiv 0$.

Let us now put all integers into a set of residue classes each of which will be designated by $\{a\}$. Here a is any integer of the class, $\{a\} = \{b\}$ if and only if $a \equiv b$. It is clear that there are m classes and that they are precisely the classes

$$\{0\}, \{1\}, \ldots, \{m - 1\},$$

where if r has any of the values $0, 1, \ldots, m - 1$, the set $\{r\}$ consists of all integers differing from r by a multiple of m.

It is a simple matter to verify the identities

$$(a + c) - (b + d) = (a - b) + (c - d),$$
$$ac - bd = (a - b)(c - d) + [d(a - b) + b(c - d)].$$

They imply that if $a \equiv b$ and $c \equiv d$ then $a + c \equiv b + d$, $ac \equiv bd$. But if follows that $\{a + c\}$ and $\{ac\}$ are uniquely determined for

every two classes $\{a\}$, $\{c\}$ and we define

$$\{a\} + \{c\} = \{a + c\}, \quad \{a\}\{c\} = \{ac\}.$$

The set $\mathcal{A}_m$ of our m residue classes is now known to be a commutative ring.

In actual use we omit the braces and compute with integers in the normal way but always drop off multiples of m. We need not use 0, 1, ..., m - 1 as a set of remainders but may choose any other m integers providing that there is one and only one from each class. For example let us study $\mathcal{A}_{26}$.

To facilitate computations we use the table of products $q \cdot 26$, $q = 2, 3, \ldots, 25$, which is given by

52, 78, 104, 130, 156, 182, 208, 234, 260, 286, 312, 338, 364,
390, 416, 442, 468, 494, 520, 546, 572, 598, 624, 650.

To use $\mathcal{A}_{26}$ we set up a cipher alphabet as a mapping

(27)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

P	Q	R	S	T	U	V	W	X	Y	Z
16	17	18	19	20	21	22	23	24	25	26.

We may now add and multiply integers as usual providing neither sum nor product exceeds 26. Then $3 + 5 = 8$, $3 \cdot 5 = 15$. However $15 + 19 = 34 \equiv 8$, and so if we replace O and S by what we may call their sum, this sum would be H. Similarly $15 \cdot 19 = 285 \equiv 25$ by the table above, and this corresponds to Y.

8. The finite field in the construction of cipher systems. We shall construct cipher systems as in equations (10), (11), (12) (13), where the set $\mathcal{N}_0$ of components u_i will be a finite ring

and the mapping U will be defined by algebraic expressions for the components $v_1, \ldots, v_n$ of U(u) in terms of the components $u_1, \ldots, u_n$ of u. A special instance of such a cipher system is that where $\mathcal{N}_0 = \mathcal{A}_{26}$,

$$U(u) = [au_1, \ldots, au_n], \tag{28}$$

for any non-zero quantity of $\mathcal{A}_{26}$. If a is the class $\{3\}$ of $\mathcal{A}_{26}$ our cipher system replaces every letter of our message by a corresponding letter such that A, ..., Z correspond respectively to

C F I L O R U X A D G J M P S V Y B E H K N Q T W Z. (29)

If we attempted to construct the similar mapping with $a = \{2\}$ we would replace A, ..., Z respectively by

B D F H J L N P R T V X Z B D F H J L N P R T V X Z, (30)

and so the mapping would not be non-singular.

The fact that the cipher system just described is singular arises from the property that the mappings

$$x \longrightarrow ax \qquad (x \text{ in } \mathcal{A}), \tag{31}$$

defined for each $a \neq 0$ of $\mathcal{A}$, are singular for some quantities a of $\mathcal{A}_{26}$. Such a mapping is non-singular for a given $a \neq 0$ if it is true that for every b of $\mathcal{A}$ there is a solution x in $\mathcal{A}$ of the equation (20). But then the mappings (31) of $\mathcal{A}$ on $\mathcal{A}$ are all non-singular for $a \neq 0$ of $\mathcal{A}$ if and only if $\mathcal{A}$ is a field.

