COMPUTER SCIENCE & TECHNOLOGY:

MAINTENANCE TESTING FOR THE DATA ENCRYPTION STANDARD

NBS Special Publication 500-61

U.S. DEPARTMENT OF COMMERCE
National Bureau of Standards

NATIONAL BUREAU OF STANDARDS

The National Bureau of Standards[1] was established by an act of Congress on March 3, 1901. The Bureau's overall goal is to strengthen and advance the Nation's science and technology and facilitate their effective application for public benefit. To this end, the Bureau conducts research and provides: (1) a basis for the Nation's physical measurement system, (2) scientific and technological services for industry and government, (3) a technical basis for equity in trade, and (4) technical services to promote public safety. The Bureau's technical work is performed by the National Measurement Laboratory, the National Engineering Laboratory, and the Institute for Computer Sciences and Technology.

THE NATIONAL MEASUREMENT LABORATORY provides the national system of physical and chemical and materials measurement; coordinates the system with measurement systems of other nations and furnishes essential services leading to accurate and uniform physical and chemical measurement throughout the Nation's scientific community, industry, and commerce; conducts materials research leading to improved methods of measurement, standards, and data on the properties of materials needed by industry, commerce, educational institutions, and Government; provides advisory and research services to other Government agencies; develops, produces, and distributes Standard Reference Materials; and provides calibration services. The Laboratory consists of the following centers:

Absolute Physical Quantities[2] — Radiation Research — Thermodynamics and Molecular Science — Analytical Chemistry — Materials Science.

THE NATIONAL ENGINEERING LABORATORY provides technology and technical services to the public and private sectors to address national needs and to solve national problems; conducts research in engineering and applied science in support of these efforts; builds and maintains competence in the necessary disciplines required to carry out this research and technical service; develops engineering data and measurement capabilities; provides engineering measurement traceability services; develops test methods and proposes engineering standards and code changes; develops and proposes new engineering practices; and develops and improves mechanisms to transfer results of its research to the ultimate user. The Laboratory consists of the following centers:

Applied Mathematics — Electronics and Electrical Engineering[2] — Mechanical Engineering and Process Technology[2] — Building Technology — Fire Research — Consumer Product Technology — Field Methods.

THE INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY conducts research and provides scientific and technical services to aid Federal agencies in the selection, acquisition, application, and use of computer technology to improve effectiveness and economy in Government operations in accordance with Public Law 89-306 (40 U.S.C. 759), relevant Executive Orders, and other directives; carries out this mission by managing the Federal Information Processing Standards Program, developing Federal ADP standards guidelines, and managing Federal participation in ADP voluntary standardization activities; provides scientific and technological advisory services and assistance to Federal agencies; and provides the technical foundation for computer-related policies of the Federal Government. The Institute consists of the following centers:

Programming Science and Technology — Computer Systems Engineering.

[1]Headquarters and Laboratories at Gaithersburg, MD, unless otherwise noted; mailing address Washington, DC 20234.
[2]Some divisions within the center are located at Boulder, CO 80303.

COMPUTER SCIENCE & TECHNOLOGY:

Maintenance Testing for the Data Encryption Standard

Jason Gait

Center for Programming Science and Technology
Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, DC 20234

U.S. DEPARTMENT OF COMMERCE, Philip M. Klutznick Secretary

Luther H. Hodges, Jr., Deputy Secretary

Jordan J. Baruch, Assistant Secretary for Productivity, Technology and Innovation

NATIONAL BUREAU OF STANDARDS, Ernest Ambler, Director

Issued August 1980

Reports on Computer Science and Technology

The National Bureau of Standards has a special responsibility within the Federal Government for computer science and technology activities. The programs of the NBS Institute for Computer Sciences and Technology are designed to provide ADP standards, guidelines, and technical advisory services to improve the effectiveness of computer utilization in the Federal sector, and to perform appropriate research and development efforts as foundation for such activities and programs. This publication series will report these NBS efforts to the Federal computer community as well as to interested specialists in the academic and private sectors. Those wishing to receive notices of publications in this series should complete and return the form at the end of this publicaton.

