DES is not a Group

Keith W. Campbell and Michael J. Wiener

Bell-Northern Research, P.O. Box 3511 Station C, Ottawa, Ontario, Canada, K1Y 4H7

Abstract. We prove that the set of DES permutations (encryption and decryption for each DES key) is not closed under functional composition. This implies that, in general, multiple DES-encryption is not equivalent to single DES-encryption, and that DES is not susceptible to a particular known-plaintext attack which requires, on average, 2^{28} steps. We also show that the size of the subgroup generated by the set of DES permutations is greater than 10^{2499}, which is too large for potential attacks on DES which would exploit a small subgroup.

1. Introduction

The Data Encryption Standard (DES) [3] defines a set of permutations on messages from the set $M = \{0, 1\}^{64}$. The permutations consist of encryption and decryption with keys from the set $K = \{0, 1\}^{56}$. Let E_k: $M \rightarrow M$ denote the encryption permutation for key k, and let E_k^{-1} be the corresponding decryption permutation. If the set of DES permutations were closed under functional composition, then for any two permutations t and u, there would exist some other permutation v such that $u(t(m)) = v(m)$ for all messages $m \in M$.

The question of whether the set of DES permutations is closed under functional composition is an important one because closure would imply that there exists a known-plaintext attack on DES that requires, on average, 2^{28} steps [4]. Furthermore, multiple encryption would be susceptible to the same attack because multiple encryption would be equivalent to single encryption.

Kaliski, Rivest, and Sherman developed novel cycling tests which gave evidence that the set of DES permutations is not closed [4]. However, their work relied upon randomness assumptions about either DES itself or a pseudo-random function ρ:$M \rightarrow K$ which was used in cycling experiments. Because of the randomness assumptions, it is difficult to use the results of their cycling tests to make any claims about the probability that DES is not closed.

We have developed our own DES cycling experiments which provide evidence that DES is not closed; this evidence does not rely upon randomness assumptions. Our cycling experiments are similar to those of Quisquater and Delescaille for finding DES collisions [7, 8]. Other recent related work is the switching closure tests of Morita, Ohta, and Miyaguchi [6].

Don Coppersmith has developed an approach to finding a lower bound on the size of the subgroup generated by the DES permutations [1]. He has shown this lower bound to be greater than the number of DES permutations, providing conclusive proof that DES is not closed.

Section 2 contains the new probabilistic argument against closure which relies upon the ability to find a set of four keys which quadruple-encrypt a particular plaintext message to a particular ciphertext message. Finding such four-key mappings can be done with an approach similar to finding DES collisions. In Section 3, we review previous work in collision finding and build up to the new method of finding four-key mappings. Section 4 contains further details on our experiments. In Section 5, we describe Don Coppersmith's approach to obtaining a lower bound on the size of the subgroup generated by the DES permutations, thereby proving that DES is not closed. We also discuss our results based on his approach.

2. Strong Evidence Against Closure

We begin with the hypothesis that the set of DES permutations is closed and search for a contradiction. Let S_p be the set of messages that can result from encrypting or decrypting a particular message p with any DES key. Because there are 2^{56} keys, S_p contains at most 2^{57} messages. From the hypothesis, S_p is also the set of all possible messages which can result when multiple permutations are applied to p. If a message $c \in M$ is selected at random, the probability that $c \in S_p$ is at most $2^{57}/2^{64} = 2^{-7}$. We selected 50 messages at random (by coin tossing), and for each random message c, we searched for a set of permutations which map p to c using p=0 in each case. In all 50 cases we found a set of four DES keys i, j, k, and l such that $E_l(E_k(E_j(E_i(p)))) = c$ (see Appendix). Therefore, $c \in S_p$ and the probability of this event occurring 50 times is at most $(2^{-7})^{50} = 2^{-350}$. Because this is an extremely unlikely occurrence, we must conclude that the original hypothesis is incorrect and the set of DES permutations is (almost certainly) not closed under functional composition.

The argument above does not rely upon any assumptions about the randomness of DES or any other function; the fact that four keys exist which map p to c for each randomly selected message c is sufficient to draw the conclusion. However, the method used to find the four keys in each case does rely upon randomness assumptions.

3. Collision Finding

The method used to find four keys which map one message to another is similar to the approach taken by Quisquater and Delescaille in finding DES collisions[1] [7]. In both cases a function $f:M \rightarrow M$ and an initial message x_0 are chosen which define the sequence $x_{i+1} = f(x_i)$ for $i = 0, 1, \ldots$. Because M is finite, this sequence must eventually fall into a cycle. Unless x_0 is in the cycle, the sequence consists of a leader flowing into a cycle. The algorithms described by Sedgewick, Szymanski, and Yao [9] can be used to find the leader

[1] We have a DES collision when $E_i(m) = E_j(m)$ for some $m \in M$, and $i, j \in K$, $i \neq j$.

length λ and the cycle length μ. If $\lambda \neq 0$, this leads directly to finding a collision in f (i.e., $a, b \in M$ such that $f(a) = f(b)$, $a \neq b$, see Figure 1).