The finite rings $\mathcal{A}_m$ with $m = st$ for positive integers $s > 1$, $t > 1$ are not fields. This follows since $\{s\}\{t\} = \{0\}$, the existence of a solution x of $\{t\}x = \{1\}$ would imply that

$\{s\}\{t\}x = \{s\} = \{0\}x = \{0\}$. The rings $\mathcal{A}_m$ with m a prime integer are fields and two instances of such rings important for our use are

$$\mathcal{A}_{29},\ \mathcal{A}_{31}. \tag{32}$$

Let us now set up the cipher alphabet given by $\mathcal{A}_{29}$ and the correspondence

(33)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	-1	2	-2	3	-3	4	-4	5	-5	6	-6	7	-7	8

P	Q	R	S	T	U	V	W	X	Y	Z	,	.	-
-8	9	-9	10	-10	11	-11	12	-12	13	-13	14	-14	C.

We shall use the table of products q·29 for q = 2, ..., 14 given by

58, 87, 116, 145, 174, 203, 232, 261, 290, 319, 348, 377, 406.

Then we see that the cipher system defined by the mapping $x \longrightarrow \{3\}x$ of $\mathcal{A}$ on $\mathcal{A}$ sets up a correspondence of A, ..., Z respectively to

(34)

E	F	K	L	Q	R	W	X	.,	V	U	P	O	J	I	D	C	A	B
G	H	M	N	S	T	Y	Z	-										

Here we have used properties contained in the set of congruences

$28 \equiv -1,\ 27 \equiv -2,\ 26 \equiv -3,\ 25 \equiv -4,\ 24 \equiv -5,\ 23 \equiv -6,\ 22 \equiv -7,$
$21 \equiv -8,\ 20 \equiv -9,\ 19 \equiv -10,\ 18 \equiv -11,\ 17 \equiv -12,\ 16 \equiv -13,\ 15 \equiv -14$
modulo 29.

There are also other finite fields obtained from our finite fields $\mathcal{A}_m$, where m is a prime. Such fields are the sets of polynomials of the form

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_t\alpha^{t-1} \quad (a_0, \ldots, a_t \text{ in } \mathcal{A}_m),$$

where α is a root of an equation $f(x) = 0$ of degree t, coefficients in $\mathcal{A}_m$, and not factoring in $\mathcal{A}_m$. Then α is a primitive $(q - 1)$-st root of unity, $q = m^t$ is the number of elements in this field. We designate such fields by

$$GF(m^t) \tag{35}$$

(read G, F, m^t), and call such a field a Galois field of m^t quantities. There are no other finite fields.

The fields $\mathcal{A}_m = GF(m)$, $t = 1$. Another important example is the field $GF(3^3)$ of 27 elements. Then its quantities are sums

$$a_0 + a_1\alpha + a_2\alpha^2, \tag{36}$$

where $a_i = \{0\}, \{1\}, \{2\}$ modulo 3,

$$\alpha^3 = \alpha + 1. \tag{37}$$

9. Simple and multiple alphabet substitution ciphers. A substitution cipher is a non-singular mapping

$$x = [x_1, \ldots, x_n] \longrightarrow S(x) = [u_1, \ldots, u_n], \tag{38}$$

where the x_i are the letters or other symbols of our message, and the u_i are the corresponding symbols determined by S. An important type of substitution cipher is a non-singular mapping of the type above in which

$$S(x) = [T_1(x_1), \ldots, T_n(x_n)], \tag{39}$$

for non-singular mappings T_i on $\mathfrak{M}_a$ to $\mathfrak{M}_o$, where $\mathfrak{M}_o$ is the set

of symbols we are using. Thus the mappings $T_i = T$ given by (29), (34) define such substitution ciphers. Let us also use any finite ring $\mathcal{A}$ in a cipher alphabet which is a non-singular mapping

