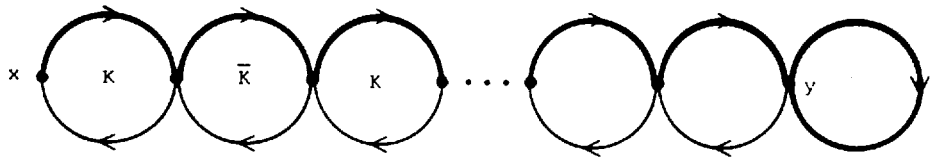
Cycle Structure of the DES with Weak and Semi-Weak Keys*

Judy H. Moore and Gustavus J. Simmons
Sandia National Laboratories
Albuquerque, NM 87185

As part of a report on cycling experiments with DES, Rivest [1] announced at Crypto'85 that a small cycle had been found when alternately encrypting with the all zeroes key and the all ones key. This cycle contained approximately 2^{33} points. Later in the same meeting, Coppersmith [2] explained this phenomenon by noting that if a fixed point occurred in the cycle, since with these keys encryption is the same as decryption, the successive encryptions would actually be decryptions and would retrace the steps to the starting point. We can picture this as follows:



where x is the starting point, y is the fixed point and K and $\bar{K}$ represent the keys used. He also argued that since there are 2^{32} such fixed points for each of these keys, the apparently small size of the cycle reported was not actually surprising. Intrigued by these observations, we began an in-depth study of the cycle structure of DES using weak and semi-weak keys. The results presented in this paper outline the current status of that study.

* This work performed at Sandia National Laboratories supported by the U. S. Dept. of Energy under contract no. DE-AC04-76DP00789.

A.M. Odlyzko (Ed.): Advances in Cryptology - CRYPTO '86, LNCS 263, pp. 9-32, 1987.

Notation

A complete description of the DES algorithm will not be given here, but since we will use a nonstandard notation, introduced by Grossman and Tuckerman [3], we begin with the specifics of that notation. Omitting the initial and final permutations, the DES transformation can be viewed as a sequence of 32-bit vectors

$$m_0, m_1, m_2, \ldots, m_{16}, m_{17}$$

defined recursively by

$$m_{i+1} = m_{i-1} \oplus f(K_i, m_i)$$

where K_i is the i^{th} round key and f is the nonlinear DES function described in the original FIPS Publication 46 [4]. The concatenation , $m_0 m_1$, represents the 64-bit input after the initial permutation, while $m_{17} m_{16}$ represents the output before the inverse of that permutation. This notation is much better suited to our purposes than the original description of the DES. For all of the work reported in this paper, the initial and final permutations are irrelevant, so we will routinely omit them.

Some details of the nonlinear function f are required for our discussion. The function takes as input a 32-bit vector X and expands it to a 48-bit vector E(X). The 48-bit round key K_i is then exclusive-ored with E(X). The resulting vector is used as input to the S-boxes, yielding a 32-bit vector. The output of f is a permuted form of this 32-bit vector. This process is shown in the following figure.

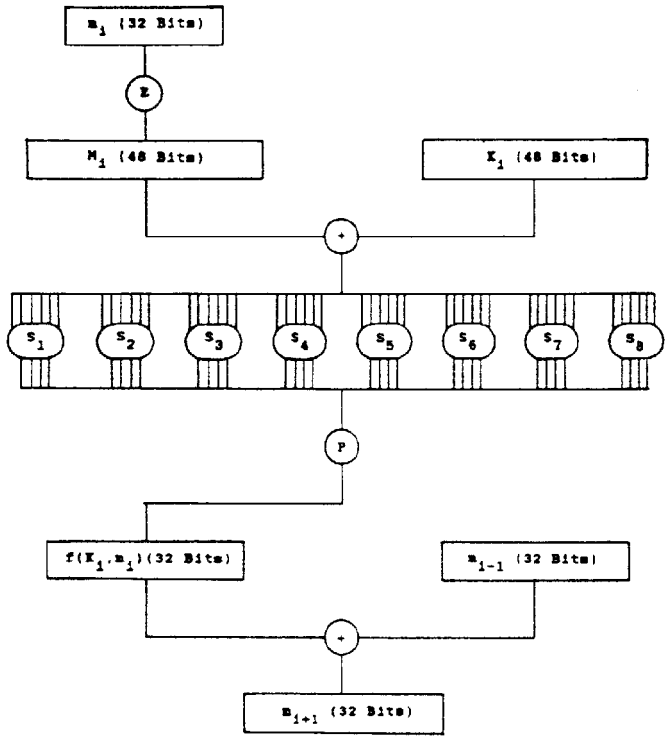


Figure 1.

