Information theory without the finiteness assumption, II. Unfolding the DES

G. R. Blakley

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

AMS(MOS) Subject Classifications:
03D15, 08A99, 15A99, 20B99, 20D99, 68B99, 68C99, 94A99

ACM CR Categories and Subject Descriptors:
E.3, E.4, F.2.0, F.2.1, G.1.3, J.7

Key Words

alphabet, arithmetic, associativity, Caesar cipher, code, codomain, commutativity, composite, confusion, continuous, cryptosystem, cyclic group, DES, diffusion, discrete, distributivity, domain, field, function, galois field, group, matrix, message, polyalphabet, position, product, ramp scheme, relation, replacement, ring, substitution, sum, symbol, symmetric group, threshold scheme, toroidal matrix, transposition, universal algebra, vector space.

Abstract

The DES is described in purely mathematical terms by means of confusion, diffusion and arithmetic involving a group of messages and a group of keys. It turns out to be a diffusion/arithmetic cryptosystem in which confusion plays no role, although the S-boxes effect an arithmetic operation of replacement (which is sometimes mistaken for confusion) as an important part of the encryption process.

H.C. Williams (Ed.): Advances in Cryptology - CRYPTO '85, LNCS 218, pp. 282-337, 1986.

1. Introduction

Group-theoretic structures appear to underly all of cryptography and error control. In particular, cryptosystems all appear to employ four groups: a group K of keys; a group A, called the alphabet, of symbols; a group P of positions which symbols can occupy; and a group A^P of messages, i.e. functions from P to A. Every cryptosystem is a pair (c, d) of self-maps of $K \times A^P$ and is thus, from a mathematical viewpoint, a pair of very large matrices c and d. The coding map c turns an encrypt key $k \in K$ and a plaintext message $m \in A^P$ into a decrypt key $\overline{k} \in K$ and a cryptext message $\overline{m} \in A^P$. The decoding map d takes the pair $(\overline{k}, \overline{m})$ as inputs and recovers (k, m). The keys k and $\overline{k}$ are merely inverses of each other in the group K. In a conventional cryptosystem the group K is widely known and it is easy to produce the inverse $\overline{k}$ of k. Not so in a public key cryptosystem. In either type of cryptosystem the cryptext message $\overline{m}$ depends in a complicated way on both k and m.

Interestingly, all cryptosystems appear to be built up on the basis of just three primitives:

> (Shannon) confusion, a generalization of cryptographic substitution;
>
> (Shannon) diffusion, a generalization of cryptographic transposition; and

arithmetic (in the sense of universal algebra operations derived from the composition laws associated with the groups K, A, P and A^P). One extremely important arithmetic operation is replacement, a generalization of the notion of a cryptographic codebook.

These notions of confusion, diffusion and arithmetic can now be precisely defined, and so the general definition of cryptosystem herein is at once less general and more abstract than the one [DI79, p. 398; KO81, p. 28; DE82, p. 7; BE82, pp. 125-130; ME82, p. 14-53] which appears in the literature to date.

The DES exhibits rich structure, and is therefore a good exemplar of this approach to cryptography. The four groups in question are as follows. The alphabet group A is the field $A = GF(2) = Z/2Z$ with two elements. The group P of positions is the ring $P = Z/64Z$ of integers modulo 64. Hence the group A^P of messages is the 64-dimensional vector space $A^P = (Z/2Z)^{(Z/64Z)}$ of 64-bit words. The key group K is a 56-dimensional vector subspace of A^P. When DES is expressed in these terms it becomes clear that it uses no confusion at all, merely diffusion and arithmetic. However, part of the arithmetic is a unary operation based on the S-boxes. Unary operations, replacements in our terminology, are reminiscent of confusions and are often mistaken for them.

2. Messages, codes, cryptosystems, confusion, diffusion, arithmetic

This paper continues and refines the approach begun in [BL83; BL85b]. The idea is to reformulate information-theoretic objects such as codes (both error-control codes and cryptographic codes) ciphers, cryptosystems, and ramp schemes [BL85a] in terms of group theory. By this means we hope to produce many new objects (both continuous [BL87] and discrete) of the sorts described above, as well as to gain a deeper understanding of the existing ones.

As far as cryptography goes, the idea is to define a message as a map $m : P \rightarrow A$ from a group P of symbol positions to a group A of alphabetic characters (i.e. symbols). A map between groups might be expected to be a group homomorphism. If the groups are topological groups it might be expected to be continuous. But cryptosystem designers often try to avoid "nice" algebraic, analytic or probabilistic structure. Even if messages (i.e. members of A^P) have significant algebraic, analytic or probabilistic structure, cryptosystems are often built so as to have as little such structure as possible. The set A^P is a group in a natural manner induced by the group structure on A. Composition of maps is indicated by the $\circ$ operation symbol everywhere below. Thus $d \circ c$ is the map d following the map c, and $d * c$ is the product of d and c if a natural product operation $*$ exists.

Definition 2.1: Let K, A and P be groups. We call A the alphabet. We call P the group of symbol positions. We call A^P the group of messages. We call K the group of keys. A cryptosystem on A^P with keyspace K is a pair of maps

$$c : K \times A^P \to K \times A^P$$

$$d : K \times A^P \to K \times A^P$$

such that

$$(d \circ c)((k, m)) = d(c((k, m))) = (k, m)$$

for all $(k, m) \in K \times A^P$.

If we write

$$c((k, m)) = (\overline{k}, \overline{m})$$

it seems usually to be true that $\overline{k}$ does not depend on m, but is merely the inverse of k in whatever arithmetic is natural on K. In DES we have

$$\overline{k} = -k = k$$

in a vector space K over $GF(2)$, whence $-k = k$. In RSA we have [BL85b, p. 332]

$$\overline{k} \equiv k^{-1} \bmod \lambda(p * q)$$

in a ring $Z/\lambda(p * q)Z$ in which k is invertible. In a simple substitution cipher the decode key $\overline{k}$ is the permutation inverse k^{-1} of the encode key $k \in \mathrm{SYM}(A)$. Here, as in [KO81, p. 65], we use the notation $\mathrm{SYM}(A)$ for the symmetric group on the set A, i.e.

the group of all permutations of A. In a transposition cipher we similarly have $\overline{k} = k^{-1} \in \mathrm{SYM}(P)$. The cryptext message $\overline{m}$, on the other hand, seems always to depend on both k and m. In fact cryptosystem designers often have to force some mutual compatibility on the group structures of A^P and K in order to make this dependence easy to calculate.

Definition 2.1 can certainly be generalized. We have assumed that the set A^P of plaintext messages is the same as the set of cryptext messages. This'is often true, but doesn't have to be.

In short, a cryptosystem is a pair of matrices whose entries are chosen from the set of their (common) indices. This matrix structure does not necessarily make a cryptosystem easy to reconstruct or cryptanalyze. DES, for example, can be viewed as a 2^{56} by 2^{64} matrix with entries chosen from $GF(2)^{56} \times GF(2)^{64}$. Sometimes it is preferable to regard DES as a 2^{64} by 2^{64} matrix with entries chosen from $GF(2)^{64} \times GF(2)^{64}$, as we shall see in Section 3 below. An RSA is typically a $\phi(\lambda(p*q))$ by $p*q$ matrix with entries chosen from

$$K \times A^P = [Z/\phi(\lambda(p*q))Z] \times [Z/p*qZ],$$

where the primes p and q exceed 2^{250}.

Our thesis is that all known cryptosystems are built using only three notions: confusion, diffusion, and arithmetic. Confusion (a generalization of substitution) is a selfmap

$$s : A \to A$$

of A or even merely a binary relation s on A. In other words a confusion acting on a message $m : P \to A$ is a member s of the power [HA60, p. 100] set $2^{A \times A}$. But often a confusion is a member s of A^A. There is a well known canonical injection

$$i : A^A \to 2^{A \times A}.$$

So the $s \in A^A$ definition is just a (most commonly encountered) case of the $s \in 2^{A \times A}$ definition. Actually we are sometimes driven even further than this (e.g. when we have to describe [BL85b, pp. 322-326] polyalphabetic substitutions [DE82, pp. 73-87] and one-time pads [DE82, pp. 86-87]). So our final definition of confusion is a family s of members of A^A, or even of members of $2^{A \times A}$. In ultimate generality, then, we have

Definition 2.2: Let A and P be groups. We call A^P the group of messages. A confusion on A^P is a family

$$s : I \to 2^{A \times A}$$

of binary relations on A. In particular, a family

$$s : I \to A^A$$

of self-maps of A is a confusion on A^P. Here, I is any index set. If I is a singleton and

$$s : I \rightarrow \mathrm{SYM}(A)$$

then s is a monalphabetic substitution on A^P.