$$x_i \longrightarrow y_i, \tag{40}$$

on $\mathcal{M}_0$ to $\mathcal{A}$. Then the mappings

$$T_i: \quad y_i \longrightarrow a_i y_i + b_i \qquad (i = 1, \ldots, n) \tag{41}$$

on $\mathcal{A}$ to $\mathcal{A}$ are non-singular for every b_i in $\mathcal{A}$ and every non-zero a_i in $\mathcal{A}$. It follows that the cipher systems defined by (38), (39), (40), (41) are definable as follows. Replace each letter of our message of n letters by a corresponding "number" of the ring $\mathcal{A}$ determined by (40). Multiply the i-th such number by the fixed non-zero number a_i in $\mathcal{A}$, add the fixed b_i, and then replace the result by the corresponding letter determined also by (40). Such ciphers are usually called <u>multiple alphabet</u> ciphers and are called <u>simple</u> or <u>monoalphabet</u> ciphers if the transformations (41) are all the same, that is, if

$$y_i \longrightarrow ay + b \qquad (i = 1, \ldots, n). \tag{42}$$

10. <u>Special multiple alphabet substitution ciphers.</u> The so-called <u>Caesar</u> cipher is the case where (41) is given by

$$y_i \longrightarrow y_i + b, \tag{43}$$

for b fixed. If we use $\mathcal{A}_{26}$ and use (27) for the mapping (40) of the Roman letters on the quantities of our ring then b is a class $\{r\}$ defined for $r = 0, 1, \ldots, 25$ and every letter x is replaced by a letter obtained by shifting it r units in the sequence

A, ..., Z of which it is a member.

The Vigenère, Gronsfield, Porta, and Beaufort cipher systems are all variants of our cipher systems determined by (27), the use of $\mathcal{A}_{26}$, and (41) for $a_i \neq \pm 1$. In the original Vigenère we use the form

$$y_i \longrightarrow y_i + b_i \qquad (i = 1, \ldots, n \tag{44}$$

of (41), where $b_i = \{r_i\}$ for r_i one of 0, 1, ..., 25, and we carry each set of n letters x_i of our messages to corresponding letters $z_1, \ldots, z_n$. Here we obtain the letter z_i by a shift of r_i letters in the alphabet on the letter x_i. The amount of shift depends upon i. Thus a key word of n symbols $g_1, \ldots, g_n$ may be given, we carry each letter g_i to a corresponding residue class $\{r_i\}$, we use $\{26\} = \{0\}$, we have $0 \leq r_i < 26$, and we shift r_i letters.

The Saint-Cyr cipher is also a true Vigenère cipher and its mechanism need not be described. The Gronsfield cipher differs only from the Vigenère in that $r_1, \ldots, r_n$ are given rather than the key word. The so called true Beaufort is the cipher system determined by

$$y_i \longrightarrow z_i = y_i - b_i \qquad (i = 1, \ldots, n), \tag{45}$$

where $b_i = \{r_i\}$, each r_i lies between 0 and 25, and we shift r_i letters backward in the alphabet. Mathematically this is identical with the Vigenère but with a different cipher system. The so-called modified Vigenère and Beaufort systems are given by

$$y_i \longrightarrow z_i = -y_i + b_i \qquad (i = 1, \ldots, n), \tag{46}$$

and

$$y_i \longrightarrow z_i = -y_i - b_i \qquad (i = 1, \ldots, n), \tag{47}$$

respectively, and are mathematically identical.