The descriptions of E,P and the S-boxes can be found in FIPS Publication 46 [4]. The complete DES encryption of a 64-bit vector Y with a key K will be denoted in this paper by E(K,Y), while decryption with with K will be denoted by D(K,Y).

The Keys

We begin with a review of what is known about the weak and semi-weak keys. Davies [5] and Jueneman [6] have studied the structure of these keys and some of the results have also appeared

in FIPS Publication 74 [7]. The approach in this paper basically follows that of Moore and Simmons [8].

The keys used in this study fall into two classes. The first class, the weak keys, consists of four keys distinguished by the fact that all 16 round keys are the same. This means that decryption is identical to encryption since reversing the calling sequence for the round keys has no effect.

The second class consists of the semi-weak keys. A key K is a semi-weak key if there exists another key K^* so that the round keys for these keys satisfy $K_i^* = K_{17-i}$ for $0 < i < 17$. This property has the effect of providing "inverse keys" in the sense that decryption with K is the same as encryption with K^*.

The following theorem verifies that the weak and semi-weak keys are the only such keys having this kind of inverse keys.

Theorem 1

A DES key K has an inverse key K^* satisfying

$$K_i^* = K_{17-i}$$

if and only if K is one of the 16 keys in which all 14 of the bits in each of the four subsets A, B, C, and D of K listed below are alike.

A	(1	2	3	17	18	19	33	34	35	36	49	50	51	52)
B	(4	5	6	7	20	21	22	23	37	38	39	53	54	55)
C	(9	10	11	25	26	27	41	42	43	44	57	58	59	60)
D	(12	13	14	15	28	29	30	31	45	46	47	61	62	63)

Proof:

The proof is a tedious but straightforward bit tracing of the round keys. ∎

The sets A, B, C, and D in the previous theorem also give rise to a labeling technique for the keys used in this study. This label consists of a four-bit number, the most significant bit of which identifies the value for the bits in set A. The next bits identify the values for sets B, C and D. For example, K(3) is the key in which the bits in sets A and B are zero and the bits in sets C and D are one since the binary representation of 3 is 0011. That is,

$$K(3) = 0000000(1)\ 1111111(0)\ 0000000(1)\ 1111111(0)$$
$$0000000(1)\ 1111111(0)\ 0000000(1)\ 1111111(0)$$

The bits in parentheses are the parity bits and are set by the rule that each byte must have odd parity. The 16 keys mentioned in the previous theorem are listed below using this notation with their corresponding inverse keys identified.

K	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
K^*	0	4	8	12	1	5	9	13	2	6	10	14	3	7	11	15

The following easy lemma is a consequence of the fact that the expansion operator E is a homomorphism.

Lemma 2

For any 32-bit vectors U and M, and any 48-bit vector K,

$$f(K,M) = f(K \oplus E(U),\ M \oplus U).$$

Proof:

$$\begin{aligned} f(K \oplus E(U),\ M \oplus U) &= K \oplus E(U) \oplus E(M \oplus U) \\ &= K \oplus E(U) \oplus E(M) \oplus E(U) \\ &= K \oplus E(M) \\ &= f(K,M) \quad . \blacksquare \end{aligned}$$

The argument used to count the number of fixed points of a weak key can be captured in a more general statement in the next theorem.

Theorem 3

Suppose that for some key K, the round keys satisfy

$$K_i \oplus K_{17-i} = E(U) \quad ,$$

where E(U) is the 48-bit expansion of some 32-bit vector U. Then the following are equivalent:

1) $m_8 \oplus m_9 = U$,

2) $m_i \oplus m_{17-i} = U$, for $0 < i < 17$,

3) $m_0 \oplus m_{17} = U$ and $m_1 \oplus m_{16} = U$.

