INFORMATION THEORY WITHOUT THE FINITENESS ASSUMPTION, I:

CRYPTOSYSTEMS AS GROUP-THEORETIC OBJECTS

G. R. Blakley

Department of Mathematics
Texas A&M University
College Station, Texas 77843-3368

1. INTRODUCTION

This paper gives a definition of cryptosystem in terms of confusion, diffusion and replacement. This definition lends itself to infinite, as well as finite, structures, and the notion of group appears to play an essential role in it. We offer three theses for discussion. The first is that all known cryptosystems fit the definition. The second is that (Shannon) confusion amounts to left composition of a cryptographic relation with a message and left action of a cryptographic relation on a message, as well as that (Shannon) diffusion amounts to left composition of a message with a cryptographic relation and left action of a message on a cryptographic relation. The third is that what Shannon calls mixing cannot occur unless a certain type of "nonassociativity", or at least lack of adherence to some algebraic laws, is present in the descripton of a cryptosystem in accordance with this definition.

The three theses are supported by examples below. If the first cannot be readily falsified, it would be interesting to express every cryptosystem -- as well as the known cryptanalytic attacks on it -- in the style of this paper. If the second cannot, it might be appropriate to use it as a precise definition of the notions of confusion and diffusion. If the third cannot, it might be a jumping-off point for a mathematical exploration of mixing.

The approach of this paper can suggest new cryptosystems. It describes finite cryptosystems and infinite cryptosystems (such as analog speech scramblers) with equal facility. It organizes and simplifies the current variety of descriptions of cryptosystems. It is purely formal and has no place for mechanical or electrical

G.R. Blakley and D. Chaum (Eds.): Advances in Cryptology - CRYPTO '84, LNCS 196, pp. 314-338, 1985.

notions, such as lug, pin, rotor, box, etc. It can, however, describe the workings of crypto boxes which use such devices.

2. MESSAGES, CONFUSION, DIFFUSION AND REPLACEMENT

We define a message to be a map (i.e. function)

$$m: P/E \rightarrow A/L$$

where P and A are groups [PA66, p. 79], E is a normal subgroup [PA66, p. 110] of P, and L is a normal subgroup of A. We speak of P/E as being the set of character positions, and of A/L as being the alphabet. In other symbolism, a message m is a member of the cardinal power [MA67, p. 15] $(A/L)^{P/E}$. We use the algol arrow notation for exponents, and so we write instead

$$m \in (A/L) \uparrow P/E.$$

A confusion operation s is a (binary) relation [PA66, p. 15] on A/L, i.e. a subset of $A/L \times A/L$. A diffusion operation t is a (binary) relation on P/E. A replacement operation is a (binary) relation r on $(A/L) \uparrow P/E$. Usually a replacement operation is a function

$$r: (A/L) \uparrow P/E \rightarrow (A/L) \uparrow P/E ,$$

i.e. is a map which turns a message into another message. Our first thesis states that all known cryptosystems are families of cryptographic keys, and that every cryptographic key is a succession of confusion, diffusion and replacement operations or messages. Thus this paper actually moves away from the generality of the "family of maps" definition which dominates the literature [DE82, p. 7; DI79, p. 398; KO81, p. 28] at present.

For example a simple substitution cryptosystem key s is the simplest kind of confusion operation. It is a permutation of A/L, i.e. a member of the set $SYM(A/L)$ consisting [KO81, p. 65] of all permutations of A/L. To encrypt a message

$$m \in (A/L) \uparrow P/E$$

by means of a simple substitution key

$$s \in SYM(A/L) \subseteq (A/L) \to A/L$$

one forms the ordinary composite [PA66, p. 63] function

$$s \circ m \in (A/L) \to P/E$$

defined by setting

$$(s \circ m)(p) = s(m(p))$$

for every $p \in P/E$. As an example we will consider the plaintext message m = SUBSTITUTION. Let us take

$$P = Z, \quad \text{the integers under addition}$$
$$E = 12Z = \{\ldots,-12,0,12,24,36,\ldots\}$$
$$A = Z$$
$$L = 26Z$$

Thus we can view SUBSTITUTION as a function

$$m: Z/12Z \to Z/26Z$$

where we source-code by making the identification

$$1 \leftrightarrow A$$
$$2 \leftrightarrow B$$
$$\vdots$$
$$25 \leftrightarrow Y$$
$$26 = 0 \leftrightarrow Z\ .$$

In this case we have, for example,

$$m(1) = S \quad (= 19, \text{ really}),$$
$$m(2) = U \quad (= 21),$$
$$m(3) = B \quad (= 2),$$
$$\vdots$$
$$m(11) = O \quad (= 15),$$
$$m(12) = N \quad (= 14).$$

If s is the Caesar [KO81, pp. 69-72] cipher

$$s: \mathbb{Z}/26\mathbb{Z} \to \mathbb{Z}/26\mathbb{Z}$$

defined by setting

$$s(\zeta) = \zeta + 2 \pmod{26}$$

i.e.

$$A \to C$$
$$B \to D$$
$$\vdots$$
$$X \to Z$$
$$Y \to A$$
$$Z \to B.$$

then $s \circ m$ is the message

$$s \circ m(1) = s(m(1)) = s(19) = 21 = U$$
$$s \circ m(2) = s(m(2)) = s(21) = 23 = W$$
$$s \circ m(3) = s(m(3)) = s(2) = 4 = D$$
$$\vdots$$
$$s \circ m(11) = s(m(11)) = s(15) = 17 = Q$$
$$s \circ m(12) = s(m(12)) = s(14) = 16 = P$$

in other words the plaintext message SUBSTITUTION is replaced by the

cryptext message UWDUVKVWVKQP under the Caesar cryptosystem key "move two places down the alphabet."