The Porta cipher is fundamentally the Vigenère but with the cipher alphabet given by

(48)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	2	3	4	5	6	7	8	9	10	11	12	13	-1	-2

P	Q	R	S	T	U	V	W	X	Y	Z
-3	-4	-5	-6	-7	-8	-9	-10	-11	-12	-13

11. Autoencipherment. A polygram substitution cipher is a cipher system given by the use of a cipher alphabet and a non-singular mapping $y = [y_1, \ldots, y_n] \longrightarrow T(y) = [z_1, \ldots, z_n]$, where each z_j is a function of all the y_i rather than a single y_i. A special case of such a system is that given by

$$z_i = y_i + b_i \qquad (i = 1, \ldots, s), \tag{49}$$

and by

$$z_i = y_i + y_{i-s} \qquad (i = s + 1, \ldots, n), \tag{50}$$

for some fixed $s < n$. Thus it results from a shift of r_i units for the first s letters and is a Vigenère for this part, and by a shift dependent on the message itself for the remaining letters in each group of n letters.

12. The cipher systems of Hill. Let us suppose that a cipher alphabet involving a finite ring $\mathcal{A}$ has been prescribed and thus that we may replace any sequence of n symbols of a message

by a sequence

$$y = [y_1, \ldots, y_n] \tag{51}$$

of quantities y_i of the ring $\mathcal{A}$. We assume that n^2 quantities a_{ij} in $\mathcal{A}$ are given as well as n other quantities $g_1, \ldots, g_n$ in $\mathcal{A}$ and let z_j be given by

$$z_j = y_1 a_{1j} + y_2 a_{2j} + \cdots + y_n a_{nj} + g_j \tag{52}$$

for $j = 1, \ldots, m$. Then the mapping defined by

$$y \longrightarrow z = [z_1, \ldots, z_m] \tag{53}$$

is a non-singular mapping if the quantities a_{ij} are such that it is possible to solve for the y_i uniquely in terms of the z_j. This occurs if $m = n$ and there exist quantities b_{ji} in $\mathcal{A}$ such that

$$y_i = z_1 b_{1i} + \cdots + z_n b_{ni} + h_i \quad (i = 1, \ldots, n), \tag{54}$$

where

$$h_i = -(g_1 b_{1i} + \cdots + g_n b_{ni}) \quad (i = 1, \ldots, n), \tag{55}$$

If $\mathcal{A}$ is any commutative ring with a unity quantity 1 the elementary theory of systems of linear equations and determinants is applicable. Its results imply that the mapping (53) is non-singular if and only if the determinant

$$d = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdot & \cdot & \cdots & \cdot \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} \tag{56}$$

has an inverse d^{-1} in $\mathcal{A}$ such that $dd^{-1} = 1$. Then it is possible to give explicit formulas for the b_{ji} in terms of d^{-1} and the $n - 1$ rowed minors of the array of which d is the determinant. In particular, if $\mathcal{A}$ is a field the mapping (53) is non-singular if and only if $d \neq 0$. Also (53) is non-singular when $\mathcal{A}$ is the residue-class ring modulo m if and only if the residue class $d = \{r\}$ for a representative integer r prime to m.]

It must be evident by now that the common substitution ciphers of Sections 10 and 11 are all special cases of the systems given by the use of (53), (52). The general transposition cipher is also such a special case. For we use a cipher alphabet with $\mathcal{A} = \mathcal{A}_{26}$ and thus replace each sequence $x = [x_1, \ldots, x_n]$ of n letters by a sequence $y = [y_1, \ldots, y_n]$ of n residue classes. We use a permutation P replacing x by $[x_{i_1}, \ldots, x_{i_n}]$ and have our result if we can use (52) to obtain $z = [y_{i_1}, \ldots, y_{i_n}]$. This may be accomplished when we take the g_i all zero, the $a_{ij} = \{0\}$ for all values of i and j except those where $i = i_j$ in which case $a_{ij} = \{1\}$.