National Bureau of Standards Special Publication 500-61
Nat. Bur. Stand. (U.S.), Spec. Publ. 500-61, 28 pages (Aug. 1980)
CODEN: XNBSAV

Library of Congress Catalog Card Number: 80-600105

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1980

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402
Price $2.00
(Add 25 percent for other than U.S. mailing)

TABLE OF CONTENTS

Maintenance Testing for the Data Encryption Standard

Jason Gait

This publication describes the design of four maintenance tests for the Federal Information Processing Data Encryption Standard (DES). The tests consist of an iterative procedure that tests the operation of DES devices by using a small program and minimum data. The tests are designed to be independent of implementation and to be fast enough to test devices during actual operation. The tests are defined as four specific stopping points in a general testing process and satisfy four testing requirements of increasing degree of completeness depending on the thoroughness of testing desired.

Key words: Communications security; computer security; cryptography; data encryption standard; in-service testing; maintenance tests; Monte-Carlo testing; stuck-fault testing; test cases.

1. INTRODUCTION

The Federal Information Processing Data Encryption Standard (DES) is the standard cryptographic algorithm for use within the Federal Government for protecting non-classified transmission and storage of computer data. The DES algorithm is normally implemented in hardware and commercial DES devices are presently available from eight different sources. The National Bureau of Standards has validated the designs of the various hardware implementations with a validation test, i. e., a collection of input-key-output triplets which, when applied as a test to a device, and if successfully executed, insures that the device being tested in fact correctly executes the DES algorithm. A Monte-Carlo test using random data is also a part of this test [8].

A small maintenance test, residing in read only memory and executed by the same microprocessor that controls the DES device provides a means of testing the operation of the DES hardware in the field. Since one criterion for a field test is that it be economical, the tests are designed so that only a partial test may be needed in a given application. The test is so designed that a full functional test can be executed if it is convenient and desirable to do so.

The maintenance test provides results which are a combination of the validation test and of the Monte-Carlo test described in [8]. The maintenance test uses an initial fixed input-key pair and the resulting ciphertext is then fed back as input or as key, as in the Monte-Carlo test, and this cycling process is repeated. By simply checking the output of this process against four known results the test determines if the DES algorithm is properly functioning. A maximum of 192 cycles has been determined to test completely the DES device but three earlier check points are defined which result in specific partial tests. In all, four categories of tests have been defined. They range from a simple test for stuck-faults of the 64 output bits of the DES to a complete functional test.

1.1 Validation vs Maintenance Testing

The maintenance tests described here replicate the functionality of both the validation test and the Monte-Carlo test procedure used to validate implementations of the DES [8,9]. In fact, by taking advantage of the pseudo-random nature of the DES output, we are able to describe a smaller, more efficient test procedure that is equivalent to the test previously described in [8], although the extensive Monte-Carlo test is not reproduced.

1.2 The Maintenance Tests

The maintenance tests depend only on the functionality of the algorithm and not on any particular implementation. The tests can be performed with a short program whose two inputs consist of an initial plaintext and an initial key and whose output is a final ciphertext. The test program creates a cycling process that tests the complete functionality of the DES algorithm as well as testing for stuck-at-one and stuck-at-zero faults at the various input and output interfaces. Stuck-at-one or stuck-at-zero faults occur due to a circuit failure, e. g., an open circuit. The device is known to be performing correctly if the observed final ciphertext matches the expected result. The cycling process consists of a maximum of 192 encipherments and decipherments intermixed in such a way as to test all aspects of the algorithm. The execution of the test program requires little time and hence the test can be used on-line to examine the functionality of a device in-service as well as for other testing purposes.

The complete test is determined by the following recurrence relation:

$$
\begin{aligned}
K_1 &= 5555555555555555 \\
P_1 &= FFFFFFFFFFFFFFFF
\end{aligned}
$$

$$
\begin{aligned}
C_i &= E(K_i, P_i) \\
C_{i+1} &= E(K_i, C_i) \\
C_{i+2} &= D(C_{i+1}, C_i) \\
K_{i+3} &= C_{i+2} \\
P_{i+3} &= C_i
\end{aligned}
$$

where K_i, P_i and C_i denote key, input and output at time n, with the value of i determined from the equation $i = 3(n-1)+1$ for n=1,2,3,..., TESTLENGTH. Here the symbol E denotes the DES encryption operation and D denotes the DES decryption operation. The initial values of key and plaintext, K_1 and P_1, are 64 bit numbers represented in hexadecimal notation with correct parity for each 8-bit byte of the key.

The test can be used in any of four modes depending on the degree of certainty required and the time available to perform the test. In each of the four modes only the final ciphertext differs, initial plaintext and key remain the same.

Test 1: Tests all output bits for stuck-at-one and stuck-at-zero faults; the P and E matrices used by the DES algorithm are also tested.