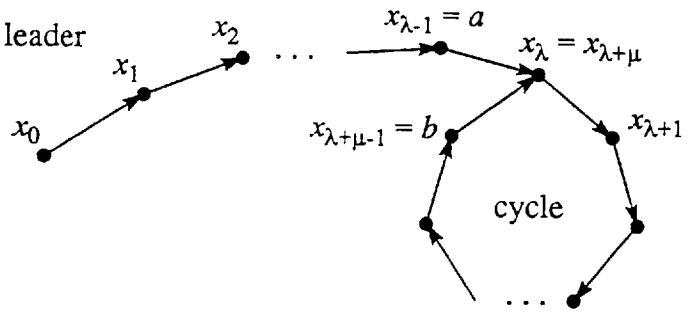

Figure 1. Leader and Cycle in a Sequence

DES Collisions

To find DES collisions, Quisquater and Delescaille used the function $f(x) = E_{g(x)}(m)$, where g: $M \rightarrow K$ takes a message and produces a key for DES encryption, and m is a fixed message. In this case, a collision in f is not necessarily a DES collision; if $f(a) = f(b)$, $a \neq b$, but $g(a) = g(b)$, then we have found a pseudo-collision where the keys are the same. Because there are fewer keys than messages, there can be at most $|K|$ distinct outputs from f. Assuming that DES is random and a suitable function g is selected, the probability of a collision in f leading to a DES collision is about $|K|/|M| = 2^{-8}$, and the expected time required to find a collision in f is on the order of $\sqrt{|K|} = 2^{28}$. Thus, the overall work factor in repeating this procedure until a DES collision is found is about $2^{28}/2^{-8} = 2^{36}$. This can be reduced somewhat using the method of distinguished points [7].

Two-Key Mapping

The method of finding DES collisions above was extended by Quisquater and Delescaille to find pairs of keys which double-encrypt a particular plaintext p to produce a particular ciphertext c [8]. In this case, collisions were found between two functions $f_1(x) = E_{g(x)}(p)$ and $f_0(x) = E^{-1}_{g(x)}(c)$. Given messages a, b such that $f_1(a) = f_0(b)$, $g(a)$ and $g(b)$ are a pair of keys with the desired property (i.e., $E_{g(b)}(E_{g(a)}(p)) = c$). To find a collision between f_1 and f_0, define the function f as follows:

$$f(x) = \begin{cases} f_1(x) & \text{if a particular bit of } x \text{ is set} \\ f_0(x) & \text{otherwise} \end{cases} \qquad (1)$$

The particular bit that is used to choose between f_1 and f_0 is called the *decision bit*.

If DES is random, then we can expect collisions found in f to be collisions between f_1 and f_0 about half of the time. This increases the expected work factor from 2^{36} in the single-DES collision case to 2^{37} in this case.

Four-Key Mapping

The double-encryption collision finding above can be applied directly to the problem discussed in Section 2 of finding a set of permutations which map p to c. However, we improved upon this approach by searching for four keys rather than two. We chose different functions f_1 and f_0:

$$f_1(x) = E_{h(x)}(E_{g(x)}(p)) \quad \text{and} \quad f_0(x) = E^{-1}_{h(x)}(E^{-1}_{g(x)}(c)) \tag{2}$$

where functions g and h produce keys from messages, and the ordered pair $(g(x), h(x))$ is distinct for all $x \in M$. This approach doubles the number of encryptions which must be performed at each step of collision finding, but it eliminates the possibility of pseudo-collisions. The expected number of steps required to find a collision in f in this case is on the order of $\sqrt{|M|} = 2^{32}$. To compare this running time to the two-key mapping above, we should take into account that fact that this approach requires two DES operations at each step instead of one. Also, only about half of the collisions in f are collisions between f_1 and f_0. Thus, assuming that DES is random, the work factor in finding four keys with the required property is about 2^{34}, which is eight times faster than finding a two-key mapping. The speed-up may be less than a factor of eight if the method of distinguished points is used for finding two-key mappings.

4. Further Details on the Cycling Experiments

In the cycling experiments, four-key mappings were sought as described in section 3 using the functions f, f_1, and f_0 in equations (1) and (2). The functions g and h in equation (2) were selected for ease of implementation. In the DES document [3], keys are represented in 64 bits with every eighth bit (bits 8, 16, ..., 64) a parity bit,[1] leaving 56 independent bits. The function g produces a key from a message by converting every eighth bit into a parity bit. Function h produces a key from a message by shifting the message left one bit, and then converting every eighth bit into a parity bit. Note that the ordered pair $(g(x), h(x))$ is distinct for all $x \in M$ so that there is no possibility of pseudo-collisions.