Proof:

First note that 2) => 3) and 2) => 1) are obvious. From the definition of m_j and m_{17-j+2}, we have

$$m_j \oplus m_{17-j} = m_{j-2} \oplus f(K_{j-1}, m_{j-1}) + m_{17-j+2} \oplus f(K_{17-j+1}, m_{17-j+1})$$

$$= m_{j-2} \oplus m_{17-j+2} \oplus f(K_{j-1}, m_{j-1}) \oplus f(K_{j-1} \oplus E(U), m_{17-j+1}). \quad (*)$$

For 3) => 2) the above equation yields

$$m_2 \oplus m_{15} = m_0 \oplus m_{17} \oplus f(K_1, m_1) \oplus f(K_1 \oplus E(U), m_1 \oplus U)$$

$$= m_0 \oplus m_{17}$$

$$= U \quad .$$

Then if we assume that for all $j < i$, $m_j \oplus m_{17-j} = U$, then (*) above can be used to show that $m_i \oplus m_{17-i} = U$. Thus by induction 2) is established.

For 1) => 2) we have

$$m_{10} \oplus m_7 = m_9 \oplus m_8 \oplus f(K_9, m_9) \oplus f(K_9 \oplus E(U), m_9 \oplus U) = U \quad .$$

The induction argument used above applies again to complete the proof. ∎

For the all zeroes or the all ones key, the hypothesis of Theorem 3 is satisfied for U equal to the all zeroes vector. Hence, fixed points for these keys coincide with those messages in which $m_8 = m_9$ during the encryption process. Since there are 2^{32} such possible equations, there are precisely 2^{32} fixed points for each key.

This theorem appears to be quite powerful, so the next issue is the identification of those keys which satisfy the hypothesis of the theorem.

Theorem 4

If for some key K, the round keys satisfy

$$K_i \oplus K_{17-i} = E(U) \quad ,$$

where U is the 48 bit expansion of some 32 bit vector U, then U is either the all zeroes or the all ones vector.

Proof:

The proof is again rather tedious and we refer the reader to [8] for its details.▌

This theorem states that the only keys satisfying the hypothesis of Theorem 3 are those in which the round keys either form a palindromic sequence:

$$K_i = K_{17-i} \quad , \text{ or}$$

an antipalindromic sequence

$$K_i = \bar{K}_{17-i} \quad .$$

The following theorem connects these conditions with the weak and semi-weak keys.

Theorem 5

A DES key K has a palindromic round key sequence or an antipalindromic round key sequence if and only if K is one of K(0), K(5), K(10) or K(15) in the first case or one of K(3), K(6), K(9) or K(12) in the second case.

Proof: See [8].

To end this section, we give a theorem which will be useful in studying the cycles structure of weak and semi-weak keys. One definition is required first. A point x is an antifixed point of a key K if $E(K,x) = \bar{x}$.▌

Theorem 6

For each of the keys with a palindromic round key sequence there are precisely 2^{32} fixed points and for each of the keys with an antipalindromic round key sequence there are precisely 2^{32} antifixed points.

Proof:

The fixed point argument was given earlier. For the antifixed point argument, the keys with an antipalindromic round key sequence satisfy Theorem 3 with U being the all ones vector. Hence the antifixed points for these keys will coincide with those messages in which $m_8 = \bar{m}_9$ during the encryption process. Since there are 2^{32} such possible equations, there are 2^{32} possible antifixed points for each such key.∎

The DES Engines

Two special-purpose hardware devices were designed and built at Sandia as part of this study. These devices will be referred to in this paper as the DES Engine and the Micro DES Engine.

The DES Engine was designed to perform several types of cycle testing. It consists of 16 identical PC boards, each running a DES chip, the AM 9568, at high speed without changing keys. An IBM PC is used to provide communication with the user and to count the number of encryptions performed.

There are two basic modes of operation for this machine. In the first mode, each board performs a cycle test experiment using its preset key, independently of all other boards. In the second mode, the boards are paired so that cycle testing using alternating keys may be performed. The output of one board in the pair is used as the input to the other board. By this means, the pair can

perform an experiment with alternating keys, while each DES chip keeps its preset key unchanged.