Test 2: Includes Test 1, tests the S-boxes and includes a test for stuck-faults at all the key and input bits except one input bit.

Test 3: Includes Test 2, a complete test for stuck-faults and a test of the IP^{-1} matrix.

Test 4: Tests all aspects of the algorithm.

The following table provides a concise display of the various tests, the number of iterations required for each test, the number of encryption or decryption operations performed during each test, the final output for each test and the specific properties of the DES algorithm that are tested during each test.

Table 1. Properties of the Four Maintenance Tests

	test1	test2	test3	test4
iterations	3	6	8	64
enc/dec ops	9	18	24	192
final output	BF1FF37B C46CC2CA	1DFCF1C8 44E84A9B	00B82CBB E58DBB9F	246E9DB9 C550381A
props tested	output stuck faults, P, E	test 1 and S-boxes	test 2 and input stuck faults	complete test

1.3 The Values for the Parameters of the Test

The efficacy of the testing procedure depends largely on the effectiveness of the DES as a pseudo-random number generator [5]. The number of iterations needed to satisfy each test requirement could not be determined in advance. However an upper-bound value for TESTLENGTH was determined from a Markov chain model of the full testing procedure. The results were that if pseudo-random input vectors are presented to a linear device with n inputs, then the expected number of tests required to test completely the device for sufficiently large n is approximately n+2. Since n is the minimum number required, the distribution has a very small standard deviation. Hence we need to examine at most n+3 or n+4 pseudo-random input vectors to be sure of obtaining a maximal linearly independent set (=basis) of appropriate dimension. See Appendix C for the details of the calculation.

2. DESCRIPTION OF THE DES ALGORITHM

The Federal Information Processing Data Encryption Standard published on January 15, 1977 [3] is a complex non-linear ciphering algorithm that was designed for efficient hardware implementation. Although there are software implementations, they do not comply with the standard and are generally quite inefficient compared to hardware versions [6]. The DES algorithm operates on 64 bits of input to produce 64 bits of output under the action of a 56-bit keying parameter. With the exception of initial and final permutations, the algorithm is a series connection of sixteen rounds. Each round uses 48 bits of the key in a sequence determined by a key schedule. With the exception of this difference in the round keys, the sixteen rounds are identical to one another. Each round receives an input of 64 bits; the 32-bit right half is expanded by the linear operator E to 48 bits and the result is mod 2 added to the round key; the 48 bit sum is divided into eight 6-bit blocks, each of which determines a 4-bit S-box entry; the resulting 32 bits are added mod 2 to the left half and the two halves are interchanged, thus producing 64 bits of output for the round. Sixteen rounds connected in series, each using a different round key as determined by the key schedule, together with initial and final permutations make up the DES algorithm. Despite its complexity the DES is capable of operating at high speed when implemented in hardware. For example, an encryption or decryption of one

64-bit block on the NBS DES unit takes 9 microseconds. Appendix A contains a complete functional description of the DES algorithm parameters, i. e., permutations, S-boxes and key schedule.

2.1 The Permutations and E Operator

The role of the permutation P is to mix thoroughly the data bits. The operator E expands its 32 bit input to a 48 bit output that is added mod 2 to the round key. The permutations in the key-schedule, PC1 and PC2, intermix the key bits among the round keys in such a way as to equalize key-bit utilization. No key bit is used more than 15 times nor less than 12 times. The initial and final permutations, IP and IP^{-1}, are byte oriented for efficient hardware implementation.

Each permutation is a linear operator, and so can be thought of as an n x m matrix and can be validated completely if it operates correctly on an appropriate maximal linearly independent set of input vectors, i. e., a suitable basis.

2.2 The S-boxes

The non-linear substitution tables, or S-boxes, constitute an important part of the algorithm. The purpose of the S-boxes is to ensure that the algorithm is not linear [1,2]. Each of the eight S-boxes contains 64 entries, organized as a 4x16 matrix. Each entry is a four bit binary number, represented as 0-15, so the output of the parallel connection of eight S-boxes is 32 bits. A particular entry in a single S-box is selected by six bits, two of which select a row and four select a column. The entry in the corresponding row and column is the output for that input. Each row in each S-box is a permutation of the numbers 0-15, so no entry is repeated in any one row.