As a test, a four-key mapping was sought for $p = c = 0$. This value of c is not one of the 50 randomly-selected values which contribute to the argument in section 2. Using bit number 30 as the decision bit and an initial message x_0=`0123456789ABCDEF` (hexadecimal) yielded a collision between f_1 and f_0 with the following results:

λ = `1143005696` (decimal)
μ = `2756683143` (decimal)
keys: `8908BF49D3DFA738, 10107C91A7BF4C73,`
`4CEF086D6ED662AD, A7F7853737EAB057` (hexadecimal)

The results for the 50 random values of c are given in the Appendix. There were no additional values of c which were tried. This is important because failure for some values of c would greatly diminish the confidence in the conclusions drawn in section 2.

[2] In the DES document [3], bits of a message are numbered from 1 to 64 starting from the leftmost bit.

These experiments were conducted over a four-month period using the background cycles on a set of workstations. The average number of workstations in use over the four-month period was about ten, and in the end, more than 10^{12} DES operations were performed.

5. Conclusive Proof that DES is not Closed

In an as yet unpublished paper, Don Coppersmith described his latest work on finding a lower bound on the size of the subgroup, G, generated by the DES permutations [1]. He takes advantage of special properties of E_0 and E_1 (DES encryption with the all 0's and all 1's keys).

In earlier work [2], Coppersmith explained that the permutation E_1E_0 contains short cycles (of size about 2^{32}). This makes it practical to find the length of the cycle produced by repeatedly applying E_1E_0 to some starting message. Each of these cycle lengths must divide the order of E_1E_0. Therefore, the least common multiple of the cycle lengths for various starting messages is a lower bound on the order of E_1E_0. Also, the order of E_1E_0 divides the size of G. This makes is possible to get a lower bound on the size of G.

Coppersmith found the cycle lengths for 33 messages which proved that the size of G is at least 10^{277}. We have found the cycle lengths for 295 additional messages (see Table 2 in the Appendix). Combining our results with Coppersmith's yields a lower bound on the size of the subgroup generated by the DES permutations of 1.94×10^{2499}. This is greater than the number of DES permutations, which proves that DES is not closed. Also, meet-in-the-middle attacks on DES which would exploit a small subgroup [4] are not feasible.

It is interesting to note that in the course of investigating the cycle structure of weak and semi-weak DES keys in 1986 [5], Moore and Simmons published 5 cycle lengths from which one could have concluded that G has at least 2^{146} elements and that DES is not closed.

6. Conclusion

We have given probabilistic evidence as well as conclusive proof that DES is not a group. Furthermore, the subgroup generated by the DES permutations is more than large enough to prevent any meet-in-the-middle attacks which would exploit a small subgroup.

Acknowledgement

We would like to thank Alan Whitton for providing a large portion of our computing resources.

References

1. D. Coppersmith, "In Defense of DES", personal communication, July 1992 (This work was also described briefly in a posting to sci.crypt on Usenet News, 1992 May 18).

2. D. Coppersmith, "The Real Reason for Rivest's Phenomenon", *Advances in Cryptology - Crypto '85 Proceedings*, Springer-Verlag, New York, pp. 535-536.

3. *Data Encryption Standard*, Federal Information Processing Standards Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington, DC (1977 Jan. 15).

4. B.S. Kaliski, R.L. Rivest, and A.T. Sherman, "Is the Data Encryption Standard a Group? (Results of Cycling Experiments on DES)", *Journal of Cryptology*, vol. 1 (1988), no. 1, pp. 3-36.

5. J.H. Moore and G.J. Simmons, "Cycle Structure of the DES with Weak and Semi-weak Keys", *Advances in Cryptology - Crypto '86 Proceedings*, Springer-Verlag, New York, pp. 9-32.

6. H. Morita, K. Ohta, and S. Miyaguchi, "A Switching Closure Test to Analyze Cryptosystems", *Advances in Cryptology - Crypto '91 Proceedings*, Springer-Verlag, New York, pp. 183-193.

7. J.-J. Quisquater and J.-P. Delescaille, "How easy is collision search? Application to DES", *Advances in Cryptology - Eurocrypt 89 Proceedings*, Springer-Verlag, New York, pp. 429-434.

8. J.-J. Quisquater and J.-P. Delescaille, "How easy is collision search. New results and applications to DES", *Advances in Cryptology - Crypto '89 Proceedings*, Springer-Verlag, New York, pp. 408-413.

9. R. Sedgewick, T.G. Szymanski, and A.C. Yao, "The complexity of finding cycles in periodic functions", Siam Journal on Computing, vol. 11 (1982), no. 2, pp. 376-390.