Here, as above, $\mathrm{SYM}(A)$ is the group of permutations of A. Clearly

$$\mathrm{SYM}(A) \subseteq A^A \subseteq 2^{A \times A}.$$

Similarly

$$\mathrm{SYM}(P) \subseteq P^P \subseteq 2^{P \times P}.$$

Thus, by analogy with the definition of confusion, we have

Definition 2.3: Let A and P be groups. We call A^P the group of messages. A diffusion on A^P is a family

$$t : J \rightarrow 2^{P \times P}$$

of binary relations on P. In particular, a family

$$t : J \rightarrow P^P$$

of self maps of P is a diffusion on P. Here J is any index set. If J is a singleton and

$$t : J \rightarrow \mathrm{SYM}(P)$$

then t is a transposition on A^P (or, at worst, an anagram on A^P).

This time the idea is that a diffusion acting on A^P is a selfmap

$$t : P \rightarrow P$$

of P or, at worst, a family of binary relations on P. As before, we allow the possibility of an entire family of self-maps of P, or even of an entire family of binary relations on P. Even such an object is called a diffusion.

The word *arithmetic* is taken in the sense of universal algebra [GR68]. Nullary, unary, binary, ternary, ..., qary, ... operations on the alphabet A (i.e. the set of "symbols" used) are arithmetic. So are such operations on the group P of symbol positions, on the group K of keys, on the group A^P of messages, or on the group $K \times A^P$. A particularly important type of arithmetic is a unary operation on A^P, i.e. a map

$$r : A^P \rightarrow A^P.$$

Definition 2.4: Let A and P be groups. We call A^P the group of messages. A replacement on A^P is a unary operation on A^P, i.e. a map

$$r : A^P \rightarrow A^P.$$

Definition 2.5: Let G be a group. The following objects are arithmetic on G:

nullary operations	$\hat{n} : \{\phi\} \to G$
unary operations	$\hat{u} : G \to G$
binary operations	$\hat{b} : G \times G \to G$
ternary operations	$\hat{y} : G \times G \times G \to G$
$\vdots$	
qary operations	$\hat{q} : G \times G \times \ldots \times G \to G.$

In this way we have defined arithmetic on the following structures related to a cryptosystem:

the group P of symbol positions;

the group A of symbols (the alphabet);

the group K of keys;

the group A^P of messages;

the group $K \times A^P$.

Usually arithmetic on A^P is induced by arithmetic on A, or arithmetic on P, or both. For example, if $b, c \in A^P$ then we have

$$b : P \to A$$

$$c : P \to A\ .$$

Let $\nabla : A \times A \to A$ be a binary operation on A. Then ∇ induces a natural binary operation (which, by the usual abuse of notation, we will also call ∇) on A^P. We define $\nabla : A^P \times A^P \to A^P$ by subjecting

$$b \nabla c : P \to A$$

to the requirement that

$$(b \nabla c)(p) = b(p) \nabla c(p)$$

for every $p \in P$. If A is a field then A^P is a vector space over A. Its dimensionality is the cardinality of P.

Since a replacement is a unary operation on A^P, it follows that the notion of replacement is logically superfluous, being a special case of arithmetic on A^P. But we will nevertheless use the "replacement" terminology because this particular special case arises so often, and corresponds to the classical cryptographic notion of codebook.

There are a lot of groups K, A, P. So there are a lot of matrices

$$c : K \times A^P \to K \times A^P$$

The thesis this paper presents is to the effect that people who build cryptosystems always gravitate toward those matrices c which arise simply and naturally out of just confusion on A^P, diffusion on A^P, and arithmetic on A, on P, and on A^P. This often means they must forcibly relate K to A, or even to A and P in some, not always natural, manner.

An analogy to the thesis we present might be Cayley's theorem: If you want to understand groups, it suffices to understand permutations. There is probably no "Cayley theorem" to the effect that, if you want to understand cryptosystems, it suffices to look at confusion/diffusion/arithmetic cryptosystems. But our "Cayley thesis" (to the effect that people have never departed from the confusion/diffusion/arithmetic methodology so far in building cryptosystems) can have uses. If it is false, what is a historical counterexample? If it is true, why do people tend to do this? Either way, it is now possible to produce numerous useful cryptosystems using the confusion/diffusion/arithmetic methodology. It should be possible to exploit it to produce a taxonomy of cryptosystems. Will such a taxonomy be useful to cryptanalysts? To cryptosystem designers? Can we produce novel useful cryptosystems which are not confusion/diffusion/arithmetic cryptosystems?

3. An overview of DES as a confusion/diffusion/arithmetic cryptosystem

The highly structured DES is a good example of how the confusion/ diffusion/ arithmetic approach to cryptosystem structure works. Recall that arithmetic includes replacement (a unary operation on the message group A^P). It also includes constants (nullary operations) and binary operations on the collection K of keys, on the domain P of the collection of messages, on the codomain A of the collection of messages, on the collection A^P of messages itself (though this last is usually induced by a related operation on the codomain A), and on the cartesian product $K \times A^P$ of the key collection with the message collection.

The standard descriptions [BE82, pp. 267-285; DE82, pp. 91-97; KO81, pp. 240-249; ME82, pp. 141-165] of DES describe its underlying structure in a hybrid terminology which mixes mathematical, mechanical and electrical metaphors. Moreover, though the descriptions in [BE82; DE82; KO81; ME82] are logically equivalent, they are not the same in detail. In particular it is commonplace to index rows and columns of S-boxes by the set $Z/16Z = \{0, 1, 2, \dots , 14, 15\}$. But Konheim goes on to use 0 as the index of the first element of every set he encounters, whereas Denning often uses 1 as the index of the first member of a set. We invariably follow Konheim's [KO81] usage herein.

Our description will be written in a top-down fashion. This section will give a brief unmotivated overview of how to describe DES in confusion/diffusion/arithmetic terms. Sections 4-9 will then go into the details. Our indebtedness to [DA84] should become obvious. We start by defining the notion of toroidal matrix. A matrix over a ring R is, of course, a function

$$M : B \times C \to R$$

whose domain is a cartesian product, $B \times C$ and whose codomain is the ring R. If both B and C are cyclic groups one thinks intuitively geometrically of the matrix M as an array of numbers written on a bagel, rather than as a bunch of numbers written in a rectangle. This attitude is very natural and helpful in following our description of DES below. Consequently we will often use the phrase "toroidal matrix" to direct the reader's attention to the fact that the cartesian factors B and C of the index set $B \times C$ of M are both cyclic groups whose cyclic structure is explicitly or implicitly used in constructing or manipulating M.

We will adopt the abbreviation

$$\Delta = (Z/2Z)^{[(Z/96Z)\times(Z/2Z)]}$$

for the vector space of all 96 by 2 toroidal matrices with entries belonging to the field $Z/2Z$, as well as the abbreviation

$$D = (Z/96Z) \times (Z/2Z)$$

for the index set of these matrices. Thus we have

$$\Delta = (Z/2Z)^D .$$

The description of DES starts with a plaintext message block

$$\overline{m} : Z/64Z \to Z/2Z$$

i.e. a 64-bit word, and a key

$$\overline{k} : Z/64Z \to Z/2Z$$

i.e. another 64-bit word. This latter word is formed in such a manner [DE82, p. 96] that the values of $\overline{k}$ on the set

$$X = (Z/64Z) \cap (7 + 8Z) = \{7, 15, 23, 31, 39, 47, 55, 63\}$$

are determined by its values on the rest of $Z/64Z$.

Use the initial permutation [DE82, pp. 91-97; KO81, pp. 240-249; ME82, p. 155-160] IP and the bit-selection table [DE82, pp. 92-94; KO81, pp. 241-242; ME82, pp. 156-160] E to form a modified message

$$m : Z/96Z \times Z/2Z \to Z/2Z$$

i.e. a member of the set Δ of toroidal 96 by 2 matrices of zeros and ones.

The modified message m (which we will call a DES internal message) is formed from $\overline{m}$ by means of a pure diffusion operation

$$\pi : D \to Z/64Z,$$

followed by multiplication by a constant matrix $w \in \Delta$, so that

$$m = w * (\overline{m} \circ \pi).$$

The transition from $\overline{m}$ to m by means of the initial message diffusion π and the constant matrix w is key-independent and has no secrecy aspect. In other words $\overline{m}$ may be secret but does not depend on $\overline{k}$. But π is neither secret nor dependent on $\overline{m}$ or $\overline{k}$. The surjection π is naturally associated with a certain 64 dimensional vector subspace Π of the 192 dimensional vector space Δ.

The map π is a surjection but not an injection. Therefore [MA67, p. 9] it has no left inverse function but has many right inverse functions. Using the IP^{-1} map [DE82, p. 92] we can easily fix upon a distinguished member of this set of right inverses, call it π^{-1}, which faithfully represents the map IP^{-1}, and which correctly reformats messages after the sixteen round operation of DES.