Without describing the hardware in detail, the rudiments of its operation will be discussed. As part of the initialization of an experiment, several variables are set. These include a key, two starting points, SA and SB, and two other values, HA and HB, called "hit values". During the first step of the counter, SA is encrypted with the set key and compared to HA. If there is a match, the machine stops to report this result. It also stops if the encrypted value of SA is the same as SA, i.e., a fixed point has been found, or if a specified number of steps have been taken. The encrypted value of SA then is stored in the place of SA. During the next step of the counter, SB is encrypted with the preset key and compared to HB. The stop conditions described above are checked and, if not met, the encrypted value of SB replaces the original SB. This process continues until a condition for a machine halt is met or the operator intervenes. The machine will complete about 2^{32} encryptions per cycle per day.

The Micro DES Engine is a very specialized piece of hardware which was designed to take advantage of the internal structure of DES to find specific examples. In order to explain its operation, we need some notation. Suppose we are given two keys, K1 and K2, and two 32 bit vectors, m_0 and m_1. Let M be the concatenation of m_0 and m_1. To compute E(E(M,K1),K2) we would calculate

$$m_{i+1} = m_{i-1} \oplus f(m_i, K1_i) \quad \text{for} \quad 0 < i < 17 \quad .$$

Then letting $n_0 = m_{17}$ and $n_1 = m_{16}$, we would calculate

$$n_{i+1} = n_{i-1} \oplus f(n_i, K2_i) \quad \text{for} \quad 0 < i < 17 \quad .$$

The resulting concatenation of n_{17} and n_{16} would be the result. The Micro DES Engine allows us to specify two keys, two integers, i and j, and two 32 bit vectors U and V. It then allows m_i to

assume all 2^{32} possible values. For each such value, m_{i+1} is set to $m_i \oplus U$. Proceeding through the rounds of DES using the one of the keys, $m_{i+2}, \ldots, m_{17}$ are calculated. Now setting $n_0 = m_{17}$ and $n_1 = m_{16}$, the engine calculates the rounds of DES using the second key until it has found n_{j+1}. If $n_{j+1} = n_j \oplus V$, the result is reported before changing the value of m_i. In other words, the Micro DES Engine starts at some specified round of encryption with the first key and some linear relationship between adjacent terms of the sequence $\{m_l\}$ and stops at another specified round of encryption with the second key to check for another linear relationship between adjacent terms of the sequence $\{n_l\}$. There is a technical restriction that the combined number of rounds of DES in one of these steps cannot exceed 16. The complete experiment, trying all 2^{32} choices for m_i, requires approximately 13 hours of operation.

The Weak Key Cycle Structure

Before proceeding with the details of the cycle structures for any of the keys, we need to make the observation that the complement of any cycle is also a cycle since

$$E(K,x) = \bar{E}(\bar{K},\bar{x}) \quad .$$

This complementary cycle will also be called the dual cycle.

We are now ready to consider the cycle structure for weak keys. Several important properties of the weak keys, which have already been discussed, will now come to bear on the cycle structure. These are:

1. There are 4 weak keys K(0), K(5), K(10) and K(15),
2. Each key is its own inverse,
3. Each key has 2^{32} fixed points.

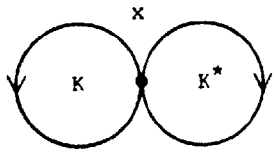
Since each key is its own inverse, a cycle of repeated encryptions with a weak key will either consist of one point, a fixed point for that key, or two points. These cycles, of course, are rather trivial.

However, alternately encrypting with a weak key and its complement has already produced some interesting results. We will call cycles of this type Coppersmith cycles. To be specific, a Coppersmith cycle is a cycle obtained by alternately encrypting with a weak key and its complement in which a fixed point is eventually encountered.

Since the complement of a cycle is a cycle, Coppersmith cycles could conceivably be self-dual or occur in isomorphic pairs. However, in [8], it was shown that only the latter case is possible. Hence, Coppersmith cycles can never contain both a point and its complement.

The Coppersmith cycles traced thus far range in size from 1 point to 12,605,533 points. Those cycles with one point are the "degenerate" Coppersmith cycles and were found with the use of the Micro DES Engine.