Appendix: Results of Cycling

For each of 50 randomly selected messages c, Table 1 shows four DES keys i, j, k, and l such that $E_l(E_k(E_j(E_i(0)))) = c$. In each case, the initial message x_0=0123456789ABCDEF was used. The DES keys in the table include eight parity bits as defined in the DES document [3]. The table also shows information from the collision search including the decision bit, the leader length λ, and the cycle length μ. All quantities are shown in hexadecimal except the decision bit, λ, and μ which are shown in decimal.

Table 2 lists the cycle lengths obtained by applying the E_1E_0 permutation to various messages.

Table 1: Four-Key Mapping Results

ciphertext c	bit	λ	μ	key i	key j	key k	key l
D239854662E333D6	30	3089881971	1373508256	1C988A57AE5B1A6D	383215AE5EB637D9	754F0E80DC32C289	3B2607C16E196145
86112178D3236C8A	30	1914494444	693463224	107658E6610D61EF	20EFB0CDC219C1DC	7340CBB02FD9769E	B920E5D916ECBACE
0ADD04B7CDF1E742	30	6780759472	218462638	467C1C9138CDB085	8CF83B2370986208	51F16808324C0E08	A8F8B50498A78604
F30125D00EABAC2B	30	943553743	7310553453	07F1DF543D9D98F7	0EE3BFA87A3B31EC	C4A167E5BA26C449	E351B3F2DC1362A4
3A318B9A2BC6020F	30	4742565084	344544569	910E9DB0A2E3103B	201C386246C72076	CE76646EC1255438	E63B32B6E0132A1C
7B5C224859F144F2	30	2627610479	3114335933	131F49C8C189C11A	253D919280138034	8F04A26BA41C869E	46025134520E43CE
E4997DCBCAE0B6BF	30	5859776140	304193764	1562DA295E800E53	2AC7B652BC021FA7	89C2E994B979F107	C4E075CB5DBC7983
FAA52FD8F51EAE92	30	20629979	4238943918	B68F3B7C9E2FFD7F	6D1F76F83D5DFBFE	23FD832C5B29041C	91FEC1162C94020E
FA59DADF9170F1A7	30	2195424046	5907332685	98858AC832DCAEA7	320B169267B95E4F	EC7FA2BF3E26C72F	76BF51DF9E926216
79D117609B40BB21	30	433231912	2154862305	73ABDA4698D06E76	E657B68C31A1DCEC	15D60E0183FB62FB	0B6B8601C17CB0FD
81B5D8A98854D867	30	2552785502	1283047449	CE43FE261570328C	9E85FE4C2AE36419	04E001D975BABA51	02F1806DBADC5DA8
751B8E4CCCB4F92C	30	2255145649	4136209653	2CBF6D135BE367FD	5B7FDA25B5C4CDFB	97CB621C524C869E	CBE5310EA826C2CE
C6E4D4B4C74306D0	30	5247598183	2207575116	1310799429D608BA	2523F22A51AD1075	E9684A167AA13BA2	75B5250B3DD01CD0
C7755387564EB1B	30	1923363275	3322757394	E92AEF709B3715EF	D057DFE0346E29DF	A4132F8F7085BA29	D389164638C2DC15
08DE8EED757013BB	30	6621189834	912287793	70948A077C5DFB52	E32A150DF8BAF4A7	1C7C02B5802F6BBF	0EBF01DA401634DF
332D867940281 6A4	30	248767409	6266969674	B0168C3704CB2CBA	612F1A6E08975B75	0EB90E89B60DE901	07DC86C4DA077580
D0B38FD1E7E1D031	30	3811140202	2843420410	461689D3B56B6EFE	8C2F13A70BD6DFFD	837AC846760EF29E	40BCE523BA86F84F
668289C44AF40EF2	30	3619413642	1147320998	CE731CEA1AC81FEC	9DE538D637923ED9	6D296BFEBAD3EAF4	3794B5FE5DE9757A
AA8EEEC736FF5B1B	30	3069331961	200562212	07AB084A761A16FE	0E571394EC372FFD	BA04CE85BA4373B0	DC836743DCA1B9D9
2079AF9D6F2C2004	30	3906585734	1184537711	9ECB0BE376314F3D	3E9716C7EF619D79	FD2A20DA084F4991	7F94106D0426A449
FBCF00BC81569693	30	193983657	2169973674	D97F6E51F40E6D7A	B3FDDFA1E91CD9F7	0D588025D338043E	86ADC113681C839E
644E4441870C966C	30	846318690	328914116	C7D57A5723DC58F8	8FABF7AE46B9B3F1	C8EF8A1552CB85B5	E5F7C48AA8E5C25B