Independently of all this initial reformatting of the plaintext message $\overline{m}$ so as to produce m, use the permuted choices (or so-called key permutations) [DE82, pp. 96-97; KO81, pp. 245-247; ME82, pp. 153-160] PC-1 and PC-2 in conjunction with the key schedule of left shifts [DE82, pp. 96-97; KO81, pp. 245-247; ME82, pp. 153-160] to turn the key $\overline{k}$ into a modified key

$$k : Z/16Z \to \Delta\,,$$

i.e. a list $(k[0], k[1], \ldots, k[15])$ of sixteen 96 by 2 toroidal matrices This modified key k (which we will call a DES internal key) is formed from (the external key) $\overline{k}$ by means of sixteen pure diffusion operations

$$\phi[i] : Z/96Z \times Z/2Z \to Z/64Z,$$

$i \in Z/16Z$, and a constant matrix $v \in \Delta$ so that

$$k[i] = v * (\overline{k} \circ \phi[i])$$

We thus write k as a list

$$\begin{aligned} k &= (k[0],\, k[1],\, \ldots,\, k[15]) \\ &= (v * (\overline{k} \circ \phi[0]),\, v * (\overline{k} \circ \phi[1]),\, \ldots,\, v * (\overline{k} \circ \phi[15])) \end{aligned}$$

of sixteen members of Δ. The sixteen functions $\phi[0], \phi[1], \ldots, \phi[15]$ are all naturally associated with a certain 48 dimensional vector subspace Φ of Δ.

The transition from $\overline{k}$ to k by means of the initial key diffusion $\phi[i]$ and the constant matrix v has no secrecy aspect. In other words $\overline{k}$ may be secret, but does not depend on $\overline{m}$. Moreover none of $v, \phi[0], \phi[1], \ldots, \phi[15]$ are either secret or dependent on $\overline{m}$ or $\overline{k}$.

At this point we have $m \in \Delta$ and $k \in \Delta^{Z/16Z}$. With these seventeen 96 by 2 toroidal matrices of zeros and ones at our disposal we can describe the 16-round internal structure of DES very simply. Note that everything done so far is possible without performing any rounds of the DES. It depends only on the message block $\overline{m}$ and the key $\overline{k}$.

The round [DE82, pp. 92-96; KO81, pp. 240-248; ME82, pp. 141-142, 156-160] in DES is a map

$$\rho : \Phi \times \Pi \to \Pi$$

with the property that the restriction $\rho|_f$ of ρ to $\{f\} \times \Pi$ is (well, amounts to, in the obvious fashion) a permutation of Π for every matrix $f \in \Phi$. We can say, if we choose, that the round ρ of DES is a family

$$\rho = \{\rho\big|_f : f \in \Phi\}$$

of replacements of Π.

The round ρ can be further analyzed. In fact,

$$\rho(x, y) = u * (y \circ \alpha) + (\sigma(x + v * y)) \circ \alpha$$

for every $x, y \in \Delta$. Here the plus sign $+$ denotes the natural vector space addition on the vector space Δ. Just add entrywise modulo 2. The times sign $*$ denotes entrywise multiplication (not matrix multiplication) of 96 by 2 toroidal matrices. The map

$$\sigma : \Delta \to \Delta$$

is a replacement corresponding to the action of the S-boxes [DE82, pp. 92-96; KO81, pp. 243-244]. The range Σ of σ is a 64 dimensional vector subspace of the 192 dimensional vector space Δ. The map

$$\alpha : D \to D$$

is a diffusions, i.e. is a self-map of the 192-element set D of ordered pairs which constitutes the domain of a modified message $m \in \Delta$. The matrix $u \in \Delta$ is a constant.

Note, at this point, that this description of DES does not speak of 16 rounds. There is just the round ρ. The round ρ is done sixteen times in succession with (presumably) different input pairs. But it is just one map, not a list of 16 maps. It has no secrecy aspect. It does not depend on $\overline{m}$ or $\overline{k}$. The action of DES in the key-setting $\overline{k}$ on the message $\overline{m}$ is thus

$$[\rho(k[15], \rho(k[14], \rho(\ldots, \rho(k[2], \rho(k[1], \rho(k[0], v*(\overline{m}\circ\pi)))) \ldots)))] \circ \pi^{-1}$$

where $v \in \Delta$ is a constant and

$$\rho(x, y) = u * (y \circ \alpha) + (\sigma(x + v * y)) \circ \alpha.$$

Let us make this more explicit. Start with three fixed 96 by 2 toroidal matrices

$$u : D \to Z/2Z$$

$$v : D \to Z/2Z$$

$$w : D \to Z/2Z$$

These three fixed members of Δ can be viewed as nullary operations on Δ. There is one fixed replacement

$$\sigma : \Delta \to \Delta.$$

It can be viewed as a unary operation on Δ. There are two fixed binary operations on Δ, namely

$$+ : \Delta \times \Delta \to \Delta$$

$$* : \Delta \times \Delta \to \Delta$$

Гhere are seventeen fixed initial diffusions

$$\pi : D \to Z/64Z$$

$$\phi[0] : D \to Z/64Z$$

$$\phi[1] : D \to Z/64Z$$

$$\vdots$$

$$\phi[15] : D \to Z/64Z$$

There is one fixed terminal diffusion

$$\pi^{-1} : Z/64Z \to D.$$

Note that the injection π^{-1} is one of the many right inverses of the surjection π. There are no left inverses of π. There is an internal diffusion

$$\alpha : D \to D$$

which takes place internal to the round. There are no confusions, i.e. no selfmaps of the alphabet $Z/2Z$ which are composed on the left of any symbols such as k, $\overline{k}$, m, $\overline{m}$, u, v, w or σ. We shall see, later that the diffusion α makes use of selfmaps of $Z/2Z$. However the $Z/2Z$ this self-map acts on is not the alphabet, but rather the second cartesian factor in the cartesian product

$$Z/96Z \times Z/2Z = D.$$

which constitutes the domain, not the codomain of a message. Hence these latter selfmaps are diffusions, not confusions.

To employ the $\overline{k}$ key-setting of DES on the plaintext message $\overline{m}$, one proceeds as follows to build a list of 17 members of Δ, followed by one member of $Z/2Z^{Z/64Z}$:

$$\begin{aligned}
q[0] &= w * (\overline{m} \circ \pi);\\
q[1] &= u * (q[0] \circ \alpha) + (\sigma(\overline{k} \circ \phi[0] + v * q[0])) \circ \alpha;\\
q[2] &= u * (q[1] \circ \alpha) + (\sigma(\overline{k} \circ \phi[1] + v * q[1])) \circ \alpha;\\
&\vdots\\
q[14] &= u * (q[13] \circ \alpha) + (\sigma(\overline{k} \circ \phi[13] + v * q[13])) \circ \alpha;\\
q[15] &= u * (q[14] \circ \alpha) + (\sigma(\overline{k} \circ \phi[14] + v * q[14])) \circ \alpha;\\
q[16] &= u * (q[15] \circ \alpha) + (\sigma(\overline{k} \circ \phi[15] + v * q[15])) \circ \alpha\\
\overline{y} &= q[16] \circ \pi^{-1}.
\end{aligned}$$

4. The initial permutation IP and its inverse

Permutations will be written as products of disjoint cycles. For example

$$\beta = (1,5,2,3)(4,6)(7) = (7)(4,6)(5,2,3,1)$$

is the function β such that: $\beta(1) = 5$; $\beta(2) = 3$; $\beta(3) = 1$; $\beta(4) = 6$; $\beta(5) = 2$; $\beta(6) = 4$; $\beta(7) = 7$;

The initial permutation IP [DE82, p. 92] can be factored [DA84, p. 190] into disjoint cycles of lengths 1,2,3 and 6 in the following fashion.

$$IP = \prod U[j],$$

where the product is over $j \in \{0, 1, 2, 3, 4, 5, 6, 8, 10, 11, 13, 18, 21, 42\}$, and

$$
\begin{aligned}
U[0] &= (0, 57, 54, 12, 27, 39)\\
U[1] &= (1, 49, 52, 28, 31, 7)\\
U[2] &= (2, 41, 50, 44, 26, 47)\\
U[3] &= (3, 33, 48, 60, 30, 15)\\
U[4] &= (4, 25, 55)\\
U[5] &= (5, 17, 53, 20, 29, 23)\\
U[6] &= (6, 9, 51, 36, 24, 63)\\
U[8] &= (8, 59, 38)\\
U[10] &= (10, 43, 34, 40, 58, 46)\\
U[11] &= (11, 35, 32, 56, 62, 14)\\
U[13] &= (13, 19, 37, 16, 61, 22)\\
U[18] &= (18, 45)\\
U[21] &= (21)\\
U[42] &= (42)\,.
\end{aligned}
$$

[DA84, pp. 189-191] contains a very complete discussion of IP from a variety of viewpoints and we will not consider it further, other than to note that (4), (5) and (7) in [DA84, p. 190] all express IP and IP^{-1} in various ways in terms of $Z/2Z$ arithmetic, the group SYM$(Z/6Z)$ of symmetries of a 6-member set, and $GF(64)$

arithmetic.