To exemplify diffusion at the simplest level we use a transposition cipher key t on the plaintext message TRANSPOSITIONS. To model this we can choose to take:

$$P = Z ;$$

$$E = OZ = \{0\}, \text{ the small trivial subgroup;}$$

$$A = Z ;$$

$$L = 27Z .$$

Here we have chosen to identify letters, plus the blank symbol, of the latin alphabet with members of $Z/27Z$ as follows:

$$\begin{aligned} 27 = 0 &\leftrightarrow \text{blank} \\ 1 &\leftrightarrow A \\ 2 &\leftrightarrow B \\ &\vdots \\ 25 &\leftrightarrow Y \\ 26 &\leftrightarrow Z . \end{aligned}$$

Then the message

$$m: Z/OZ \to Z/27Z$$

amounts to the function

$$m: Z \to Z/27Z$$

defined by setting

$$\begin{aligned} m(\zeta) &= 0 \quad \text{if} \quad \zeta \leq 0 \\ m(\lambda) &= 0 \quad \text{if} \quad \lambda \geq 15 \\ m(1) &= T \quad (= 20, \text{ really}), \\ m(2) &= R \quad (= 18), \\ m(3) &= A \quad (= 1), \\ &\vdots \\ m(13) &= N \quad (= 14) \\ m(14) &= S \quad (= 19) . \end{aligned}$$

We can choose a transposition t which turns blocks of 7 letters around, i.e. we can choose t such that

$$t(7\delta + \beta) = 7\delta + (8-\beta)$$

for any integer δ, any positive integer $\beta \leq 7$. To encrypt the plaintext message m, i.e. the 14-letter block,

TRANSPOSITIONS

preceded and followed by infinitely many blanks, using the transposition crytosystem key t we form the cryptext message $m \circ t$. Evidently

$$(m \circ t)(\zeta) = m(t(\zeta)) = 0$$

if $\zeta \leq 0$ (for then $t(\zeta) \leq 0$) and

$$(m \circ t)(\lambda) = m(t(\lambda)) = 0$$

if $\lambda \geq 15$ (for then $t(\lambda) \geq 15$). But

$$(m \circ t)(1) = m(t(1)) = m(7) = 0$$

$$(m \circ t)(2) = m(t(2)) = m(6) = P$$

$$\vdots$$

$$(m \circ t)(6) = m(t(6)) = m(2) = R$$

$$(m \circ t)(7) = m(t(7)) = m(1) = T$$

$$(m \circ t)(8) = m(t(8)) = m(14) = S$$

$$(m \circ t)(9) = m(t(9)) = m(13) = N$$

$$\vdots$$

$$(m \circ t)(13) = m(t(13)) = m(9) = I$$

$$(m \circ t)(14) = m(t(14)) = m(8) = S$$

The cryptext $m \circ t$ is thus the 14-letter block

preceded and followed by infinitely many blanks. We note, in passing, that the definition of t is most naturally framed in terms of the cosets of the subgroup $7\mathbb{Z}$ of the group $\mathbb{Z} \doteq P$ of message positions. We will return to this theme later.

To sum up, our second thesis is that confusion (as Shannon [SH49] used the term) is applied to a message m by forming its left composite $s \circ m$ with a relation s on its codomain [MA67, p. 4]. If, in particular, s is a permutation we have substitution. Continuing the second thesis, we assert that Shannon diffusion is applied to a message m by forming its right composite $m \circ t$ with a relation t on its domain [MA67, p. 4]. If, in particular, t is a permutation we have transposition. In either case the natural group operation on the structure in question may be utilized to produce the needed permutations (or, more generally, functions or, most generally, relations).

So far we have treated the only two ways you can form composites involving a message m, on the right and on the left. There remains the possibility of regarding m itself as a domain point, and applying a function to it. This is the idea behind replacement. Replacement is a function r whose domain consists of messages and whose codomain also does. One example, though an imperfect one, of replacement is a code book.

This paper will concentrate largely on finite non-Shannon cryptosystems, i.e. collections of keys which act on finite alphabets, and which are not based on the idea of many successive applications of confusion, diffusion and replacement. The DES, an archetypal Shannon "roll the dough and fold it" [SH49] cryptosystem, will be treated in a later paper.