9049A1B8B57DE5ED	30	1630497906	1441467245	BA9B7980D9EFBCAD	7637F201B3DC7A5B	3E58A202510DA7B0	1FADD001A80752D9
C9B5D68D2C8BAACA	30	3233207975	423171687	9152BA947A2AA149	20A4752AF7544391	D5FB894F57076BE0	EAFD45A7AB8334F1
CE3A866379E48B40	30	10304236841	1262357982	BFB0CBE313EC9DB5	7C6197C726DA3B0B	2C796D269BBC8632	163DB6924C5E4319
CD1DFC7765036088	30	2384563551	5311633846	7A51E93EB540A2E0	F7A2D07F6B8346C2	5267456201CE3720	29B3A23101E61A10
CD24C9EC7971EB73	30	5122120540	261361938	DACE2F01C420ECF4	B69D5E028940D9EA	E310ECA464527920	7089F7D332A83D91
205E69FAB5452EC6	30	10545326230	317843105	929119DA7570C22A	252332D6EAE08554	EC454AF861C2C18A	7623A4FDB0E0E0C4
B79918774FBDE001	27	2401212140	1891297161	8C040B38A7CE46BA	190815704F9E8C76	57D0CE646120D5D3	ABE9E632B0916BE9
BB14D70900EFEC85	27	1975301710	5537484933	643DF2ABBC8F64AB	CB79E6547A1FC854	8AE55E83AE8CC410	C473AEC1D6C7E389
0A0BE33486A26CF1	27	6114881693	3979311181	4657573EF78CF4AE	8CAEAE7CEC1AEA5D	321C8A54072F8ACB	988F452A0216C4E5
7E306674557B57C7	27	3329518115	5406967207	FE2938C2B0BAA26B	FD527085627546D6	3B206232C802D3AB	9D103198E580E9D5
7D4EC4D9D0D88AFB	27	6829918624	455335254	7C0B2CAB8A3B5BCD	F8165B541576B59B	016D5D73A743E59B	80B62F3852A1F2CD
CD588CE10F137436	24	3325700738	674560323	76A1BAAD80152F6D	EF40755801295DDA	DFE529049801FEAD	EF739402CD807F57
57B8BB0DFADB4B17	27	6955122751	337345258	8A9852C1049BEC13	1631A7800834D925	CDAB9116F423F8C7	E654C80BFB107C62
13F59D60E96745C1	24	7238407367	2567725571	1C3797FE83F1A861	3B6E2FFE04E351C2	546107E61964C449	2AB083F28CB3E325
9CCC5AA115D52D97	27	3122231806	936075576	9E76D6F2985D3D25	3DEFADE631B97A4A	E986677008A1EF4C	7543B3B98551F726
9C13C1C217847F73	27	2505406823	3622543567	E58985732AA88C32	CB130BE657521964	268C547A3D684CB0	92C72A3D1F3426D9
922353787C7391A4	24	2577190833	169370608	9713F7D66BCED54A	2F25ECAED59DAB97	67B94A627FE36EFE	32DCA4B0BF70377F
F584C208B15488FF	27	1398059397	1014634505	73E5E5E6C43D75F4	E5C8C8CD8979E9E9	925E45D9FEA783AB	492F23ECFE5240D5
DB8F5045AC15612D	27	3276162424	1167926168	3E57AEA7F17C200E	7FAE5D4CE0F8431C	343EBCF8AEA213E3	1A1FDFFDD6D008F1
79E11F131781C081	27	3245667395	2355021803	B55D923DA4EAD068	68B9257949D6A1D0	B68A2CD646082C07	DA4516EAA2851602
6CD19C16143DB1B1	27	686670224	741307196	F13E7CD37AB99D13	E07FF8A4F4703825	C83EC43DA285C1FE	649EE39E5143E07F
2760D762F033022C	24	535710959	1933193087	6D68294F2A923157	D9D3529E542662AE	6B19FD3152EA5DF2	348C7F98A8752FF8
CB354D2FF5FF4048	27	2971721429	2763618490	D9CECD62198CFD83	B39D9BC4321AFB07	20A19ED06B2A08CB	9151CEE934158564
DE629517D229E809	24	4623799728	500111498	7610B0F452A479AD	EC2062E9A74AF258	01F719E567649715	017A8C733232CB0B
F24793142CC1A3B8	24	247977759	60533389	D6FE2FFD672A4545	ADFD5EFBCE578A89	C1736BB57961BA9E	613834DABCB0DC4F
D16E12E55A7D90EE	21	3617826299	2992595032	A1C752DFB5D3D508	438CA7BC68A4AB10	340EEA3DFDF104BC	1A86F41F7F79025E
21110855E8A87EB3	21	119490113	1525366355	01F74CF29ECB6D3B	02EC9BE53D97D976	51D5B59E43E5A207	A86BDACE20F25102
42D93C3251BE47CD	18	4397358172	1945651024	EC949EDF292F89BA	D92A3EBF515D1075	E07C79041331AE8F	F1BF3D02B998D646