5. The initial diffusions which turn a 64-bit plaintext message block $\overline{m}$ into a DES internal message m.

Let

$$\begin{aligned}
A &= [Z/96Z] \cap [(1+3Z) \cup (0+12Z) \cup (11+12Z)] \\
&= \{0,1,4,7,10,11,12,13,16,19,22,23,24,25,28,\ldots, \\
&\qquad 67,70,71,72,73,76,79,82,83,84,85,88,91,94,95\} \\
D &= Z/96Z \times Z/2Z \\
Q &= A \times Z/2Z \\
G &= A \times \{0\} \\
F &= A \times \{1\} \\
L &= [(Z/96Z) \cap (1+3Z)] \times \{1\} \\
X &= (Z/64Z) \cap (1+3Z)] \times \{1\}\,.
\end{aligned}$$

Then, clearly,

$$\begin{aligned}
\text{cardinality } (A) &= 32+8+8 = 48 \\
\text{cardinality } (D) &= 96 * 2 = 192 \\
\text{cardinality } (Q) &= 48 * 2 = 96 \\
\text{cardinality } (G) &= 48 * 1 = 48 \\
\text{cardinality } (F) &= 48 * 1 = 48 \\
\text{cardinality } (L) &= 32 * 1 = 32\,.
\end{aligned}$$

We define $\nu : F \longrightarrow L$ by setting

$$\nu(f) = f \quad \text{if } f \in F$$

$$\nu((12t, 1)) = (12t - 2, 1)$$

$$\nu((12t - 1, 1)) = (12t + 1, 1)$$

if $t \in Z/8Z$. See Table 5.1 below.

It is evident that ν is a 3 to 2 surjection. We define several vector spaces over the field $GF(2) = Z/2Z$. Let

$$\Delta = (Z/2Z)^{D}$$

$$\Pi = \{d \in \Delta : d(i, j) = 0 \quad \text{if } i \notin A\}$$

$$\Gamma = \{q \in \Pi : q(i, j) = 0 \quad \text{if } j \neq 0\}$$

$$\Phi = \{q \in \Pi : q(i, j) = 0 \quad \text{if } j \neq 1\}$$

Thus Π is the vector subspace of Δ consisting of all 96 by 2 toroidal matrices whose support is Q. Similarly Γ is the vector subspace of Π consisting of matrices supported on $A \times \{0\}$, and Φ consists of all matrices supported on $A \times \{1\}$. Also we need

$$\hat{\Pi} = \{q \in \Pi : q(12t - 2, j) = q(12t, j) \quad \text{and}$$

$$q(12t - 1, j) = q(12t + 1, j) \text{ for every } t \in Z, \text{ every } j \in Z\}$$

$$\hat{\Gamma} = \hat{\Pi} \cap \Gamma$$

$$\hat{\Phi} = \hat{\Pi} \cap \Phi \, .$$

Clearly we have $\Pi = \Gamma \ominus \Phi$ and $\hat{\Pi} = \hat{\Gamma} \oplus \hat{\Phi}$. Table 5.2 below describes dimensionalities and subspace relationships among these 7 vector spaces.

We also need the masks w, u and v which turn members of Δ into members of Π, Γ and Φ respectively. The vector $w \in \Pi$ has as many entries equal to 1 as a member of Π can have, i.e.

$$\begin{aligned} w(i,j) &= 1 \quad \text{if } (i,j) \in A \times Z/2Z \\ &= 0 \quad \text{otherwise} \end{aligned}$$

Similarly $u \in \Gamma$,

$$\begin{aligned} u(i,j) &= 1 \quad \text{if } (i,j) \in A \times \{0\} \\ &= 0 \quad \text{otherwise} \end{aligned}$$

and $v \in \Phi$,

$$\begin{aligned} v(i,j) &= 1 \quad \text{if } (i,j) \in A \times \{1\} \\ &= 0 \quad \text{otherwise} \end{aligned}$$

Evidently

$$u * v = 0$$

$$u * w = u$$

$$v * w = v$$

$$u + v = w$$

Also, for any $d \in \Delta$ we have

$$u * d = d * u \in \Gamma$$

$$v * d = d * v \in \Phi$$

$$w * d = d * w \in \Pi$$

We will set up a bijection between $\hat{\Pi}$ and the space of all 64-bit plaintext DES words. Then we will proceed in the spirit of [DA84] and do all further DES operations in Π. The larger vector space Δ arises naturally from an attempt to make the data expansion effected by the bit selection [DE82, p. 93] table E and the workings of the DES round more simple.

The initial [KO81, pp. 240-242] permutation IP and the bit-selection [DE82, pp. 93-94] table E are two of the diffusions used to reformat a 64-bit plaintext message block for internal use by DES. In the treatment below it will be part of the conversion of a plaintext message block

$$\overline{m} \in (Z/2Z)^{Z/64Z}$$

into an internal DES message $m \in \Delta$. Tables 5.3 and 5.4 below give the values of γ, $\overline{\pi}$, π, $\overline{m} \circ \pi = \overline{m} \circ IP \circ \overline{\pi}$, w and $m = w * (\overline{m} \circ \pi)$. All of them are displayed as 96 by 2 toroidal matrices.

The diffusion

$$\gamma : D \to D$$

is the identity permutation of D, represented as a matrix. It is shown to give the reader a clear picture of where the $(\acute{j}, \hat{j})$th entry of each of the matrices shown is located. The diffusion

$$\pi = IP \circ \overline{\pi} : D \to Z/64Z$$

is a 3-to-1 surjection, represented as a matrix The map

$$\overline{m} \circ \pi = \overline{m} \circ IP \circ \overline{\pi} : D \to Z/2Z$$

is a member of Δ, and is represented as a matrix. The nullary operation (i.e. constant, or mask) $w \in \Delta$ is represented as a matrix.

The entrywise product

$$p = w * (\overline{m} \circ \pi) = w * (\overline{m} \circ IP \circ \overline{\pi})$$

is represented as a matrix. An entry of this matrix $w * (\overline{m} \circ \pi)$ must be zero if the corresponding entry of w is zero. Other entries of $w * (\overline{m} \circ \pi)$ can also be zero (for example the (0,0)th entry of $w * (\overline{m} \circ \pi)$ is zero if $\overline{m}(7) = 0$). Its left column consists of the entries indexed by indices of the form $(0, j) \in D$, and amounts to a 48-bit left-half word. Its right column consists of the entries indexed by pairs of the form $(1, j) \in D$, and amounts to a 48-bit right half word. There are relationships among its rows. Thus

$$\begin{gathered}
\text{row } 0 = \text{row } 94 \\
\text{row } 12 = \text{row } 10 \\
\text{row } 24 = \text{row } 22 \\
\vdots \\
\text{row } 72 = \text{row } 70 \\
\text{row } 84 = \text{row } 82
\end{gathered}$$

also

$$\begin{gathered}
\text{row } 11 = \text{row } 13 \\
\text{row } 23 = \text{row } 25
\end{gathered}$$

$$\text{row } 35 = \text{row } 37$$

$$\vdots$$

$$\text{row } 83 = \text{row } 85$$

$$\text{row } 95 = \text{row } 1$$

Hence 32 of the rows of $w * (\overline{m} \circ \pi)$ determine all its rows. See [DA84, pp. 191-192] for an arithmetical description of the bit selection table E. Our approach is similar but we spread the bits of the initial 64-bit message more uniformly through a larger array.

We note that $\overline{\pi}$ and $\pi = IP \circ \overline{\pi}$ are single matrices. But the collection

$$\{w * (\overline{m} \circ \pi) : \overline{m} \in (Z/2Z)^{Z/64Z}\}$$

is a 64 dimensional subspace of Δ.

$$\nu(0,1) = (94,1)$$

$$\nu(1,1) = (1,1)$$

$$\nu(4,1) = (4,1)$$

$$\nu(7,1) = (7,1)$$

$$\nu(10,1) = (10,1)$$

$$\nu(11,1) = (13,1)$$

$$\nu(12,1) = (10,1)$$

$$\nu(13,1) = (13,1)$$

$$\nu(16,1) = (16,1)$$

$$\nu(19,1) = (19,1)$$

$$\nu(22,1) = (22,1)$$

$$\nu(23,1) = (25,1)$$

$$\nu(24,1) = (22,1)$$

$$\nu(25,1) = (25,1)$$

$$\nu(28,1) = (28,1)$$

$$\vdots$$

$$\nu(83,1) = (85,1)$$

$$\nu(84,1) = (82,1)$$

$$\nu(85,1) = (85,1)$$

$$\nu(88,1) = (88,1)$$

$$\nu(91,1) = (91,1)$$

$$\nu(94,1) = (94,1)$$

$$\nu(95,1) = (1,1)$$

Table 5.1. The 3 to 2 surjection $\nu : F \to L$

	dimension							
	of space	Is the space at left a subspace of the						
space	at left	space below?						
Δ	192	yes						
Π	96	yes	yes					
$\hat{\Pi}$	64	yes	yes	yes				
Γ	48	yes	yes		yes			
$\hat{\Gamma}$	32	yes	yes	yes	yes	yes		
Φ	48	yes	yes				yes	
$\hat{\Phi}$	32	yes	yes	yes			yes	yes
		Δ	Π	$\hat{\Pi}$	Γ	$\hat{\Gamma}$	Φ	$\hat{\Phi}$