To find a one point Coppersmith cycle, we must find a point which is fixed by both a weak key K and its complementary key K^*. Pictorially this cycle will be



Hence, we initialize the Micro DES Engine with these keys, K and K^*, set i and j equal to 8, and let U and V be the all zero vectors. The engine will then produce a list of all possible values for m_8, so that $m_8 = m_9$ in the encryption with K and $n_8 = n_9$ in the encryption with K^*. From this we can produce a list of all fixed points of K which are also fixed points of K^*. There is

exactly one degenerate pair of complementary cycles for the key pair K(0), K(15) and one for the key pair K(5), K(10). These are

$$x = 74080FA36E793E74(\text{Hex})$$

and $\bar{x}$ fixed by K(0) and K(15) and

$$y = 1BDAFF22E4BDDA52(\text{Hex})$$

and y fixed by K(5) and K(10).

Excluding these degenerate cases, the remaining Coppersmith cycles traced thus far range in size from 12,605,533 points ($\approx 2^{23.6}$) to 26,717,619,870 points ($\approx 2^{34.6}$). We have traced 174 such cycles and find that these appear to end in fixed point cycles on the same key or on different keys with equal probability. We give one example in each case:

$$x = A1E1751167FED858(\text{Hex}) \quad \text{fixed by} \quad K(15)$$

and

$$y = 07CDA64B52C48D2F(\text{Hex}) \quad \text{fixed by} \quad K(0)$$

with a cycle length of 12,605,633 points ($\approx 2^{23.6}$) and

$$x = 0A60B8BCFB7F4116(\text{Hex}) \quad \text{fixed by} \quad K(15)$$

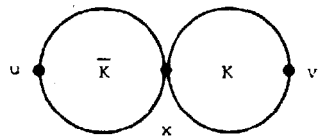
and

$$y = C4D9A9A9EDC0988C(\text{Hex}) \quad \text{fixed by} \quad K(15)$$

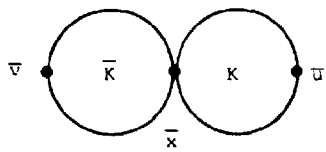
with a cycle length of 158,461,212 points ($\approx 2^{27.2}$).

The process of alternately encrypting with a weak and a semi-weak key may never encounter a fixed point. Cycles of this type

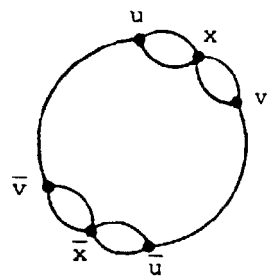
type will be called non-Coppersmith. These seem to naturally divide into two classes depending upon whether or not a point and its complement occur in the same cycle. The cycle containing a point x and the cycle containing $\bar{x}$, which may be disjoint, have the local structure



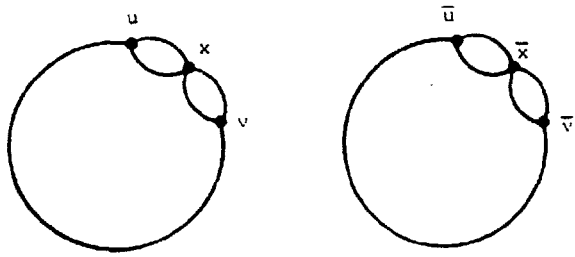
and



since $E(\bar{K},\bar{x}) = \bar{E}(\bar{K},\bar{x}) = \bar{v}$, etc. Analysis of the structure of such cycles leads to the discovery that non-Coppersmith cycles occur either as self-dual, centrally symmetric, cycles of the form



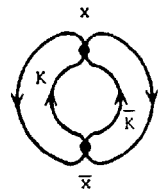
or as isomorphic pairs of the form.



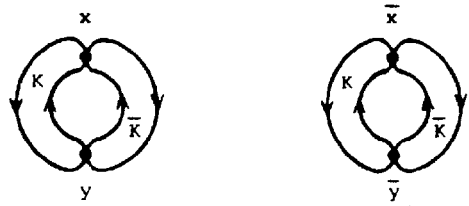
The central symmetry of both keys and points on the self-dual non-Coppersmith cycles means that the size of such a cycle must be congruent to 2 mod 4. The details of these theoretical results are in [8].