Table 2: Cycles in E_1E_0

Fixed Point	Cycle Length
FCF4DFCDCD6258EF	28737542
2637A924F58B74BD	52726102
5FE79E047C375C9E	87605490
F86F776A3F29D215	120183041
4533781698641582	123741142
E8147AC7621EA6DB	141524875
A22C41175610DD0A	157126532
964C03BF6D9484CE	180757910
9A8F18520C494C0F	181353093
FE5532899F4D01FC	204877793
D3C92F24ECD607A5	229430263
7B4E903C419FEE77	241491405
D1BF57C1681B0239	241970136
B1C537BD77E825CD	274132024
74AF3228EAA0ADE2	277651190
2F03BED91D7CB16E	286320467
63FD39D830340D5F	311120314
8CB3ECBFADD205B3	337827436
F16941B21534C8CB	346375060
BAE2F389EDCDD00C	366197309
E8B79DDBA4FD8A13	370898345
23F50E3C63854946	382784102
F4FEB022D6662CC6	385833869
A382D83B6FB435C3	404923308*
96302873436936D5	417479850
633553B9521C31D6	448409291*
811F3718D8F04175	467147934
6DE9D894B80190A0	508130786
24D57E95080A4FB0	527729106
92B6FDDCEFE9CF2D	541798255
6F2DFEBB3E989D95	543178224
DFFFD1E64201DA17	549298502
B5E233FC14574CDA	559493983
022BED7A22E59128	572474003
4A7B87657BEE8666	607033653
FA2C0E43E4665530	628125220
C533E49F19CA472E	654423452
E72B8A2EAE9BB13B	678517304
1883A14E567687FF	681583312
66A0EC36E6F3F100	700905971
B4E9F57BD0F8B679	726834017
D99C26BC6DA73936	766356532
172F4F9F90B6228D	767546884
9E571181C12E4DAB	794419263
8FA5A8261FC20EFA	805683389

Fixed Point	Cycle Length
FDB78F429EEADFA4	823007021
12C328347DF3EAE8	862573395
5FE93A859DAD6C29	870494059
FD30744EFF9EA757	883285821
ACE0A8987991A8F5	903017135
DAEF18D6317C75F0	935440566*
AA757AAB74AC0B8C	954473685
F0591F59BD1C79D1	962933872
04968AFAB3A17659	1019170568
191CC6BFB3252119	1035340219
C4DEF2633D6B2BAD	1046106143
1F5A6143115FA46B	1056029096
AC3C22BAF7113361	1078179118
FD4ADA2B652DAF14	1095417692
34BFC05A291EFCB8	1099384916
1DEB703B3971041A	1102596768
593D785FEECB2E11	1124554449
EC93D670E0F981E9	1139686928*
0BEF1110DC771C55	1160996502
9A28778C1832A029	1259919806
DF45B97314256B6F	1270969573
CB979FAD005CA52A	1288329310*
30AD6A3EB26D7780	1295682916
106D8B45E41BB505	1316780514
D9555838874F07A8	1329512762
C75D3DEA483F8F92	1333813692
A798A0EC64F530D6	1362776543
A507CDD9A0E37CDD	1377253295
733C24355AF016C4	1408952249
582AE8818F89CED8	1411745523*
73D1BEF31F743DE7	1440389551
272004C5A8C08C1B	1452838755*
4E80AED88C4D7447	1456332586
54A3323DBC545563	1457931391
A3D1FAD47B65B2CE	1481121159
610723A4A638B148	1555624211
267CE6D2F57D4C4C	1572366534
116B35ABAC82B83D	1596684580
E5A7FB895D8B4283	1621444990
74ED56B5BB009873	1646234340
774042FF322B933B	1658279926*
AE6E861A366EDCEE	1667794970
723CAD0D7864D442	1720726879
74FCEF92A67710EB	1729629273
D5F679288259D405	1765832040*

Fixed Point	Cycle Length
293B8B4916116A73	1772480044
719D8FD9CC2A871B	1802710702
C4B4504254122C8F	1840982002
A8C7DF3F521679BC	1859355033
FAF0AE36AA5F1EA5	1860438650
5928C2BFD514AED2	1869960235
8C034F890968F42A	1878340485
1B8EEE8441CDD382	1892427527
9A2569A0AEDB49D2	1916660837
D2A5D7A973197B4B	1950547180
AFA1ABBF4BB955DF	1951540803
16A1D35AC590E575	1960590858*
62BB3BD4C5E03810	1963575439
517B782B6B245EE8	1974439655
AF15F768E46CFF88	1975291199
494B23CCE0E156FB	1976289957*
147157851C2DA94E	1985676665
5EF2C597356007C5	2006244556
F0A1E4C1FA9CDB4C	2014317312
6B284B5BC26557D3	2014541822
4D1BBD29B150C61C	2035226896
A4C744B6AD127B55	2069824992
299ADCF37CE8CD3F	2071794071*
01DE680F4FAB48E2	2073876626*
E0F67CC670C2C14C	2096398889
BD31B8A755F45A9B	2135153368
CD95869B7FDDDB46	2135924274*
1AAC771E9380091A	2194367878
481DCC93A14C20EE	2204440708
F059BD9059CEA918	2221853644*
97BCA3E48ED8979F	2279115448
9EA20A640426420C	2340054706*
0EE144EFFE5F7712	2351534544
D7A28C63755E1EEA	2369454965*
DB0F8C73A69DAFEE	2369547694
71D4FBDEDBF5A305	2371894158
C33A4F952102CF5F	2441900413*
9DB78A73F7CF9573	2446217335*
D098E4F9B7C4ED43	2515072933
EB9B39F90FF44710	2515145939
E77FAFDCEAB4452C	2582506813
3EEA319352E87106	2600936023
DE1067C794525386	2606685976
0C5FCCE93C32AD03	2630972069
23423A96946D85BF	2708430383