Table 5.2

$$\begin{array}{ccc}
\begin{bmatrix}
(0,0) & (1,0) \\
(0,1) & (1,1) \\
(0,2) & (1,2) \\
(0,3) & (1,3) \\
(0,4) & (1,4) \\
(0,5) & (1,5) \\
(0,6) & (1,6) \\
(0,7) & (1,7) \\
(0,8) & (1,8) \\
(0,9) & (1,9) \\
(0,10) & (1,10) \\
(0,11) & (1,11) \\
(0,12) & (1,12) \\
(0,13) & (1,13) \\
(0,14) & (1,14) \\
(0,15) & (1,15) \\
(0,16) & (1,16) \\
\vdots & \vdots \\
(0,81) & (1,81) \\
(0,82) & (1,82) \\
(0,83) & (1,83) \\
(0,84) & (1,84) \\
(0,85) & (1,85) \\
(0,86) & (1,86) \\
(0,87) & (1,87) \\
(0,88) & (1,88) \\
(0,89) & (1,89) \\
(0,90) & (1,90) \\
(0,91) & (1,91) \\
(0,92) & (1,92) \\
(0,93) & (1,93) \\
(0,94) & (1,94) \\
(0,95) & (1,95)
\end{bmatrix}
&
\begin{bmatrix}
31 & 63 \\
0 & 32 \\
31 & 63 \\
0 & 32 \\
1 & 33 \\
2 & 34 \\
1 & 33 \\
2 & 34 \\
1 & 33 \\
2 & 34 \\
3 & 35 \\
4 & 36 \\
3 & 35 \\
4 & 36 \\
3 & 35 \\
4 & 36 \\
5 & 37 \\
\vdots & \vdots \\
26 & 58 \\
27 & 59 \\
28 & 60 \\
27 & 61 \\
28 & 60 \\
27 & 61 \\
28 & 60 \\
29 & 61 \\
30 & 62 \\
29 & 63 \\
30 & 62 \\
29 & 63 \\
30 & 62 \\
31 & 63 \\
0 & 32
\end{bmatrix}
&
\begin{bmatrix}
7 & 6 \\
57 & 56 \\
7 & 6 \\
57 & 56 \\
49 & 48 \\
41 & 40 \\
49 & 48 \\
41 & 40 \\
49 & 48 \\
41 & 40 \\
33 & 32 \\
25 & 24 \\
33 & 32 \\
25 & 24 \\
33 & 32 \\
25 & 24 \\
17 & 16 \\
\vdots & \vdots \\
45 & 44 \\
39 & 38 \\
31 & 30 \\
39 & 38 \\
31 & 30 \\
39 & 38 \\
31 & 30 \\
23 & 22 \\
15 & 14 \\
23 & 22 \\
15 & 14 \\
23 & 22 \\
15 & 14 \\
7 & 6 \\
57 & 56
\end{bmatrix}
\\
\gamma,\ \text{the identity on } D & \overline{\pi} & \pi = IP \circ \overline{\pi}
\end{array}$$

Table 5.3

$$
\begin{array}{ccc}
\begin{bmatrix}
\overline{m}(7) & \overline{m}(6) \\
\overline{m}(57) & \overline{m}(56) \\
\overline{m}(7) & \overline{m}(6) \\
\overline{m}(57) & \overline{m}(56) \\
\overline{m}(49) & \overline{m}(48) \\
\overline{m}(41) & \overline{m}(40) \\
\overline{m}(49) & \overline{m}(48) \\
\overline{m}(41) & \overline{m}(40) \\
\overline{m}(49) & \overline{m}(48) \\
\overline{m}(41) & \overline{m}(40) \\
\overline{m}(33) & \overline{m}(32) \\
\overline{m}(25) & \overline{m}(24) \\
\overline{m}(33) & \overline{m}(32) \\
\overline{m}(25) & \overline{m}(24) \\
\overline{m}(33) & \overline{m}(32) \\
\overline{m}(25) & \overline{m}(24) \\
\overline{m}(17) & \overline{m}(16) \\
\vdots & \vdots \\
\overline{m}(45) & \overline{m}(44) \\
\overline{m}(39) & \overline{m}(38) \\
\overline{m}(31) & \overline{m}(30) \\
\overline{m}(39) & \overline{m}(38) \\
\overline{m}(31) & \overline{m}(30) \\
\overline{m}(39) & \overline{m}(38) \\
\overline{m}(31) & \overline{m}(30) \\
\overline{m}(23) & \overline{m}(22) \\
\overline{m}(15) & \overline{m}(14) \\
\overline{m}(23) & \overline{m}(22) \\
\overline{m}(15) & \overline{m}(14) \\
\overline{m}(23) & \overline{m}(22) \\
\overline{m}(15) & \overline{m}(14) \\
\overline{m}(7) & \overline{m}(6) \\
\overline{m}(57) & \overline{m}(56)
\end{bmatrix}
&
\begin{bmatrix}
1 & 1 \\
1 & 1 \\
0 & 0 \\
0 & 0 \\
1 & 1 \\
0 & 0 \\
0 & 0 \\
1 & 1 \\
0 & 0 \\
0 & 0 \\
1 & 1 \\
1 & 1 \\
1 & 1 \\
1 & 1 \\
0 & 0 \\
0 & 0 \\
1 & 1 \\
\vdots & \vdots \\
0 & 0 \\
1 & 1 \\
1 & 1 \\
1 & 1 \\
1 & 1 \\
0 & 0 \\
0 & 0 \\
1 & 1 \\
0 & 0 \\
0 & 0 \\
1 & 1 \\
0 & 0 \\
0 & 0 \\
1 & 1 \\
1 & 1
\end{bmatrix}
&
\begin{bmatrix}
\overline{m}(7) & \overline{m}(6) \\
\overline{m}(57) & \overline{m}(56) \\
0 & 0 \\
0 & 0 \\
\overline{m}(49) & \overline{m}(48) \\
0 & 0 \\
0 & 0 \\
\overline{m}(41) & \overline{m}(40) \\
0 & 0 \\
0 & 0 \\
\overline{m}(33) & \overline{m}(32) \\
\overline{m}(25) & \overline{m}(24) \\
\overline{m}(33) & \overline{m}(32) \\
\overline{m}(25) & \overline{m}(24) \\
0 & 0 \\
0 & 0 \\
\overline{m}(17) & \overline{m}(16) \\
\vdots & \vdots \\
0 & 0 \\
\overline{m}(34) & \overline{m}(38) \\
\overline{m}(31) & \overline{m}(30) \\
\overline{m}(39) & \overline{m}(38) \\
\overline{m}(31) & \overline{m}(30) \\
0 & 0 \\
0 & 0 \\
\overline{m}(23) & \overline{m}(22) \\
0 & 0 \\
0 & 0 \\
\overline{m}(15) & \overline{m}(14) \\
0 & 0 \\
0 & 0 \\
\overline{m}(7) & \overline{m}(6) \\
\overline{m}(57) & \overline{m}(56)
\end{bmatrix}
\\
\overline{m} \circ \pi = \overline{m} \circ IP \circ \overline{\pi} & w & w * (\overline{m} \circ IP \circ \overline{\pi})
\end{array}
$$

Table 5.4

6. The initial diffusions which turn a 64-bit external key block $\overline{k}$ into a DES list of k sixteen internal keys.

The permuted [KO81, pp. 245-247] choices $PC-1$ and $PC-2$ are initial diffusions which will be used in this paper to help turn a 56 bit external DES key block

$$\overline{k} \subseteq (Z/2Z)^{Z/64Z}$$

into a list

$$k = (k[0], k[1], \ldots, k[15])$$

of sixteen internal DES keys belonging to the 48 dimensional vector subspace Φ of the 192 dimensional vector space Δ. We will follow [DE82, p. 96] in regarding $PC-1$ as an injection of the 56 member set $Z/64Z \setminus X$ into a 64 member set $Z/64Z$ rather than as a permutation of the 56-member set $Z/64Z \setminus X$. As always, however, we will follow [KO81] in starting our indexing with 0, rather than with 1. The table of DES key schedule shifts also plays a part in the process of converting a conventional DES key into a list of internal keys. It is necessary to perform several successive diffusions on a 64-bit DES key $\overline{k}$ followed by an (entrywise) matrix multiplication, so as to produce an "internal key", i.e. a list

$$k = (k[0], k[1], \ldots, k[15])$$

of sixteen 96 by 2 toroidal matrices which will serve as key material in the internal format of the round structure of DES. For each $i \in$

$Z/16Z$ the internal ith key entry $k[i]$ will be a member of the 48 dimensional vector subspace Φ of the 192 dimensional vector space Δ of all 96 by 2 toroidal matrices over $GF(2) = Z/2Z$.