3. MONALPHABETS AND CAESARS

The composite $q \circ s$ of two simple (i.e. monalphabetic) substitution cipher keys

$$q: A/L \to A/L$$

$$s: A/L \to A/L$$

is itself a simple substitution cipher key

$$q \circ s\colon A/L \to A/L$$

which encrypts a message

$$m\colon P/E \to A/L$$

by the rule which defines

$$(q \circ s) \circ m\colon P/E \to A/L$$

by setting

$$((q \circ s) \circ m)(p) = (q \circ s)(m(p)) = q(s(m(p)))$$

for every P/E. The associativity, $(q \circ s) \circ m = q \circ (s \circ m)$, of function composition is what Hellman calls the closure property. It means that one cannot achieve greater strength through mixing when one merely follows one substitution by another. Since $SYM(A/L)$ is a group it follows that the collection $MON[A/L]$ of all monalphabetic substitution cipher keys on an alphabet A/L is a group isomorphic to $SYM(A/L)$. The collection $LCAE[A/L]$ of all left Caesar cipher keys on A/L is defined as follows. For each $\alpha \in A/L$ define

$$\lambda[\alpha]\colon A/L \to A/L$$

by setting

$$\lambda[\alpha](\beta) = \alpha \# \beta,$$

where $\#$ is the group operation of A/L. To encrypt a message $m\colon P/E \to A/L$ form the composite function

$$\lambda[\alpha] \circ m\colon P/E \to A/L$$

defined by setting

$$(\lambda[\alpha] \circ m)(\beta) = \lambda[\alpha](m(\beta))$$

$$= \alpha \# m(\beta)$$

for every $\beta \in P/E$. The collection $RCAE[A/L]$ of right Caesar cipher keys is defined analogously. If A/L is abelian then $LCAE[A/L] = RCAE[A/L] = CAE[A/L]$, the set of all two-sided Caesar cipher keys on A/L. It is obvious from the proof of Cayley's theorem [PA66, pp. 120-121] that $LCAE[A/L]$ (under function composition) is isomorphic to A/L. Similarly $RCAE[A/L]$ is isomorphic to A/L.

A heuristic principle suggests itself here. If there are only about as many keys in a simple substitution cipher as there are

letters in the alphabet, you may be dealing with a Caesar cipher. We shall, in accordance with this heuristic principle, see that the Pohlig-Hellman and the Rivest-Shamir-Adleman number-theoretic cryptosystems are very Caesar-like.

4. POLYALPHABETS AND ONE-TIME PADS

We now give the group-theoretic formulation of classical polyalphabetic ciphers. Let us again use source coding to replace the latin alphabet by the set $\{0, 1, 2, \ldots, 25\} \subset Z$

$$A \leftrightarrow 1$$

$$B \leftrightarrow 2$$

$$\vdots$$

$$Z \leftrightarrow 26 = 0$$

and let us agree to regard it not merely as a set [HA60, pp. 1-3], but as an additive [MA67, p. 71] abelian [MA67, pp. 71-77] group, $Z/26Z = C_{26} = Z_{26}$ [MA67, pp. 129-132]. Here, as often below, we allow ourselves to indulge in the common abuse of language which uses equality (=) where isomorphism [MA67, pp. 56-57] ($\cong$) is meant. A polyalphabetic (n alphabets) cipher key is determined by a family [HA60, p. 34]

$$s: Z/nZ \to SYM(Z/26Z)$$

of permutations [MA67, p. 72] of the "alphabet" $Z/26Z$. The family is indexed by the cosets [MA67, p. 51] (let us agree to call them by the coset leader names 1, 2, ..., n) within Z (considered as an additive abelian group) modulo the subgroup [MA67, p. 84] nZ.

From the plaintext message

$$m: Z \to Z/26Z$$

and the n-alphabetic cipher key

$$s: Z/nZ \to SYM(Z/26Z)$$

we form the cryptext message

$$y: Z \to Z/26Z$$

according to the rule

$$y(e+\lambda) = s_{\lambda}(m(e+\lambda))$$

for every member e of the subgroup $E = nZ$, every coset leader name $\lambda \in \Lambda = \{1, 2, \ldots, n\}$. There is no harm in making the identification

$$\Lambda = Z/nZ$$

as long as you stick to a particular set of coset leaders (i.e. a particular set of names of cosets). In a strict mathematical sense Λ is the range of a choice function [HA60, p. 60]

$$f: Z/nZ \to Z.$$

Such a function f has the property that $f(\Omega) \in \Omega$ for every coset $\Omega = j + nZ = \{ j + n\zeta: \zeta \in Z\}$ of nZ in Z.

To exemplify this definition in a 3-alphabet substitution case, take the message

POLYALPHABET

i.e.