2.3 The Key Schedule

The purpose of the key schedule is to provide a thorough intermixing of the key bits for the algorithm. The key schedule is linear, so its implementation can be verified by presenting 56 basis vectors (= a maximal linearly independent set for this operator) as keys. The encryption process uses left shifts in the key schedule while decryption uses right shifts, so an additional 56 decryptions are required for testing. The key schedule is extremely important to the security of the algorithm: it has been shown [4] that similar algorithms without similar key schedules may be substantially weaker even if they have much larger keys.

2.4 Maintaining the Correctness of DES Devices

The test program verifies the correct operation of an implementation by performing one of several optional series of tests on the device during operation. The pseudo-random tests have been examined to be sure that a basis of vectors is presented to each of the matrix operators in the algorithm, thus verifying their correct implementation as linear operators, and to exercise every element in each S-box.

<u>2.4.1 DES Tests.</u> The tests are designed to assure the correctness of each of the following components of the algorithm (see Appendix A):

1. Initial permutation, IP
2. Inverse permutation, IP^{-1}
3. Expansion matrix, E
4. Data Permutation, P
5. Key Permutation, PC1
6. Key Permutation, PC2
7. Substitution tables: S_1, S_2,..., S_8
8. Mod 2 adders

In addition the tests protect against the possibility of stuck-faults at the interfaces between any of the above elements as well as at the input, key and output of the DES itself.

2.4.2 Relationship to Validation Tests. The NBS validation test of DES devices consists of operating on a sequence of discrete input-key-output triples. The input and key are entered into the DES device, an encryption or decryption operation is performed and the result is compared with the known correct output. Each linear aspect of the DES algorithm, e. g., P, E, and so forth, is tested independently by presenting to it a standard unit basis to be operated on. The maintenance test performs an equivalent test by relying on the pseudo-random nature of the DES algorithm to present a basis, but not necessarily the standard unit basis, to each linear element of the algorithm, thereby insuring that they are tested completely. The maintenance test is set up in such a way that various aspects of the algorithm are tested simultaneously and the tester does not receive the information provided by the validation test regarding the location of a failure. However the purpose of these tests is simply to verify that the DES device is working correctly rather than to isolate the location of failures.

3. TESTING PHILOSOPHY

The DES has been implemented by many vendors using many different techniques. To be most useful a test for the DES should be applicable to all DES devices without regard to implementation. The maintenance tests are therefore designed only to test the functionality of the algorithm itself at the well defined interfaces, such as input, key and output. While the NBS validation test could be used for maintenance, it does not meet the desirable criterion of a maintenance test for minimizing the amount of data stored. It was also desired to minimize the total number of encipherments and decipherments during the test to make the test more practical in an on-line environment during intervals between transmissions.

3.1 Stuck-faults in Cipher Feedback Mode

One of the modes of operation of the DES is cipher feedback, where the output of the DES is added mod 2 to the plaintext to produce ciphertext. If the output of the DES is subject to stuck-faults, either at one or at zero, then some part of the plaintext, or its complement, is being transmitted in the clear. It is therefore desirable that the device be tested for stuck-faults, preferably during all encipherment operations, while being used in cipher feedback mode.

3.2 Generating the Pseudo-random Tests

Since the DES is known to be a good pseudo-random number generator [5], the maintenance test was designed to use the output of the DES fed back as data or as key-text alternatively. Both encryption and decryption operations are used in order to exercise all parts of the algorithm. When all the cycles of each test have been completed, the final output is compared with a single stored value. If the two values are the same, then the device has passed the test, otherwise the device should be rendered inoperable.

The following program is used to do this:

```
key = 5555555555555555
input = FFFFFFFFFFFFFFFF
for(n=1; n<TESTLENGTH; n=n+1){
        crypt('e', key, output, input)
        input = output
        crypt('e', key, output, input)
        key = output
        crypt('d', key, output, input)
        key = output
}
if(output==LASTCIPHER)OK
else NG
```

The 64 bit starting values for key and input are represented in hexadecimal notation. The value of TESTLENGTH, either 3, 6, 8 or 64, is user supplied and is determined according to the degree of completeness of testing desired. The value of LASTCIPHER is as listed in Table 1 for the appropriate number of iterations. The values of TESTLENGTH and LASTCIPHER are set according to which test is desired.

The following list specifies the values of TESTLENGTH and LASTCIPHER for each of the four testing modes described.