13. The Hill systems in matrix form. A rectangular array

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1t} \\ a_{12} & a_{11} & \cdots & a_{2t} \\ \cdot & \cdot & \cdots & \cdot \\ a_{s1} & a_{s2} & \cdots & a_{st} \end{pmatrix} \tag{57}$$

is called an s by t matrix. It has s rows and t columns of elements in a ring $\mathcal{A}$ and the element a_{ij} is that element in its i-th row and j-th column. Then we may replace (57) by the abbreviated notation

(58) $$A = (a_{ij}) \qquad (i = 1, \ldots, s;\ j = 1, \ldots, t).$$

For every two s by t matrices A and

(59) $$B = (b_{ij}) \qquad (i = 1, \ldots, s;\ j = 1, \ldots, t),$$

we define

(60) $$A + B = (c_{ij}),\ c_{ij} = a_{ij} + b_{ij} \qquad (i = 1, \ldots, s;\ j = 1, \ldots, t)$$

Similarly A - B is defined so as to have $a_{ij} - b_{ij}$ in the i-th row and j-th column.

We now let

(61) $$Y = (y_{ki}) \qquad (k = 1, \ldots, r;\ i = 1, \ldots, s),$$

be any r by s matrix. Then we define the product

(62) $$W = YA = (w_{kj}) \qquad (k = 1, \ldots, r;\ j = 1, \ldots, t)$$

to be the r by t matrix whose element in the k-th row and j-th column is given by

(63) $$w_{kj} = y_{k1}a_{1j} + y_{k2}a_{2j} + \cdots + y_{ks}a_{sj}.$$

Equations (52) may be written by the use of matrices in a very simple form. The sequences y in (51) and z in (53) are both one by n matrices and we write $g = [g_1, \ldots, g_m]$. Let A be the n by m matrix whose element in the i-th row and j-th column is the coefficient a_{ij} in our equations (52). Then (52) becomes

(64) $$z = yA + g.$$

The identity mapping $y \longrightarrow z = y$ has the form (64) for $g = [0, \ldots, 0]$, $m = n$, and A the matrix I whose elements a_{ij} are all zero except that the a_{ii} are all 1. Then (54) is given by

$$y = (z - g)B, \tag{65}$$

where $AB = I$, B is the matrix inverse of A.

One may now set up what appears to be a generalization of the equations (52). We let

$$y = [Y_1, \ldots, Y_n]$$

for a set of q by s matrices Y_i. Let $A_{11}, \ldots, A_{ij}, \ldots, A_{nm}$ be a set of s by t matrices, $C_{11}, \ldots, C_{ji}, \ldots, C_{mn}$ be a set of r by q matrices, $G_1, \ldots, G_m$ be a set of r by t matrices. Then each $C_{ji}Y_iA_{ij}$ is an r by t matrix and so are the sums

$$Z_j = C_{j1}Y_1A_{1j} + \cdots + C_{jn}Y_nA_{nj} + G_j \qquad (j = 1, \ldots, m). \tag{66}$$

Nevertheless the mapping defined by (66) is only a psuedogeneralization of (52). For y may be regarded as being a sequence of nqs elements in $\mathcal{A}$, $z = [Z_1, \ldots, Z_n]$, as being a sequence of mrt elements in $\mathcal{A}$, (66) can always be expressed in the form (52).

However, the form (66) may be more convenient to use than (52). For example a mapping on a sequence $[y_1, y_2, y_3, y_4]$ involves the use of a four rowed matrix. However we may write this sequence as a matrix

$$Y = \begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix}, \tag{67}$$

and then use the mappings defined as in (66) by the equation

(68) $$Z = CYA + G$$

for two rowed square matrices C, A, G. The mapping is non-singular if matrices B and D exist such that $AB = DC = I$,

(69) $$Y = D(Z - G)B.$$

It is not as general as the mapping (52) but may be quite adequate for actual use.