$$m: Z/12Z \to Z/27Z$$

such that

$$m(1) = 16 = P$$

$$m(2) = 15 = O$$

$$m(3) = 12 = L$$

$$m(4) = 25 = Y$$

$$m(5) = 1 = A$$

$$m(6) = 12 = L$$

$$m(7) = 16 = P$$

$$m(8) = 8 = H$$

$$m(9) = 1 = A$$

$$m(10) = 2 = B$$

$$m(11) = 5 = E$$

$$m(12) = 20 = T$$

and take

$$s: Z/3Z \to SYM(Z/27Z)$$

defined by setting

$$s_0(\alpha + 0) = \alpha + 2$$

$$s_1(\alpha + 1) = \alpha + 3$$

$$s_2(\alpha + 2) = \alpha + 5$$

for each $\alpha \in 3Z$, where we have taken

$$\Lambda = Z/3Z = \{0,1,2\} .$$

Thus

$$s_1(m(1)) = s_1(16) = 16 + 3 = 19 = S$$

$$s_2(m(2)) = s_2(15) = 15 + 5 = 20 = T$$

$$s_0(m(3)) = s_0(12) = 12 + 2 = 14 = N$$

$$s_1(m(4)) = s_1(25) = 25 + 3 = 2 = B$$

$$s_2(m(5)) = s_2(1) = 1 + 5 = 6 = F$$

$$s_0(m(6)) = s_0(12) = 12 + 2 = 14 = N$$

$$s_1(m(7)) = s_1(16) = 16 + 3 = 19 = S$$

$$s_2(m(8)) = s_2(8) = 8 + 5 = 13 = M$$

$$s_0(m(9)) = s_0(1) = 1 + 2 = 3 = C$$

$$s_1(m(10)) = s_1(2) = 2 + 3 = 5 = E$$

$$s_2(m(11)) = s_2(5) = 5 + 5 = 10 = J$$

$$s_0(m(12)) = s_0(20) = 20 + 2 = 22 = V$$

So the 3-alphabetic encryption of

POLYALPHABET

in this key s is

STNBFNSMCEJV .

Suppose that $n = 1$. Then $nZ = 1Z = Z$ is the large trivial subgroup and

$$Z/nZ = Z/Z = \{0\} = 0Z$$

(up to isomorphism). In this case the key s is a one-permutation family, i.e. a monalphabetic substitution cipher key. If $n = 0$ then

$$nZ = 0Z = \{0\}$$

is the small trivial subgroup and

$$Z/nZ = Z/0Z = Z/\{0\} = Z$$

(up to isomorphism). In this case the key $s: Z \to SYM(Z/26Z)$ is an infinite family of permutations of the "alphabet" $Z/26Z$, one for each plaintext message letter. This is a one-time substitution (somewhat fancier than the classical bitwise one-time pad [KO81, p. 135] which uses $Z/2Z$ rather than $Z/26Z$ as its alphabet).

Evidently the underlying structure which embraces monalphabets (including Caesars), polyalphabets, and one-time pads is

$$m: P \to A/L$$

$$s: P/E \to SYM(A/L)$$

$$y: P \to A/L$$

where P is a group with normal [MA67, p. 106] subgroup E, where A is a group with normal subgroup L, where $SYM(A/L)$ is the set (it is in an obvious and natural sense a group, of course) of permutations of A/L, where $m: P \to A/L$ is an arbitrary message, where $\#$ is the group operation in P, and where

$$y(e \# \lambda) = s_{\lambda}(m(e \# \lambda))$$

for every $e \in E$, every coset [MA67, pp. 101-103] leader $\lambda \in \Lambda = P/E$ (equality being used where isomorphism is meant). Such a structure is called a (polyalphabetic) substitution cipher key. You can use right cosets instead of left cosets, with the obvious changes. Most

classical cryptosystems are based on additive [MA67, p. 71] abelian groups, so cosets are two-sided.

The composite of two substitution cipher keys

$$s: P/E \to SYM(A/L)$$

$$\overline{s}: P/\overline{E} \to SYM(A/L)$$

is a substitution cipher key.

$$u: P/(E \cap \overline{E}) \to SYM(A/L)$$

In the commonest case we are dealing with residue classes [PA66, p. 53] of integers:

$$P/E = Z/nZ.$$

$$P/\overline{E} = Z/\overline{n}Z.$$

We let $m = \text{lcm}(n , \overline{n})$, the least common multiple [PA66, p. 44] of n and $\overline{n}$ and we find that

$$nZ \cap \overline{n}Z = mZ$$

Thus the composite of a 12-alphabetic substitution key on the alphabet A/L and a 42-alphabetic substitution key on A/L (in either order) is an 84-alphabetic substitution key on A/L.

The composite of a simple substitution cipher key with an n-alphabetic substitution cipher key is n-alphabetic. The composite of any substitution cipher key with a one-time pad is a one-time pad. The collection of all substitution cipher keys on an alphabet A/L forms a group.

5. INFINITE SUBSTITUTION CIPHERS AND TORSION

The classical Vernam/Mauborgne one-time pad using a two-member alphabet can be described as

$$m: Z \to Z/2Z$$

$$s: Z/0Z \to SYM(Z/2Z)$$

$$y(\lambda) = y(0+\lambda) = s_{\lambda}(m(0+\lambda)) = s_{\lambda}(m(\lambda))$$

for every $\lambda \in Z$. Since $0Z$ is the inverse limit (i.e. projective limit [MA71, pp. 68-72], in this case the intersection [HA60, pp. 14-18]) of the members of the sequence

$$Z = \{Z, 2Z, 3Z, \ldots\}$$

we can say that $Z = Z/0Z$ is a sort of limit of Z/Z, $Z/2Z$, $Z/3Z$,..., and thus that the one time pad is not merely an ∞ alphabetic substitution cipher. It is also a limit of polyalphabetic substitution ciphers. It is torsion-free (i.e. lacking in nonzero elements of finite order [MA67, p. 81]). But it is not the only limit of polyalphabetic ciphers. Evidently for every nonzero rational number q, the group Q/qZ amounts (up to isomorphism) to Q/Z, the rationals [MA67, pp. 166-171] modulo 1. This group Q/qZ is the direct limit (i.e. inductive limit, colimit [MA71, pp. 67-68]. In this case, in a natural sense, the direct limit is the union [HA60, pp. 12-13] of the terms) of the sequence [HA60, p. 45]