However, in an extensive computer search, no instance of either of these types of non-Coppersmith cycles has been found. Since there are exactly 2^{32} Coppersmith cycles and 2^{64} points in all, a reliable estimate of the size of Coppersmith cycles could be used to infer the likelihood of the existence of non-Coppersmith cycles. The best that can be said based on the 174 known cycles is that with a confidence of 99.9%, the fraction of the points in Coppersmith cycles is at least 96%. In other words, if 96% or fewer of the points are actually in Coppersmith cycles, 174 random selections would all be in Coppersmith cycles only one time in a thousand. This type of statistical argument can never prove the non-existence of non-Coppersmith cycles, but it can (as the number of unsuccessful tries increases) quantify the futility of continuing to search for them by a brute force random selection of starting points. If these exist, degenerate forms are also possible and would have the following structures:

Degenerate self-dual non-Coppersmith



Complementary pair of degenerate non-Coppersmith

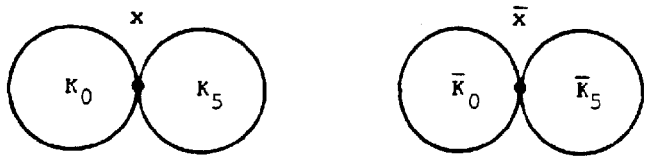


Unfortunately, we have no easy way to find these degenerate cases, if they exist, so producing one appears to be a 2^{64} search problem.

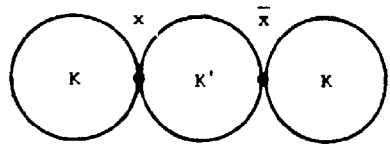
The final variety of cycle for the weak keys which we will consider consists of those obtained by alternate encryptions with any two weak keys. Obviously the cycles already discussed are special cases of these, in which the two keys are actually the same or one is the complement of the other. However, the remaining pairings give rise to some new cycle structures.

In this new setting, a cycle very much like the Coppersmith cycle is encountered in that it has a fixed point at either end of a chain of beads as in the Coppersmith cycles. However, there is no reason to believe that such a cycle would not contain both a point and its complement. Therefore, these new cycles have an extra possible class to consider. Of course, just as for the alternation of a weak key and it complement, a cycle alternating between any two weak keys might never encounter a fixed point. Thus structures corresponding to the non-Coppersmith cycles above appear to be possible. At this time, no results are available

except for those degenerate cases which could be found with the Micro DES Engine. No points were found which were fixed simultaneously by K(0) and K(10), however two points were found for K(0) and K(5). Hence, we obtain two degenerate pairs of complementary cycles, for this key pair, of the form:



If we consider the cycles in which fixed points are encountered and in which both a point and its complement are found, the degenerate case would be of the form:



This is not possible since we would have to find a point x for which $E(K,x) = x$ and $E(K,\bar{x}) = \bar{x}$. The last equation requires that $E(\bar{K},x) = x$ so that x would have to be a point fixed by K and its complement $\bar{K}$. The complete list of such points is available and for each such point x and each choice of a weak key K', we have verified that $E(K',x) \neq \bar{x}$.

The cycles in which a fixed point does not occur seem to once again require the solution of a 2^{64} search problem to locate degenerate cases, so that no such cycles have been produced.

The Semi-weak Keys

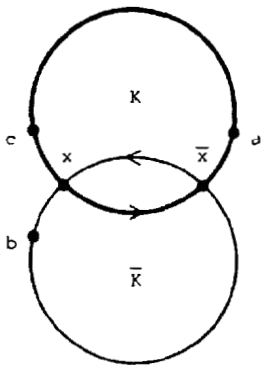
The semi-weak keys will be considered in two stages. There are four keys which have an antipalindromic sequence of round keys, as was discussed earlier. The remaining eight semi-weak keys have a different structure for their round keys. The discussion of these keys will be delayed until later in this section.

We begin by summarizing the properties, which were developed in the previous sections, of the keys with an antipalindromic sequence of round keys.

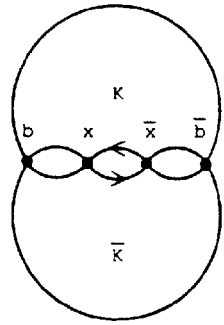
1) There are 4 of these keys K(3), K(6), K(9) and K(12).
2) The complement of one of these keys is its inverse key.
3) Each key has 2^{32} antifixed points.

Once again two cases seem to occur. A cycle which contains a point x may either contain its complementary point $\bar{x}$ or not. We will consider the first case now.