We start, therefore, with the DES internal key

$$\overline{k} = (\overline{k}(0), \overline{k}(1), \ldots, \overline{k}(63))$$

and recall that it belongs to a 56 dimensional vector subspace of the 64 dimensional space of lists of 64 bits. This is because, as noted in Section 3, the bits $\overline{k}(7), \overline{k}(15), \ldots, \overline{k}(63)$ are parity bits, whose values are determined by the other 56 bits of $\overline{k}$, the bits indexed by members of $Z/64Z \setminus X$.

The index set, $Z/28Z \times Z/2Z$, of the set of 28 by 2 toroidal matrices is important enough to have its own name. So we define

$$J = Z/28Z \times Z/2Z\,.$$

And we recall, from Section 3,

$$D = Z/96Z \times Z/2Z\,.$$

The first diffusion applied to $\overline{k}$ is

$$\psi : J \to Z/64Z\,.$$

The diffusion ψ embodies the information contained in the permuted [DE82, p. 96] choice $PC - 1$. Once again [DA84, pp. 195-196] describes $PC - 1$ in arithmetic terms and points out its simple structure, which a reader can easily discover in ψ. The diffusion ψ turns $\overline{k}$ into a 28 by 2 toroidal matrix $\overline{k} \circ \psi$ over $Z/2Z$.

Then we have a list

$$\lambda = (\lambda[0], \lambda[1], \ldots, \lambda[15])$$

of diffusions

$$\lambda[i] : J \to J$$

each of which replaces this 28 by 2 toroidal matrix $\overline{k} \circ \psi$ by a "left-shifted" version of itself (a phrase more faithful to the matrix picture would be "Ferris-wheeled") induced by the key schedule [DE82, p.96] of left shifts LS. The index set for the list λ is, of course, $Z/16Z$.

Once the 16 member list

$$(\overline{k} \circ \psi \circ \lambda[0], \overline{k} \circ \psi \circ \lambda[1], \ldots, \overline{k} \circ \psi \circ \lambda[15])$$

of 28 by 2 toroidal matrices over $Z/2Z$ has been constructed it is necessary to use a last key diffusion

$$\varsigma : D \to J$$

to produce a list

$$(\overline{k} \circ \psi \circ \lambda[0] \circ \varsigma, \overline{k} \circ \psi \circ \lambda[1] \circ \varsigma, \ldots, \overline{k} \circ \psi \circ \lambda[15] \circ \varsigma)$$

of sixteen 96 by 2 toroidal matrices over $Z/2Z$. This diffusion ς embodies all the information contained in the key [DE82, p. 97] permutation $PC - 2$. Finally we must multiply (entrywise) each of these matrices by a "mask" matrix v which is zero in 144 of its entries, and has the value one only in those 48 entries corresponding to the 48 inputs to the S-boxes [DE82, pp. 92-97]. The matrix w is the nullary operation (mask) defined in Section 5. At this point we give the explicit characterizations of ψ, λ and ς. The toroidal matrices $\psi \in (Z/64Z)^J$ and $\varsigma \in J^D$ are shown in Figure 6.1. We have deliberately left three fourths of the entries of ς unevaluated (denoted by the sharp symbol #). Any one of them can have any value in J the reader desires (such flexibility may lead to some simplification). This is because a mask v will be multiplied by the matrix we are building and will leave only zeros in these places in

$$k[i] = v * (\overline{k} \circ \psi \circ \lambda[i] \circ \varsigma) = v * (\overline{k} \circ \psi[i]) \in \Phi \subseteq \Delta$$

anyway.

For each $i \in Z/16Z$ the diffusion

$$\lambda[i] : J \to J$$

is defined by setting

$$\lambda[i](a, b) = (a + \ell(i), b)\,,$$

where the 16-entry list ℓ of positive integers is given by

$$\begin{aligned}\ell &= (\ell(0), \ell(1), \ldots, \ell(15)) \\ &= (1, 2, 4, 6, 8, 10, 12, 14, 15, 17, 19, 21, 23, 25, 27, 28).\end{aligned}$$

These successive positive integers are just the successive partial sums of the numbers of left shift positions in [DE82, p. 96]. Note that after 16 rounds the 28 by 2 toroidal matrix $k \circ \psi$ has been rolled all the way around to its original position, so that no reset is needed before encrypting the next DES message $\overline{\overline{m}}$ in the same key $\overline{k}$. Note the sum, $a + \ell(i)$, above. To show that it would be wrong to use the difference, $a - \ell(i)$, we will work out Example 6.1 below. Now it merely remains to multiply by the mask $v \in \Phi$ so as to zero out the whole left column (the entries with second index 0) as well as half of the right column of $\overline{k} \circ \psi \circ \lambda[i] \circ \varsigma$. We thus have

$$\begin{aligned}k[i] &= v * (\overline{k} \circ \psi \circ \lambda[i] \circ \varsigma) \\ &= v * (\overline{k} \circ \phi[i]) .\end{aligned}$$

Example 6.1: To verify that these diffusions actually faithfully represent the key schedule of DES let us follow k_8, k_{44} and k_{29} in Konheim's [KO81, p. 247] notation. Because we have kept the parity bits in positions 7 modulo 8 we have the correspondence

$$\begin{aligned}k_8 &= \overline{k}(9), \\ k_{29} &= \overline{k}(33), \\ k_{44} &= \overline{k}(50).\end{aligned}$$

We verify that

$$\psi((14,0))) = 9$$

$$\psi((17,0)) = 50$$

$$\psi((11,0)) = 33$$

and that

$$\lambda[1]((13,0)) = (14,0)$$

$$\lambda[1]((16,0)) = (17,0)$$

$$\lambda[1]((10,0)) = (11,0)$$

and that

$$\varsigma((0,0)) = (13,0)$$

$$\varsigma((1,0)) = (16,0)$$

$$\varsigma((4,0)) = (10,0)$$

Hence

$$\begin{aligned}\overline{k} \circ \psi \circ \lambda[1] \circ \varsigma)((0,0)) &= \overline{k}(\psi(\lambda[1](\varsigma((0,0))))) \\ &= \overline{k}(\psi(\lambda[1]((13,0)))) \\ &= \overline{k}(\psi((14,0))) \\ &= \overline{k}(9) \\ &= k_8\end{aligned}$$

and

$$\begin{aligned}(\overline{k} \circ \psi \circ \lambda[1] \circ \varsigma)((0,0)) &= \overline{k}(\psi(\lambda[1](\varsigma((1,0))))) \\ &= \overline{k}(\psi(\lambda[1]((16,0)))) \\ &= \overline{k}(\psi((17,0))) \\ &= \overline{k}(50) \\ &= k_{44}\end{aligned}$$

and

$$
\begin{aligned}
(\overline{k} \circ \psi \circ \lambda[1] \circ \varsigma)((4,0)) &= \overline{k}(\psi(\lambda[1](\varsigma((4,0))))) \\
&= \overline{k}(\psi(\lambda[1]((10,0)))) \\
&= \overline{k}(\psi((11,0))) \\
&= \overline{k}(33) \\
&= k_{29}
\end{aligned}
$$

And this, of course, is what can be found in [KO81, p. 247] as the beginning of the key used in the first round of DES.

$$\begin{bmatrix} 56 & 62 \\ 48 & 54 \\ 40 & 46 \\ 32 & 38 \\ 24 & 30 \\ 16 & 22 \\ 8 & 14 \\ 0 & 6 \\ 57 & 61 \\ 49 & 53 \\ 41 & 45 \\ 33 & 37 \\ 25 & 29 \\ 17 & 21 \\ 9 & 13 \\ 1 & 5 \\ 58 & 60 \\ 50 & 52 \\ 42 & 44 \\ 34 & 36 \\ 26 & 28 \\ 18 & 20 \\ 10 & 12 \\ 2 & 4 \\ 59 & 27 \\ 51 & 19 \\ 43 & 11 \\ 35 & 3 \end{bmatrix}$$