$$Z/Z, Z/2Z, Z/3Z, \ldots .$$

This group is also the jumping-off point for the cipher key based on

$$m: Q \to A/L$$

$$s: Q/qZ \to SYM(A/L)$$

$$y(e + \lambda) = s_\lambda(m(e + \lambda))$$

for every $e \in qZ$, every $\lambda \in \Lambda$ (the set of coset leaders of Q/qZ). This is also an ∞ alphabetic substitution cipher. But it is all torsion [MA67, pp. 344-348] (i.e. every element of Q/qZ is of finite order). It repeats its (infinitely) many permutations of its alphabet at intervals of q. This suggests yet another ∞ alphabetic substitution cipher key based on

$$m: R \to A/L$$

$$s: R/rZ \to SYM(A/L)$$

$$y(e + \lambda) = s_\lambda(m(e + \lambda))$$

for every $e \in rZ$, every $\lambda \in \Lambda$ (the set of coset leaders of R/rZ), where r is any nonzero real number. The structure R/rZ has very little torsion. Only the rational multiples of r have finite order. And they form a set of Lebesgue measure [RO71, pp. 52-63]

zero. This cipher key repeats its alphabets at intervals of r. If these last two cipher keys (the one whose permutations of its alphabet are indexed by Q/qZ and the one whose permutations of its alphabet are indexed by R/rZ) are equally easy to break, then torsion would seem to have little to do with the cryptanalysis of polyalphabetic substitution ciphers. If not, then torsion may play a role in such cryptanalysis.

6. TRANSPOSITION CIPHERS

A natural example of how cosets arise in transposition ciphers can be given in terms of a transposition cipher key which turns the message

HOMOMORPHISM

into the message

OMOHPROMMSIH.

One way to obtain this encryption is to reverse successive four letter strings

HOMO → OMOH

MORP → PROM

HISM → MSIH

This is compatible with the definitions

$$m = \{(1,H), (2,0), \ldots, (12,M)\} \cup \{ (j,\text{blank}): j \notin \{1, 2, \ldots, 12\} \}$$

and

$$t = \{(4w+1, 4w+4), (4w+2, 4w+3), (4w+3, 4w+2), (4w+4, 4w+1): w \in Z\},$$

whence

$$m \circ t = \{(1,0), (2,M), \ldots, (12,H)\} \cup \{(j,\text{blank}): j \notin \{1, 2, \ldots, 12\}\}$$

Such transposition cipher keys are clearly of the form

$$y(e + \lambda) = m(f(e + \lambda)) = m(e + t(\lambda))$$

where $f(e + \lambda) = e + t(\lambda)$ and

$$t \in SYM(\Lambda) = SYM(P/E)$$

is arbitrary. In the case at hand

$$P = Z$$

$$E = 4Z$$

$$P/E = Z/4Z = \Lambda = \{1, 2, 3, 4\}$$

$$t = \{(1,4), (2,3), (3,2), (4,1)\}.$$

7. MIXING AND "ASSOCIATIVITY"

The designer of a cryptosystem has no reason to be grateful for the associative law of function composition. Suppose, for example, that

$$q: A/L \to A/L$$

$$s: A/L \to A/L$$

are monalphabetic substitution cipher keys and that

$$t: P/E \to P/E$$

$$u: P/E \to P/E$$

are transposition cipher keys. Then we know from associativity that

$$q \circ (s \circ (m \circ (t \circ u))) = ((q \circ s) \circ m) \circ (t \circ u) = \ldots = q \circ s \circ m \circ t \circ u .$$

Such combinations of keys exhibit what Hellman calls closure. Repeated operations do not enhance security. Whenever, on the other hand, one can contrive operations such that, for example,

$$q \circ ((s \circ (m \circ t)) \circ u) \neq ((q \circ s) \circ (m \circ t)) \circ u$$

or

$$s(m(\alpha + \beta)) \neq s(m(\alpha)) + s(m(\beta))$$

the possibility of greater cryptographic strength exists. The third thesis of this paper is that mixing (in the Shannon [SH49] sense) amounts to the failure of algebraic identities (such as commutative,

distributive or, especially, associative laws) which would make a cryptanalyst's job easier when dealing with cryptosystems which are compounded of a succession of confusion, diffusion, and replacement operations.

How can associativity fail? It cannot when transposition and monalphabetic substitution are the only operations used. But we also have both polyalphabetic substitution and replacement at our disposal.