14. Fractional substitutions. We have now seen how to carry a sequence of letters in a message into a corresponding array of what we may call the numbers of a ring and how to carry each such array into another by the use of a system of linear equations returning to a cryptogram consisting of a corresponding sequence of letters. This may be complicated further by the use of non-linear equations and such substitution cipher systems are known.*

Fractional cipher systems do not differ at all from the substitution cipher systems already considered in respect to the nature of the mappings defined by (52) but do differ in that a somewhat more complicated cipher alphabet is used. We let $x = [x_1, \ldots, x_s]$ be a message of s letters and replace each letter by a sequence of t quantities of a ring $\mathfrak{R}$ and thus x by $y = [y_1, \ldots, y_n]$ for $n = st$, the y_i in $\mathfrak{R}$. Clearly (52) replaces y by a sequence z in which elements arising from parts of sequences

*For example carry a letter sequence into a sequence $[y_1, \ldots, y_n]$ for the y_i in the field $\mathfrak{F}_{29}$ and no $y_i = 0$ (i.e. do not transcribe spaces as zeros but omit them). Let $k \neq 0$ and $z = [z_1, \ldots, z_n]$ be given by $z_1 = ky_1$, $z_i = y_{i-1}y_i$, for $i = 2, \ldots, n$. This is a quadratic mapping and is non-singular, it defines a substitution cipher.

corresponding to different letters may be combined. For example we set up the mapping

A	B	C	D	E	F	G
(0,0,0)	(1,0,0)	(2,0,0)	(0,1,0)	(1,1,0)	(2,1,0)	(0,2,0)
H	I	J	K	L	M	N
(1,2,0)	(2,2,0)	(0,0,1)	(1,0,1)	(2,0,1)	(0,1,1)	(1,1,1)
O	P	Q	R	S	T	U
(2,1,1)	(0,2,1)	(1,2,1)	(2,2,1)	(0,0,2)	(1,0,2)	(2,0,2)
V	W	X	Y	Z		
(0,1,2)	(1,1,2)	(2,1,2)	(0,2,2)	(1,2,2)	(2,2,2)	

with elements of our triples in the residue class ring modulo 3. Then the word FROM becomes the sequence (2,1,0,2,2,1,2,1,1,0,1,1) which we group into the set of three sequences (2,1,0,2), (2,1,2,1), (1,0,1,1) and enscribe by the use of (52) for $n = 4$ and

$$d = \begin{vmatrix} 2 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 1 & 1 & 2 \\ 1 & 0 & 0 & 2 \end{vmatrix}.$$

The result is the sequence (1,0,0,1,0,2,2,0,0,2,1,1) which yields BTCO. Here we have combined the sequence (2,1,0) arising from F with the first element in the sequence (2,2,1) arising from R.

15. Involutorial cipher systems. A substitution cipher system defined by a cipher alphabet and a non-singular mapping T of (52) is said to be involutorial if T^{-1} is the same as T. A large class of such transformations may be determined as follows. Let A be any non-singular r-rowed square matrix with a_{ij} in the i-th row and j-th column. Assume that A is symmetric (that is, the $a_{ij} = a_{ji}$) or that r is even and A is skew ($a_{ij} = -a_{ji}$). We

carry a message into a cipher alphabet (best taken to be a finite field, say $\mathcal{A}_{29}$) in which the elements a_{ij} of A lie, and then break up the message into sets of sequences of r elements which we use in groups of r as rows of corresponding matrices Y. Then we form $AY'A^{-1}$ where the columns of Y' are the rows of A.

16. Special ciphers. Let us use the alphabet given by $\mathcal{A}_{29}$ in equation (33). Consider the message given by

T	H	E	R		E	-	A	R		E	,	O	F	-	C	O	U
-10	-4	3	-9		3	0	1	-9		3	14	8	-3	-	0	2	8	11

R	S	E	,		M	O	R	E	-	E	F	F	E	C	T	I
-9	10	3	14		7	8	-9	3	0	3	-3	-3	3	2	-10	5

V	E	-	M	,	E	T	H	S	D	S	.	-
-11	3	0	7		-3	-10	-4	8	-2	10	-14	0

and then form the matrices

$$A_1 = \begin{pmatrix} -10 & -4 \\ 3 & -9 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 3 & 0 \\ 1 & -9 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 3 & 14 \\ 8 & -3 \end{pmatrix}, \quad A_4 = \begin{pmatrix} 0 & 2 \\ 8 & 11 \end{pmatrix},$$