Fixed Point	Cycle Length
B987BE4572C1E068	2717253722
23D81F45DCBC4201	2755233816*
A587CC140147FCEC	2761360957
927814FAFBF171E4	2821852324
9E2C4EC0ABB5BB7E	2868112615
4B8A13754D14AC50	2942362723
3416B05300D49FA2	2986263853
BDEB9ECEEF8A7096	3052921261
036A9B4EAF272964	3094474831*
2D53A9077A3EF47E	3128640512
29D5A341EBF9EFD3	3166309170
3D82E8633EA0A272	3183868656
5500481254EEBF97	3212100817*
5ED8D27A34E44332	3246342391
7C2877590C8D2D5E	3273593348
F4078CF1D48F7F71	3311314857
E55FE3AD0FAE4FDD	3318474966
E57BE3D46D715A3F	3335024550
94AAF6070F545BF9	3364883533
CFC33DB97378F208	3395916196
73B3A5596976B3F3	3405347946
D706C0B5E854B9FF	3423707159
E30484E05625DFFB	3483123062*
D315B52726BDA812	3488857882
FFBA18FD815BC327	3505126062
B5F4161C355A93C3	3513382457
392E50DD868C7128	3545607921
13FC54C30DD99DCA	3553268870
FD1BE1E63CC2766C	3618749492
400B31DA21AD6C96	3644910743
D9B1719FFC04FD6C	3682602304
AEDE1C85D97D4916	3756009149
1E44C92BAA43BAF7	3761758591*
0FB4F926485E31EE	3788936982
0432B0FF9CEFC9C5	3848300992
9BAFA76824546615F	3848492727*
3E029F79AE75FF8C	3936611694
4656FA9A8F05420C	4024232999
BE4FDD565F0FB789	4068954054*
F0071E5685175134	4113784876
3E9C67C6FB4FE7EF	4148613660
759A08AD69EF31C4	4183043094
E959EF2DFCC8964E	4208755470*
56800CA94322106D	4246425419
A5C7B1B6667B772C	4249195877

Fixed Point	Cycle Length
028B303CE92C333B	4283087272
AE922AE9C4A52225	4298203540
63444CD11C18B4C4	4382270115
BACEA511BA41C759	4390335938
5B3F0EAE4D862D84	4459487784
1D7B02C8ACC7E53C	4508263560
CFF9F3C131CC7550	4580633338
EAC3E909F58A558D	4613073219*
E99B31CAA032D7C8	4624025139
E41EC962C6C47B65	4723147830
57EA50D8AD1CE918	4739063890
C8817AE4B68991EB	4784804293
683F326ECD48C5BB	4872065936
42401C77315C7B88	4894852081
4C041CA63D404722	4911410310
860301DFDA5F6CE9	4916166999
0A91867B20A0AB78	4933454607
F8EDBCF8992518D8	4981750033
0D09225A6F23920C	4993175863
C8F29864F23C76CF	5061956573
65FF5031CC043066	5063489704
C8531CF8E8266298	5096034192
5E52B788C04A56A5	5147568304
DB4303351EFF5A45	5153751028
B327F78B62127D5B	5225643840
5B040B741A69945A	5252632235
BDD52954BEB3CDB7	5338270753
7466CB0E05E47549	5375493367
192B8FB26A9A8B65	5400551559
46A3BA578D1DFF39	5435256032
F7F4B2A75E8129D3	5512472327
8493BA42C1AF97BB	5629649963
733DDF9357C79C33	5636606472
BF4CB1A6C45F21B1	5722528000
FD084D25BEC96BBD	5805144356
7F8362AAA1649DC0	5831919016
A32B99B3FC717587	5859853287
A7DE27C43B5C5C39	5958850892
20175B45BD4CA98D	5968398003
27C5CE42FB889B07	5992136736
44ACB24B48F2EA3E	5992335770
2E6571E8F9FA00CB	6005957167
196421C0522D9F27	6023557864
97E166C859F92C9B	6058340939
5358E006EAF28086	6075474474*