Consider, first, a message

$$m \in (A/L) \uparrow P/E ,$$

a simple substitution

$$s \in (A/L) \uparrow A/L$$

and a replacement

$$r: (A/L) \uparrow P/E \to (A/L) \uparrow P/E .$$

The expression $r(s \circ m)$ makes sense and, in fact,

$$s \circ m \in (A/L) \uparrow P/E ,$$

whence

$$r(s \circ m) \in (A/L) \uparrow (P/E)$$

makes perfectly good sense. But what can $(r(s)) \circ m$ mean? After all

$$s \in (A/L) \uparrow (A/L)$$

but the domain of r is $(A/L) \uparrow P/E$. So there is usually no way to make sense of $r(s)$, much less $(r(s)) \circ m$. Consequently we conclude that an equality such as

$$r(s \circ m) = (r(s)) \circ m$$

is impossible (and, in fact, nonsensical) in all but very special and contrived circumstances. What about a comparison between $r(m \circ t)$ and $(r(m)) \circ t$? In this case both symbols make sense, and both

symbols belong to

$$(A/L) \uparrow P/E \ .$$

But are they equal? Not usually. For example let

$$P = A = Z \ ,$$

$$E = L = 2Z \ ,$$

whence

$$P/E = A/L = Z/2Z \ .$$

Let

$$m = \{(0,0), (1,1)\}$$

$$t = \{(0,1), (1,0)\}$$

$$r(\{(0,0), (1,1)\}) = \{(0,1), (1,1)\}$$

$$r(\{(0,1), (1,0)\}) = \{(0,0), (1,0)\}$$

Then

$$m \circ t = \{(0,1), (1,0)\}$$

$$r(m \circ t) = \{(0,0), (1,0)\}$$

$$r(m) = \{(0,1), (1,1)\}$$

$$(r(m)) \circ t = \{(0,1), (1,1)\}$$

whence

$$r(m \circ t) \neq (r(m)) \circ t \ .$$

An equation such as

$$r(m \circ t) = (r(m)) \circ t$$

is not, of course, a true associative law, since $r(m)$ is the action of a function r on a "point" m of its domain, whereas $m \circ t$ is the composite of the function m following the function t. The design of DES uses all three operations, confusion, diffusion and replacement. And it achieves mixing by exploiting such failures of "associativity" in its rounds.

"Associativity" can fail in other ways, too. We will content ourselves with merely mentioning one more example of failure of "associativity". The reader can easily verify the fact that polyalphabetic substitutions need not commute with transposition, even though monalphabetic substitution does, i.e. even though

$s \circ (m \circ t) = (s \circ m) \circ t$ when m is a message, s is a monalphabetic substitution, and t is a transposition.

8. NUMBER-THEORETIC CRYPTOSYSTEMS, MONALPHABETS AND CAESARS

The Pohlig-Hellman [PO78] conventional cryptosystem (PHC) and the Rivest-Shamir-Adleman [RI78] public key cryptosystem (RSA) are number-theoretic cryptosystems in the sense of [BL79]. PHC is the 1-prime case. Both the prime p and $\phi(p) = \lambda(p) = p-1$ must be kept secret. RSA is the 2-prime case. The prime p and q, as well as the totient $\phi(pq) = (p-1)(q-1)$ and the universal [LE56, Vol. 1, pp. 53-56] exponent $\lambda(pq)$ must be kept secret. Both cryptosystems are monalphabetic substitutions with large Caesar subsystems.

To make this statement precise we sketch the definition of a general number-theoretic cryptosystem. So let

$$w = \Pi p$$

be a (square-free) product of odd primes p belonging to a (secret) set P of primes. Since P is secret, the universal exponent $\lambda(w)$ is secret. $\lambda(w)$ is, by definition, the least common multiple of the members of the set $\Lambda = \{p-1: p \in P\}$.

For a given modulus $w = \Pi p$ there are $\phi(\lambda(w))$ encode/decode pairs (c,d) of positive integers less than $\lambda(w)$ such that

$$cd \equiv 1 \pmod{\lambda(w)}.$$

Encoding is the process

$$x \to x \uparrow c \bmod w$$

Decoding is

$$y \to y \uparrow d \bmod w.$$

Any key (c,d) in this cryptosystem thus amounts to an encryption process which is a permutation of Z/wZ. Number-theoretic cryptosystems are thus monalphabetic substitutions on the alphabet

$$A/L = Z/wZ$$

Since there are so few keys (c,d) corresponding to a given modulus w (i.e. to an alphabet $A/L = Z/wZ$) one might suspect the existence of a Caesar cipher, perhaps on a subset of this alphabet. And one does exist. There are elements $\gamma \in Z/wZ$ with (multiplicative) order $\lambda(w)$. Let γ be one of them and let $\Gamma \subseteq Z/wZ$ be the set

$$\Gamma = \{\gamma, \gamma\dagger 2, \gamma\dagger 3, \ldots, \gamma\dagger\lambda(w) = 1\}$$

of powers of γ. Evidently Γ is a rather large subset of Z/wZ, since $\lambda(w)/w$ is fairly close to 1 if w is the product of just a few primes p such that $p-1$ does not have many small factors. The encryption process $x \to x\dagger c$ effects a permutation of the members of any such Γ, since c is relatively prime to $\lambda(w)$. Encryption on Γ is the mapping

$$\gamma\dagger a \to (\gamma\dagger a)\dagger c = \gamma\dagger(a*c) \ .$$

where the asterisk denotes multiplication modulo $\lambda(w)$. Thus the encryption process, restricted to Γ, is determined by the Caesar cipher mapping

$$a \to a*c \ .$$

But to exploit our knowledge of the existence of very large Caesar subsystems of an RSA public key cryptosystem [RI78] or a Pohlig-Hellman conventional cryptosystem [PO78] we appear to have to find some appropriate γ, as well as its corresponding set Γ, and be able to solve a corresponding discrete logarithm problem.