$$\psi$$

Figure 6.1

$$
\left\lceil\begin{array}{cc}
\# & (13,1) \\
\# & (16,1) \\
\# & \# \\
\# & \# \\
\# & (10,1) \\
\# & \# \\
\# & \# \\
\# & (23,1) \\
\# & \# \\
\# & \# \\
\# & (0,1) \\
\# & (4,1) \\
\# & (2,1) \\
\# & (27,1) \\
\# & \# \\
\# & \# \\
\# & (14,1) \\
\# & \# \\
\# & \# \\
\# & (5,1) \\
\# & \# \\
\# & \# \\
\# & (20,1) \\
\# & (9,1) \\
\# & (22,1) \\
\# & (18,1) \\
\# & \# \\
\# & \# \\
\# & (11,1) \\
\# & \# \\
\# & \# \\
\# & (3,1) \\
 & \vdots
\end{array}\right\rceil
\quad
\left|\begin{array}{cc}
 & \vdots \\
\# & \# \\
\# & \# \\
\# & (25,1) \\
\# & (7,1) \\
\# & (15,1) \\
\# & (6,1) \\
\# & \# \\
\# & \# \\
\# & (26,1) \\
\# & \# \\
\# & \# \\
\# & (19,1) \\
\# & \# \\
\# & \# \\
\# & (12,1) \\
\# & (1,1) \\
\# & (12,1) \\
\# & (23,1) \\
\# & \# \\
\# & \# \\
\# & (2,1) \\
\# & \# \\
\# & \# \\
\# & (8,1) \\
\# & \# \\
\# & \# \\
\# & (18,1) \\
\# & (26,1) \\
\# & (1,1) \\
\# & (11,1) \\
\# & \# \\
\# & \# \\
 & \vdots
\end{array}\right|
\quad
\left\lfloor\begin{array}{cc}
 & \vdots \\
\# & (22,1) \\
\# & \# \\
\# & \# \\
\# & (16,1) \\
\# & \# \\
\# & \# \\
\# & (4,1) \\
\# & (19,1) \\
\# & (15,1) \\
\# & (20,1) \\
\# & \# \\
\# & \# \\
\# & (10,1) \\
\# & \# \\
\# & \# \\
\# & (27,1) \\
\# & \# \\
\# & \# \\
\# & (5,1) \\
\# & (24,1) \\
\# & (17,1) \\
\# & (13,1) \\
\# & \# \\
\# & \# \\
\# & (21,1) \\
\# & \# \\
\# & \# \\
\# & (7,1) \\
\# & \# \\
\# & \# \\
\# & (0,1) \\
\# & (3,1)
\end{array}\right\rfloor
$$

Figure 6.2

The top,middle, and bottom thirds

of the 96 by 2 toroidal matrix ς

7. The DES round ρ, in which an internal key k interacts with an internal message m.

The DES wire-crossing [DE82, p. 93; KO81, p. 245] P and the selection [DE82, p. 94] functions, i.e. S-boxes [KO81, p. 244] are used in each of the sixteen actions of the DES round. We now see that an internal message m and an entry $k[i]$ of an internal key list k are members of Δ. In fact

$$m \in \hat{\Pi} \subseteq \Pi \subseteq \Delta$$

$$k[i] \in \Phi \subseteq \Pi \subseteq \Delta\,.$$

The round ρ of DES proceeds as follows. The mask v is such that

$$v * m \in \hat{\Phi} \subseteq \Phi\,.$$

Hence

$$v * m + k[i] \in \Phi\,.$$

This vector $v * m + k[i]$ is input to the replacement σ corresponding to the S-boxes [KO91, p. 244] and, after wire crossing [KO81, p. 245] and masking, comes out as a member δ of $\hat{\Gamma}$. Meanwhile $u * m$ (a member of $\hat{\Gamma}$) is diffused by a column interchange to produce a member $\overline{\delta}$ of $\hat{\Phi}$. The matrix

$$\delta \oplus \overline{\delta} \in \hat{\Pi} = \hat{\Gamma} \oplus \hat{\Phi}$$

is the result of the round ρ.

We now carry out this process in detail.

In detail the process is as follows. Before the first action of the round ρ there is an initial internal message $m \in \Pi$. Clearly, then the (entrywise) product satisfies

$$v * m \in \Phi.$$

Also there is an entry $k[0]$ of the internal key k. It satisfies

$$k[0] \in \Phi\,.$$

Consequently their (entrywise) sum also belongs to the 48 dimensional vector space Φ, i.e.

$$v * m + k[0] \in \Phi\,.$$

We have a choice as to how we view the action of the S-boxes in the context of Δ. We can regard this action as a replacement of Δ (i.e. as a function with domain and codomain both equal to Δ) which is independent of 144 of the 192 entries of a matrix

$$v * m + k[0] = y \in \Delta\,.$$

We can also regard it as a function from Φ to Φ, to be followed by a diffusion corresponding to wire crossing and interchange of right half and left half words. This latter approach seems more in keeping with the standard descriptions of DES and we will adopt it.

So we will start by writing

$$\Phi = \Phi[0] \oplus \Phi[1] \oplus \ldots \oplus \Phi[7]$$
$$\hat{\Phi} = \hat{\Phi}[0] \oplus \hat{\Phi}[1] \oplus \ldots \oplus \hat{\Phi}[7]$$

where each $\Phi[i]$ is 6 dimensional, each $\hat{\Phi}[i]$ is a 4 dimensional subspace of $\Phi[i]$ and, in fact

$$\Phi[0] = \{t \in \Delta : t(i,j) = 0 \quad \text{unless } j = 1$$
$$\text{and } i \in \{0,1,4,7,10,11\}\}$$
$$\hat{\Phi}[0] = \{t \in \Phi[0] : t(0,1) = t(11,1) = 0\}$$

$$\Phi[1] = \{t \in \Delta : t(i,j) = 0 \quad \text{unless } j = 1$$
$$\text{and } i \in \{12,13,16,19,22,23\}\}$$
$$\hat{\Phi}[1] = \{t \in \Phi[1] : t(12,1) = t(23,1) = 0\}$$
$$\vdots$$
$$\Phi[7] = \{t \in \Delta : t(i,j) = 0 \quad \text{unless } j = 1$$
$$\text{and } i \in \{84,85,88,91,94,95\}\}$$
$$\hat{\Phi}[7] \quad = \{t \in \Delta : t(84,1) = t(95,1) = 0\}\,.$$

The first (i.e. zeroth) S-box determines a map

$$\sigma[0] : \Phi[0] \to \hat{\Phi}[0]$$

and similarly

$$\sigma[i] : \Phi[i] \to \hat{\Phi}[i]$$

for $0 \leq i \leq 7$. We will not describe these individual S-box maps any further. The nonlinear heart of DES is thus based on the map

$$\sigma[0] \oplus \sigma[1] \oplus \ldots \ominus \sigma[7] = \overline{\sigma} : \Phi \to \hat{\Phi} \subseteq \Phi$$

Evidently the unary operation $\overline{\sigma}$ is a replacement of Φ. Its working is

$$\overline{\sigma}(f) = (\sigma[0] \oplus \ldots \oplus \sigma[7])(f[0] \oplus \ldots \oplus f[7]) = \sigma[0](f[0]) \ominus \ldots \oplus \sigma[7](f[7]).$$

In other words each S-box works separately on its 6-bit input to produce its 4-bit output.

The support of $f \in \Delta$ is the 48 member set F, whereas the support of $\overline{\sigma}(f) \in \Delta$ is the 32 member subset L of F. To turn the wire crossing [DE82, p. 93; KO81, p. 245] P to a diffusion which permutes L we introduce the permutation

$$\overline{\mu} = \overline{\overline{\mu}}[0]\overline{\overline{\mu}}[1]$$

of $Z/32Z$ where

$\overline{\overline{\mu}}[0] = (0, 15, 9, 14, 30, 3, 20, 31, 24, 18, 23, 8)$

$\overline{\overline{\mu}}[1] = (1, 6, 27, 5, 11, 25, 12, 4, 28, 21, 26, 29, 10, 22, 2, 19, 13, 17, 7, 16)$

It is easy to see [DE82, p. 93; KO81, p. 245] that $\overline{\mu}$ embodies the post S-box wire crossing P and that we use it to produce the diffusion

$$\mu : D \to D$$

such that

$$\mu(1+3i,1) = (1+3\overline{\mu}(i),1)$$

if $(1+3i,1) \in L$ and

$$\mu(j,k) = (j,k)$$

if $(j,k) \notin L$. After this we need the standard diffusion which splits L so as to cover F, i.e. the map

$$\nu : F \to L$$

defined in Section 5 above.

We also need the "column interchange" (i.e. interchange of left and right half-words) diffusion

$$\alpha : D \to D$$

defined by setting

$$\alpha((i,j)) = (i,j+1)$$

since $D = Z/96Z \times Z/2Z$ the addition takes place in $Z/2Z$ and amounts to the permutation (0,1) of the set $\{0,1\}$.