Fixed Point	Cycle Length
3FC814FE565204F7	6076137232
B82E80EE4033A771	6174407692
2EC25679D6D5E8F5	6355464088*
C05680AD3C07F1B2	6403156820
A1643E70F40AC485	6411947449
7CBFC9F1EF594543	6423946064
EC7BE141D8F8E02A	6461094891
B172E38614971BAB	6530104692
0A52F9F5B508535A	6541262041*
0D933718D67C6B59	6571553375
F4A2EAE3410D1BB0	6641226295
449949ECE4983DBB	6667170278*
41CA463EA250A332	6787002094
3BCBB7F6683AA6D5	6795225733
605B16CFA01147D6	6951857282
47141CA4E94E7215	6976824673
7598BE442B9F6882	6987647830
6897889FCC5D56D4	7073844641
A2314D0E2EBAF30D	7085878364
66CD3375E72033CC	7179626977
7B0CBBC1763305D3	7255627009
68106C0A43FE6522	7430231952
A62DDB82EDB57579	7432217460
FEB3CBBEB0CBD609	7441592579
3F1F8B74A69E06D0	7467140836
787269937CC60C95	7602958918
5AA9BC166BCBC1E0	7625629397
1BDAE545482E8836	7661134106
92F24247E8C197C1	7778204234
19E9639892EF9C12	7870418672
C34C33138F92846D	7978153130
4EDC7FDFA4EA9977	8000193283
5F02CBB6AD214792	8063326246
4CFA478543ACE2B4	8170427064
F23078B46BAA7B88	8294313318
F68931B21E24E0A6	8295656675
F6F3D76136C84022	8421270154
A0FC512859D8C21C	8480871302
15E457C279CC7499	8515184617
39CDFF9507CFDBBD	8517167189
D67AD5F40B78CA8C	8545713623
4A56F2927725A424	8561303690
18D1B12D04887B83	8852280158
B434D0C7CEA94EB9	9041567214
78C1D96C74990310	9316341100

Fixed Point	Cycle Length
E067F0D748149AF2	9476168292
8F7E4EB0297787F8	9678698128
A35245FB541E37A2	9705739403
0262CCE830A394BB	9711267022
9496D43FBCC91E87	9747304899
3FF08C6CED38A444	9769896281
ACBD4DA777D38BE3	9796615090
466AD21308BAD2EC	9823918953
70A41AB0D40CEFA0	9836467612
7E9E33C139B2015E	9917373190
008DCF4AEB733AFD	10004493651
33BC699F47851335	10068441381
062C933D766B0FA4	10076514201
CC2B00691E5EBE0E	10180552100
7F73242331744 08C	10193525631
ED201340D9A2B4E8	10407078931
E6644068626295AE	10479263238
99EC5A4CF7C3A0E9	10668733089
006DFE97E83F0FC6	10731024975
2786035A519568F8	10918119836
172899FDD1D74D0D	10990688763
0CEC14247261696B	11140433392
D39421C50130C8CA	11162679154
94EBCA90F6428304	11240761345
532B1B06EA74A0B3	11260342500
9A31D7A5723C56B4	11294586603
92200FBA0F8DF66E	11407565190
842E9956E4B81920	11494443331
E686AFB65F2092F3	11893145004
C383AFB82A0EF481	12160327293
D5473BE134496315	12192580878
A0773F73D932371D	12742315020
0F7BCD33015A75D1	13004312584
413AE03B7A9AAA6F	13136649204
3F75DD7BC68203AB	13548566368
09C0CC2DC8C31CEE	13564048102
E7BBD0F753EB7080	13650787679
BC3F0AA77B7EC4B7	14285353135
9EBE7F47C30CD9FA	14336899988
927A18722DBC03CA	14604244081
9197B53934E55BEF	15006473066
8E93415C528F9B68	15041961023
1E901C02D65BD8B5	15287551934
F73F935649B46D88	15298372664
2F6B424E5673266A	15827495095

Fixed Point	Cycle Length
E2F75B968FBECDF5	16062224185
086E5AED560BE868	16065667731
571A296A3C28BC1D	16077856896
736E43159A4294F5	16201395230
DC951D638F8AEEB2	17174407494
7B443B3A7D272FA5	20737469521*
52329A83D7D8B6D1	21076207728
119EA346AFAAE345	21665705336
8BF8AF4A80AAF623	23510577127
6A0095E0DFB3309D	24142549973
D0401BB66BF30BB4	26928043663
A5349E5B476385A1	27732705289
D3E42C9F9156E120	32908364861

* Starred entries were computed independently by Coppersmith. Taken in isolation they yield a lower bound of 1.16×10^{277}. The least common multiple of all the lengths listed is 1.94×10^{2499}.