$$A_5 = \begin{pmatrix} -9 & 10 \\ 3 & 14 \end{pmatrix}, \quad A_6 = \begin{pmatrix} 7 & 8 \\ -9 & 3 \end{pmatrix}, \quad A_7 = \begin{pmatrix} 0 & 3 \\ -3 & -3 \end{pmatrix}, \quad A_8 = \begin{pmatrix} 3 & 2 \\ -10 & 5 \end{pmatrix},$$

$$A_9 = \begin{pmatrix} -11 & 3 \\ 0 & 7 \end{pmatrix}, \quad A_{10} = \begin{pmatrix} -3 & -10 \\ -4 & 8 \end{pmatrix}, \quad A_{11} = \begin{pmatrix} -2 & 10 \\ -14 & 0 \end{pmatrix}.$$

Then we compute BA_i, where

$$B = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}, \quad B^{-1} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix},$$

and the result is enscribed as ZIZ. CQBU JXYQ PRZR XH.Z IGDE KLRY FKOV HUUM UVFW SET . The frequencies in the original message are thereby completely destroyed.

Using the same B we may also define the A_i by

$$A_1 = \begin{pmatrix} -10 & -4 \\ -4 & 3 \end{pmatrix}, \quad A_2 = \begin{pmatrix} -9 & 3 \\ 3 & 0 \end{pmatrix}, \ \ldots, \quad A_{15} = \begin{pmatrix} -14 & 1 \\ 1 & 3 \end{pmatrix}$$

and then carry our original message of 43 symbols (plus one or two nulls) into one of 60 letters. It might be said that the second -4, 3, etc. in our symmetric matrices B_i are nulls but they are still really a part of our message.

The two systems above may be combined and thus we write

$$A_1 = \begin{pmatrix} -10 & -4 \\ -4 & 3 \end{pmatrix}, \ A_2 = \begin{pmatrix} -9 & 3 \\ 0 & 1 \end{pmatrix}, \ A_4 = \begin{pmatrix} -9 & 3 \\ 3 & 14 \end{pmatrix}, \ \ldots,$$

$$A_{12} = \begin{pmatrix} -4 & 8 \\ -2 & 10 \end{pmatrix}, \quad A_{13} = \begin{pmatrix} -14 & 5 \\ 5 & -2 \end{pmatrix}$$

in which the 5, -2 are nulls. Then our message is transformed into one of 52 elements. Yet each of these systems uses the <u>same</u> matrix for enciphering and could be deciphered by one knowing the possibilities without explicit knowledge as to when the encipherer changes from ordinary to symmetric A_i.

There are over 600,000 distinct non-singular two-rowed matrices with elements in J_{29} and the particular matrix used as above may be changed at will. For example in written text it might be agreed that certain four prescribed letters represent the matrix A used to encipher that paragraph. Or we might write

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A = \begin{pmatrix} 3 & 5 \\ -2 & -3 \end{pmatrix}, \quad B = \begin{pmatrix} 3 & 3 \\ 4 & 5 \end{pmatrix}, \quad C = \begin{pmatrix} -3 & 7 \\ -1 & 2 \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

and then use the first four letters of each paragraph to give the matrix used. Thus a paragraph beginning with CIAB would have been enciphered with

$$CAB = \begin{pmatrix} -10 & 12 \\ 3 & 1 \end{pmatrix}.$$

However it might be simpler to prescribe A and B as well as four positions for letters d_1 d_2 d_3 d_4 in a paragraph of a cryptogram and use the matrix product

$$A\begin{pmatrix} d_1 & d_2 \\ d_3 & d_4 \end{pmatrix}B$$

to encipher the paragraph. Of course other devices than paragraphing to indicate a change in cipher system could be used.

The University of Chicago