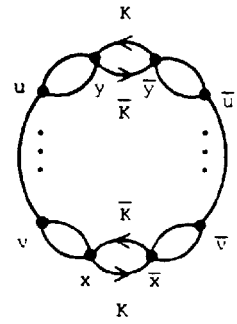
Suppose that x is an antifixed point of a key K. Thus x and $\bar{x}$ are in the cycle for K, but because $E(K,x) = \bar{E}(\bar{K},\bar{x})$, these points are also in the cycle for $\bar{K}$. Schematically, we have



Now consider the points $a = E(K,\bar{x})$ and $b = E(\bar{K},x)$. Notice that $\bar{b} = E(\bar{K},x) = E(K,\bar{x}) = a$. Also, since $\bar{K}$ is the inverse key for K, we have that $c = D(K,x) = E(\bar{K},x) = b = \bar{a}$. Hence the structure shown in the last diagram can be replaced by



By repeating this argument, we see that the points in the cycle all occur as complementary points with one of the antifixed point pairs at each of the antipodal points as shown in the following diagram.



Of course, this means that these cycles are self-dual and have diametrical symmetry, i.e., every point, u, in the cycle is reflected in the diameter drawn through the centers of the antipodal antifixed point pairs into its complement, $\bar{u}$. Since each of these cycles must have precisely two antifixed point pairs

in it and there are precisely 2^{32} such points for each key, there are exactly 2^{31} such cycles for each of the pairings of these semi-weak keys.

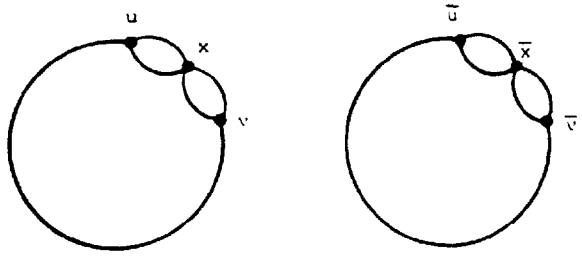
An example of a cycle of this type using K = K(3), has as the antipodal antifixed points:

$$x = 9EDB66CF776212B8(Hex)$$
$$y = 4B659E4C304032BF(Hex) \quad .$$

The cycle has a length of 6,236,877,706 $\approx 2^{32.5}$.

We have not traced sufficiently many cycles of this type to permit a reliable estimate of the expected cycle size. It would appear to be in the vicinity of 2^{32}, which, since there are only 2^{31} such cycles in all, would suggest that only half of the total number of points are in these self-dual (under complementation) cycles.

The other cycles for these keys must occur in complementary pairs. The form of these pairs of cycles is pictured below.



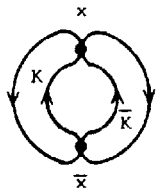
An example of a complementary pair of such cycles using K = K(3) are those on x and $\bar{x}$ where

$$x = 51F25587495909A5(Hex)$$

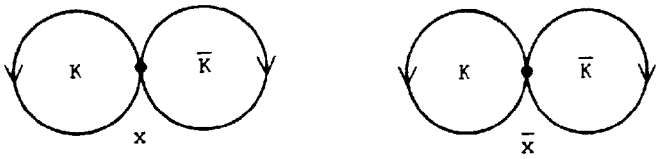
which has a cycle length of 6,671,292,514 $\approx 2^{32.6}$.

Given that both types of cycles occur for the semi-weak keys, i.e., self-dual and isomorphic pairs of cycles, an intriguing

question is whether degenerate cycles exist or not. A degenerate self-dual cycle would be of the form



while a degenerate isomorphic pair would be of the form



The Micro DES Engine allows us to answer the first half of the question. By letting the two keys be a complementary pair of the keys with antipalindromic round key sequences, choosing i = j = 8, and letting U and V be the all ones vectors, the set of all points which are antifixed by both of the chosen keys can be found. After trying all possible key pairs, we found that there is exactly one degenerate cycle for the key pair K(3), K(12) and one for the pair K(6), K(9). These are

$$x = 2046CAC677DCA40F(Hex)$$

for K(6) and K(9) and

$$x = 5A77FF65EC179215(Hex)$$

for K(3) and K(12). Unfortunately, Theorem 3 does not (so far as we can see) provide a means to reduce the 2^{64} search for degenerate isomorphic pairs. We therefore do not know how many, if any, degenerate cycles of this type exist for the semi-weak keys.