Let us take an RSA example. Let $w = 35$. The RSA is a monalphabet substitution cipher on the 35 member alphabet $Z/35Z$. In this case

$$\lambda(w) = \lambda(35) = 12$$

The $\phi(\lambda(35)) = \phi(12) = 4$ keys amount to the 4 encrypt/decrypt exponent pairs

$$(c,d) = (1,1),$$

$$(c,d) = (5,5),$$

$$(c,d) = (7,7),$$

$$(c,d) = (11,11).$$

One such Γ is the set

$$\Gamma = \{2,4,8,16,32,29,23,11,22,9,18,1\}$$

of all powers of $\gamma = 2$. Let us note what happens when the key (5,5) is used.

$$2\uparrow 5 = (2\uparrow 1)\uparrow 5 = 2\uparrow(1*5) = 2\uparrow 5 = 32$$
$$4\uparrow 5 = (2\uparrow 2)\uparrow 5 = 2\uparrow(2*5) = 2\uparrow 10 = 9$$
$$8\uparrow 5 = (2\uparrow 3)\uparrow 5 = 2\uparrow(3*5) = 2\uparrow 3 = 8$$
$$16\uparrow 5 = (2\uparrow 4)\uparrow 5 = 2\uparrow(4*5) = 2\uparrow 8 = 11$$
$$32\uparrow 5 = (2\uparrow 5)\uparrow 5 = 2\uparrow(5*5) = 2\uparrow 1 = 2$$
$$29\uparrow 5 = (2\uparrow 6)\uparrow 5 = 2\uparrow(6*5) = 2\uparrow 6 = 29$$
$$23\uparrow 5 = (2\uparrow 7)\uparrow 5 = 2\uparrow(7*5) = 2\uparrow 11 = 18$$
$$11\uparrow 5 = (2\uparrow 8)\uparrow 5 = 2\uparrow(8*5) = 2\uparrow 4 = 16$$
$$22\uparrow 5 = (2\uparrow 9)\uparrow 5 = 2\uparrow(9*5) = 2\uparrow 9 = 22$$
$$9\uparrow 5 = (2\uparrow 10)\uparrow 5 = 2\uparrow(10*5) = 2\uparrow 2 = 4$$
$$18\uparrow 5 = (2\uparrow 11)\uparrow 5 = 2\uparrow(11*5) = 2\uparrow 7 = 23$$
$$1\uparrow 5 = (2\uparrow 12)\uparrow 5 = 2\uparrow(12*5) = 2\uparrow 0 = 1$$

So more than 1/3 of this RSA is a concealed version of the Caesar cipher

$$t \to 5t \text{ modulo } 12$$

acting on the set

$$\{1,2,\ldots,10,11,0 = 12 = \lambda(35)\}$$

A different γ, Γ pair would be

$$\gamma = 3$$
$$\Gamma = \{3,9,27,11,33,29,17,16,13,4,12,1\}.$$

A similar analysis can be provided for the Caesar cipher based on this γ, Γ pair.

It seems inappropriate to regard number-theoretic cryptosystems as weak because each of them has a huge subsystem Γ such that the cryptosystem operation on Γ is equivalent to a Caesar cipher key. We are left, rather, with a renewed respect for the much-maligned Caesar cipher because it can be transformed and inserted into a

number-theoretic cryptosystem in a natural way that, as of this writing, leaves it unbroken.

9. RSA and factorization

RSA is formulated with Z and Z/wZ as the rings which draw most of our notice. We therefore pay a lot of attention to the problem of factoring w into the product of two primes p and q in the ring Z of integers. But the group-theoretic approach is neutral as regards the ring in question. There are infinitely many factorizations of an RSA modulus w. Many, such as the trivial factorizations

$$w = 2 * (w/2)$$

or

$$w = \sqrt{3} * (w/\sqrt{3})$$

seem to hold out little promise to a cryptanalyst.

At Crypto '83 H. C. Williams suggested a somewhat more disciplined -- and perhaps more informative -- approach to factorization. It might be interesting to look at factorizations in the integral domain $Q[\theta]$ of an algebraic number [LE56, vol. 2, pp. 34-81] field $Q(\theta)$ (Here Q is the field of rational numbers, and θ is algebraic over Q). Such a factorization might [CR83] contain information sufficient to enable a cryptanalyst to calculate a large multiple $k\phi(pq)$ of $\phi(pq) = (p-1)(q-1)$. This would be enough information to provide a (very large) decoding exponent.

The question of how to search for an appropriate θ (perhaps of the form $\theta = \sqrt{d}$ for $d \varepsilon Z$) and how to calculate a generalized Euler totient function in that $Q[\theta]$ is open. But it would seem that those who wish to use RSA might want to satisfy themselves that it does not yield to attacks of the $Q[\theta]$ type any more readily than to attacks made entirely within Z.

10. DISCUSSION

The motivation behind this work was to extend cryptography to infinite structures by analogy with recent extensions of the notion of threshold scheme [BL83] to infinite structures. But it seems

necessary to justify the naturalness of the group-theoretic formulation as an abstraction arising out of consideration of many finite, as well as a few infinite, structures. So this paper dealt largely with finite examples, and very simple ones, to argue for the ubiquity of the

$$m: P/E \to A/L$$

structure of messages. In the analog case, to be considered elsewhere, P/E and A/L are more likely to be infinite groups such as $R/OR = R$, or $R/2\pi Z$ (essentially the complex unit circle under multiplication).