The round of DES thus takes $m \in \Delta$, and splits it into $u*m \in \Gamma$ and $v*m \in \Phi$ in the sense that

$$u \in \Gamma$$

$$v \in \Phi$$

$$u * m + v * m = (u + v) * m = m \in \Delta \,.$$

Then $k[i]$ is added to $v * m$ to yield

$$k[i] + v * m \in \Phi \,.$$

The replacement $\overline{\sigma} : \Phi \to \Phi$ is then applied to yield

$$\overline{\sigma}(v * m + k[i]) \in \Phi$$

$$\overline{\sigma}(k[i] + v * m) \in \Phi \,.$$

Then the two diffusions

$$\mu : D \to D$$

$$\nu : f \to L$$

are applied to $\overline{\sigma}(k[i] + v * m)$ to yield

$$\sigma(k[i] + v * m) = (\overline{\sigma}(k[i] + v * m)) \circ \mu \circ \nu \in \Gamma$$

and α is applied to m and to $\sigma(k[i] + v * m)$ to yield

$$m \circ \alpha \in \Delta$$

$$\sigma(k[i] + v * m) \circ \alpha \in \Gamma$$

Then $m \circ \alpha$ is masked by $u \in \Phi$ to yield

$$u * (m \circ \alpha)$$

Finally, an addition produces

$$\begin{aligned} & u * (m \circ \alpha) + (\bar{\sigma}(k[i] + v * m)) \circ \mu \circ \nu \circ \alpha \\ & = u * (m \circ \alpha) + \sigma(k[i] + v * m) \circ \alpha \\ & = \rho(k[i], m) \,. \end{aligned}$$

8. The terminal diffusion π^{-1} which produces a cryptext message in 64-bit block form.

The final [DE82, p. 92] permutation IP^{-1} is one of the diffusions used to reformat an internal DES message after the sixteenth operation of the round so as to produce a correctly formatted 64-bit cryptext message block. Consider the injection

$$\pi^{-1} : Z/64Z \to D$$

defined by setting

$$\pi^{-1} = (IP^{-1}(3t+1), 0)$$

if $0 \leq t \leq 31$, and

$$\pi^{-1} = (IP^{-1}(32 + 3t + 1), 1)$$

if $32 \leq t \leq 63$. It is easy to verify that $\pi \circ \pi^{-1}$ is the identity function on $Z/64Z$.

9. Recap of DES from the confusion/diffusion/arithmetic viewpoint.

It is clear from the foregoing that DES used only diffusion and replacement, no confusion. We thus seem, on a superficial reading, to be at odds with [DA84, p. 187] when those authors speak of "a representation of the DES as a cascade of substitutions and permutations." But this surface appearance of conflict is only because they are using intuitively plausible terminology, whereas we have set confusion (hence substitution) in a rigorous context which banishes replacement (hence the action of the S-boxes) to the realm of arithmetic. This is, in turn, true because we have explicitly defined the alphabet of symbols which DES uses, namely the 2-letter alphabet

$$\{0,1\} = GF(2) = Z/2Z\,,$$

and have, consequently been forced to choose

$$P = Z/64Z$$

as the set of letter positions in a 64-bit "message". The reader can object that the alphabet could be taken as the set of all $A = (Z/2Z)^{(Z/64Z)}$ 64-bit words. But at that level DES would merely be a simple substitution cipher, and no deeper analysis would be called for. What about regarding DES words as lists of sixteen

4-bit words, i.e. choosing

$$P = Z/16Z$$

$$A = (Z/2Z)^{Z/4Z} \ ?$$

Neither we nor [DA84] have devoted any space to explicit consideration of such a formulation of the DES, though it might prove interesting.

Why didn't its designers put any confusion into DES? For one thing, the alphabet A used by DES is the field

$$A = GF(2) = Z/2Z \, .$$

Since A has only 2 members, we see that SYM(A) has only 2 members, A^A has only 4 members, and even $2^{A \times A}$ has only 16 members. A cryptosystem designer with only 16 confusion maps at his disposal doesn't have much running room and might be inclined to abandon the confusion approach for that reason. He could, however, fall back on a large family (i.e. a family determined by a large index set I)

$$f : I \to 2^{A \times A}$$

of binary relations on $A = Z/2Z$. One attractive possibility is a polyalphabetic substitution cipher in the sense made precise in [BL85, pp. 322-326].

Another reason for shunning confusion in DES could be that diffusion is cryptographically stronger, in a sense, on messages belonging to $(Z/2Z)^G$, where G is a group of reasonably large order.

Consider a known plaintext attack on a 16-alphabetic substitution cipher acting on 16 bit messages

$$m \in (Z/2Z)^{(Z/16Z)} .$$

If the cryptext version of

$$m = (1,1,1,1,1,1,1,1,0,0,0,0,0,0,0,0)$$

is m itself then all 16 alphabets have been recovered and the cryptanalyst has completely broken the cipher (i.e. has narrowed the original 2^{16} possible polyalphabetic cipher keys down to 1). But if she is dealing with a transposition cipher and finds that the above message m is encrypted as itself under the cipher, she has merely narrowed an original 16! possible cipher keys down to $(8!)^2 = 16!/12,870$ possible keys. So she has both a smaller reduction factor (12,870 vs. 65,536) and a larger remaining collection of possible keys.

The expansion of perspective in this paper from lists of 64 bits to members of the vector space Δ of 96 by 2 toroidal matrices over $Z/2Z = GF(2)$ simplified the description of the operation of the bit selection table E [DE82, p. 93; KO81, p. 242]. Further expansion of the size of the vector space beyond 192 dimensions can be used to simplify the description of key diffusions and, perhaps, S-boxes. The question is where the optimum stopping place lies. This would be a vector space within which most operations are very simple, but yet a space not too large to admit of manipulation by a cryptanalyst.

There are precedents for such an expansion of viewpoint in the success of tensor product methods in algebra and geometry. One example would be the use of multilinear maps on $R^n \times R^n \times \ldots \times R^n$ to define polynomial maps on R^n. It remains to be seen to what extent a comparable approach will benefit cryptosystem design or cryptanalysis.

By this time the general features of the confusion/diffusion arithmetic approach to cryptography begun in [BL85b] are fairly clear. In DES we see quite a lot of simple arithmetic of binary operations (e.g., group addition modulo 2 or modulo 28, monoid multiplication modulo 2) and of nullary operations (such as the constant matrices u, v and w belonging to the vector space Δ) as well as a little fancy (and expensive) arithmetic of unary operations (the map σ corresponding to the S-boxes, some expansions and wire crossing) and a lot of diffusion. Most of our diffusions were, in fact, functions. Indeed most were either injections or surjections.

We hope at this point, to have clarified for the reader all the wire crossings, tables, boxes, (so called) substitutions which are really replacements, permutations which aren't really permutations, left shifts, schedules, half words (which are merely columns of matrices), blocks.

Employment of the methodology of this paper makes it possible to exorcise lugs, pins, rotors, shift registers, grilles, squares, wheels, ... from other well-known cryptosystems. Not that these notions have served ill up to now – after all, many of them have been, or even still are, physically present and functioning in our crypto boxes, or grilles, or spools, or .... It's just that they are too many, too baroque, too far from the silicon medium and too unlike the mathematical notions which both builders and breakers employ in their work on cryptosystems. Also, of course, they have an unnecessarily finitist influence on our ways of speaking (hence thinking) about cryptography.

NSA Grant MCS 904-83-H-0002 supported this research.

10. References.

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

BL83 G. R. Blakley and Laif Swanson, Infinite structures in information theory, Advances in Cryptology: Proceedings of Crypto '82, Plenum Press (1983), pp. 39-50.

BL85a G. R. Blakley and Catherine Meadows, Security of ramp schemes, in G. R. Blakley and D. Chaum, (editors), Advances in Cryptology, Proceedings of Crypto '84, Springer-Verlag, Berlin (1985), pp. 242-268.

BL85b G. R. Blakley, Information theory without the finiteness assumption, I: Cryptosystems as group-theoretic objects, in

G. R. Blakley and D. Chaum, (editors), Advances in Cryptology, Proceedings of Crypto '84, Springer-Verlag, Berlin (1985), pp. 314-338.

BL87 G. R. Blakley and W. Rundell, A cryptosystem based on an analog of heat flow, Technical Report, September (1985).

DA84 M. Davio, Y. Desmedt, M. Fosseprez, R. Govaerts, J. Hulsbosch, P. Neutjens, P. Piret, J. -J. Quisquater, J. Vandewalle and P. Wouters, Analytical Characteristics of the DES, in Advances in Cryptology, Proceedings of Crypto '83, D. Chaum, Editor, Plenum Press, New York (1984), pp. 171-202.

DE82 D. E. R. Denning, Cryptography and Data Security, Addison-Wesley, Reading, Massachusetts (1980).

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

GR68 G. Grätzer, Universal Algebra, Van Nostrand, Princeton, New Jersey (1968).

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

HO71 K. Hoffman and R. Kunze, Linear Algebra, Second Edition, Prentice Hall, Englewood Cliffs, New Jersey (1971).

KI71 J. Killingbeck and G. H. A. Cole, Mathematical Techniques and Physical Applications, Academic Press, New York (1971).

KO56 A. N. Kolmogoroff, On the Shannon theory of information transmission in the case of continuous signals, IEEE Transactions on Information Theory, vol. IT2 (1956), pp. 102-108.

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

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

LI83 R. Lidl and H. Niederreiter, Finite Fields, Volume 20 of the Encyclopedia of Mathematics and its Applications, Addison-Wesley, Reading, Massachusetts (1983).

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

MA78 F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam (1978).

ME82 C. H. Meyer and S. M. Matyas, Cryptography: A New

Dimension in Computer Data Security, Wiley-Interscience, New York (1982).

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

NI59 H. K. Nickerson, D. C. Spencer and N. E. Steenrod, Advanced Calculus, Van Nostrand, Princeton, New Jersey (1959).

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

RO64 G. -C. Rota, On the foundations of combinatorial theory, I. The theory of Möbius functions, Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete, Vol. 2 (1964), pp. 340-368.