We will now turn our attention to the remaining semi-weak keys. Listed below are the facts known about these keys:

1) There are 8 such keys,
2) The inverse of any key in the set is also in the set,
3) The complement of any key in the set is also in the set.

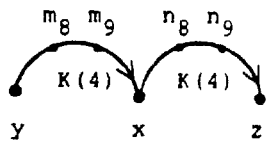
The round keys for a key K in this collection satisfy

$$K_i \oplus K_{17-i} = V$$

where V is either the vector consisting of 24 ones followed by 24 zeroes or the vector consisting of 24 zeroes followed by 24 ones. Of course, the round keys do not satisfy the hypothesis of Theorem 3, since $V \neq E(U)$ for any 32 bit vector U.

At this time, we do not know about the cycle structure for these keys, but some intriguing experiments have been completed on the Micro DES Engine. We offer a few of them here simply as tantalizing bits of information. For the description of these experiments, let U_1 be the vector of 16 zeroes followed by 16 ones; U_2 be the vector of 32 zeroes; and U_3 be the vector of 32 ones.

The first experiment used the key K(4) in both key positions of the Micro DES Engine and the values of i and j were both set to 8. There were three stages to this experiment and in each stage U and V were set to be equal. When the value of U was set to U_1 the engine found 2 values for m_8 and when $U = U_3$, the engine found 1 value for n_8. However, none were found when U was equal to U_2. Pictorially we have



where the arrows from y to x and from x to z show encryption with key K(4). The points marked along the arrow show the middle step in the rounds, that is, the position of m_8, m_9 and n_8, n_9. The results of the experiment show that there exists a value for y in this diagram for which $m_8 \oplus m_9 = U = n_8 \oplus n_9$ when U is equal to U_1 or U_3 but not when $U = U_2$.

A similar experiment was performed with K(4) and K(11) as the keys in the Micro DES Engine. We found that a value for y existed for which $m_8 \oplus m_9 = U = n_8 \oplus n_9$ when U is equal to U_1 or U_2 but not when $U = U_3$.

Perhaps these strange results will point to new directions in this study of cycles of cycles for these semi-weak keys.

New Directions

The results reported here are part of a study which is not yet complete. We will continue to collect statistics on the cycles obtained by alternate encryptions using two weak keys and also on the cycles using semi-weak keys which have antipalindromic sequences of round keys. The remaining semi-weak keys seem to be an open area of discussion with many possible avenues to pursue.

References

1. B. S. Kaliski, Jr., R. L. Rivest, and A. T. Sherman, "Is DES a Pure Cipher? (Results of More Cycling Experiments on DES)," Proceedings of Crypto'85, Santa Barbara, CA, August 18-22, 1985, in Advances in Cryptology, Ed. by H. C. Williams, Springer-Verlag, Berlin (1986), pp. 212-222.

2. D. Coppersmith, "The Real Reason for Rivest's Phenomenon", Proceedings of Crypto'85, Santa Barbara, CA, August 18-22, 1985, in Advances in Cryptology, Ed. by H. C. Williams, Springer-Verlag, Berlin (1986), pp. 535-536.

3. E. K. Grossman and B. Tuckerman, "Analysis of a Weakened Feistel-like Cipher," IBM Research Report, RC 6375, January 31, 1977; also, Proceedings ICC'78.

4. "Data Encryption Standard," U. S. Dept. of Commerce, National Bureau of Standards, FIPS Pub. 46, January 15, 1977.

5. D. W. Davies, "Some Regular Properties of the 'Data Encryption Standard; Algorithm," Proceedings of Crypto'82, Santa Barbara, CA, August 23-25, 1982, in Advances in Cryptology, Ed. by D. Chaum, R. L. Rivest, and A. T. Sherman, Plenum Press, New York (1983) pp. 89-96.

6. R. R. Jueneman, Privately circulated letter to American cryptologists, March 1, 1983.

7. "Guidelines for Implementing and Using the NBS Data Encryption Standard," U. S. Dept. Of Commerce, National Bureau of Standards, FIPS Pub. 74, April 1, 1981.

8. J. H. Moore and G. J. Simmons, "Cycle Structure of the DES for Keys Having Palindromic (or Antipalindromic) Sequences of Round Keys," Proceedings of Eurocrypt'86, Linköping, Sweden, May 20-22, 1986.