We have given candidates for precise definitions of the rather intuitive notion of confusion (including substitution as a special case) and diffusion (including transposition). We have distinguished between a cryptosystem (a family of keys) and a key, i.e. a map which can be expressed in terms of confusion, diffusion, and replacement. This approach to key seems more mathematically natural than the old-fashioned viewpoint which regards a key as a number which, when entered into a crypto box, gives rise to the map this paper calls a key.

We have given a precise definition of Caesar cipher more general than the one commonly found [KO81, pp. 69-72] in the literature, and have shown that Caesars are not as cryptographically trivial as the conventional wisdom dictates. The Caesar cipher illustrates well, in a confusion/substitution context, what we hope to exemplify elsewhere regarding diffusion/transposition, namely that the natural group operation on the domain (resp. codomain) is often the basis of the diffusion operator t (resp. confusion operator s).

The maps encountered in the keys which make up most well-known cryptosystems are not morphisms. Indeed the less algebraic structure these maps exhibit, the more likely the cryptosystems employing them in keys are to be secure. This seems to suggest more reliance on nonabelian groups P and A both in the design of future cryptosystems and in the upgrading of existing cryptosystems. Perhaps, eventually, even more general structures (e.g. monoids, semigroups, etc.) might become useful in cryptosystem design.

More complicated finite cryptosystems, such as Polybius, Delastelle, Playfair [KA67] and the remarkably highly structured DES, require a deeper and more interesting elaboration of the topics introduced above. After that it will be natural to turn to infinite structures and to cryptanalysis. We will treat such topics elsewhere.

NSA Grant MDA-83-H-0002 supported this work.

11. REFERENCES

AD83 L. M. Adleman, C. Pomerance and R. S. Rumely, On distinguishing prime numbers from composite numbers, Annals of Mathematics, vol. 117 (1983), pp. 173-206.

BA64 R. G. Bartle, The Elements of Real Analysis, Wiley, New York (1964).

BE82 H. Beker and F. Piper, Cipher Systems: The Protection of Communications, Wiley-Interscience, New York (1982).

BE83 G. R. Blakley and Laif Swanson, Infinite structures in information theory, in D. Chaum, R. L. Rivest and A. T. Sherman, Advances in Cryptology, Proceedings of Crypto '82, Plenum Press, New York (1983), pp. 39-50.

BL79 Bob Blakley and G. R. Blakley, Security of number theoretic public key cryptosystems against random attack, Part I, Cryptologia, Vol. 2 (1978), pp. 305-321, Part II, Vol. 3 (1979), pp. 29-42, Part III, Vol. 3 (1979), pp. 105-118.

CR83 J. T. Cross, The Euler ϕ function in the Gaussian integers, American Mathematical Monthly, vol. 90 (1983), pp. 518-528.

DE82 D. E. R. Denning, Cryptography and Data Security, Addison-Wesley, Reading, Massachusetts (1982).

DI79 W. Diffie and M. E. Hellman, Privacy and authentication, An introduction to cryptography, Proceedings of the IEEE, vol. 67 (1979), pp. 397-427.

GD58 C. Goffman, Real Functions, Rinehart, New York (1958).

HA60 P. R. Halmos, Naive Set Theory, Van Nostrand, Princeton, New Jersey (1960).

KA67 D. Kahn, The Codebreakers, MacMillan, New York (1967).

LE56 W. J. LeVeque, Topics in Number Theory, Addison-Wesley, Reading, Massachusetts (1956).

KO81 A. G. Konheim, Cryptography: A Primer, Wiley-Interscience, New York (1981).

MA67 S. MacLane and G. Birkhoff, Algebra, Macmillan, New York (1967).

MA71 S. MacLane, Categories for the Working Mathematician, Springer-Verlag, Berlin (1971).

ME82 C. H. Meyer and S. M. Matyas, Cryptography: A New Dimension in Computer Data Security, Wiley-Interscience (1982)

MO63 G. D. Mostow, J. H. Sampson and J.-P. Meyer, Fundamental Structures of Algebra, McGraw-Hill, New York (1963).

PA66 H. Paley and P. M. Weichsel, A First Course in Abstract Algebra, Holt, Rinehart and Winston, New York (1966).

PO78 S. C. Pohlig and M. E. Hellman, An improved algorithm for computing logarithms over GF(p) and its cryptographic significance, IEEE Transactions on Information Theory, Vol. IT-24 (1978), pp. 106-110.

QU82 J.-J. Quisquater and C. Couvreur, Fast decipherment algorithm for RSA public-key cryptosystem, Electronics Letters, Vol. 18, No. 21, Oct. 14 (1982), pp. 905-907.

RI78 R. L. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public key cryptosystems, Communication of the ACM, Vol. 21 (1978), pp. 120-126.

RO71 H. L. Royden, Real Analysis, Macmillan, London (1971).

SH49 C. E. Shannon, Communication theory of secrecy systems, Bell System Technical Journal, vol. 28, (1949), pp. 656-715.

ST33 H. S. Stone, Discrete Mathematical Structures and their Applications, Science Research Associates, Chicago (1973).