Test 1 Parameters: TESTLENGTH = 3
LASTCIPHER = BF1FF37BC46CC2CA

Test 2 Parameters: TESTLENGTH = 6
LASTCIPHER = 1DFCF1C844E84A9B

Test 3 Parameters: TESTLENGTH = 8
LASTCIPHER = 00B82CBBE58DBB9F

Test 4 Parameters: TESTLENGTH = 64
LASTCIPHER = 246E9DB9C550381A

3.3 Description of Tests

Test 1 uses three cycles of the program, corresponding to nine encryptions or decryptions. Test 1 is useful as a maintenance test for the DES when used in cipher feedback mode to ensure that no stuck-faults in the output will expose plaintext. It is a short test and can be practically executed on-line between transmissions. Note that for this test each bit of the output is both zero and one at least once.

Test 2 uses six cycles, corresponding to eighteen encipherments or decipherments, which are enough to test completely the S-boxes, the P and E matrices, all outputs for stuck faults and almost all inputs for stuck-faults (plaintext bit 54 is stuck-at-one throughout this part of the test). Two more cycles, actually five more operations, are required to unstick data bit 54, and carry out test 3. Test 3 tests for stuck-faults at the input and output of every algorithm element, i. e., IP, P, E, IP^{-1}, PC1, PC2, the S-boxes, the shifts in the key-schedule and the inputs and outputs of the mod 2 adders.

Test 4 is a complete test of the functionality of the algorithm. The verification of both tests 2 and 4 requires examination of the inputs to each of the linear elements of the algorithm to ensure that a basis, i. e., a maximal linearly independent set of vectors of appropriate dimension, is presented to each, thus ensuring that all matrix entries are fully exercised. The DES validation test presents standard unit basis vectors to these linear elements, while the maintenance test presents random inputs. Thus the inputs have been checked, not for the standard unit basis, for which we would have to wait a long time, but for any basis of the proper dimension. This is equivalent to the standard unit basis in terms of testing linear elements. A variant of the Gram-Schmidt orthogonalization process was used to do this, as described in Appendix B. The application of this process shows that the first 32 vectors applied to P are linearly independent, thus testing P completely; this corresponds to just two encipherments, since P is used 16 times during each encryption or decryption operation, or one cycle of the program. Similarly, the first 34 vectors applied to E contain a maximal linearly independent set (the 17th and 33rd vectors are dependent on the others); again the first cycle of the program suffices to test E. Hence test set 1 for stuck-faults tests P and E as well.

The first 66 encipherments, corresponding to 22 cycles of the program, test completely IP^{-1}; the first 87 encipherments, corresponding to 29 program cycles, test the entire key schedule for both encipherment and decipherment; and 64 complete cycles are required to test IP. It is this requirement of testing the initial permutation that fixes the value of TESTLENGTH for test 4 at 64, or 192 encipherments or decipherments.

4. SUMMARY AND CONCLUSIONS

A variety of maintenance tests for DES devices in the field have been described, ranging from testing for stuck-faults in the output to a full test of the DES device. The tests are simple and efficient and can be executed from a small ROM program on-board with the DES. Recommended testing environments include:

1. manufacturer's assembly-line checkout for DES devices,

2. user acceptance test for newly acquired and recently repaired devices,

3. field-maintenance service testing, and

4. in-service testing of DES devices to maintain the integrity of the encryption system.

Users of DES devices can choose one of the four tests described, depending on their evaluation of which test is most convenient and meaningful in the given operational environment. However test 4, the complete functionality test, encompasses all the other tests and is hence the best test to use whenever practicable.

During each test there is no verification of intermediate values, just a check of the final output for correctness. Thus there is a possibility for undetected, self-cancelling double errors that these tests are not designed to detect. Many such errors will be detected if they occur in different functional units of the DES, but the user of these tests should be alert to the possibility, however remote, that such errors might not be detected.

5. Appendix A: The DES Algorithm Specification

For the convenience of the reader, this appendix contains a complete specification of the parameters involved in the definition of the DES algorithm.

The DES acts on a 64 bit block of plaintext, which is first permuted by IP:

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

(e. g., bit one of the output is bit 58 of the input and bit two is bit 50, etc.)

The result is separated into two 32 bit registers, L and R, and then passed through the sixteen rounds. The final 64 bit result is operated on by the inverse of IP, IP^{-1}:

IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

The round keys K_n are determined by the key schedule. There are three parameters to be specified, PC1, PC2 and the shift schedule:

PC1

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

PC2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

and the shift schedule is:

Iteration	Number of shifts
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

For a single round the expansion operator E and the permutation P need to be specified:

E

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

P

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

There remain only the S-boxes:

S_1

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

S_2

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

S_3

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

S_4

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

S_5

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

S_6

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

S_7

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

S_8

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

The reader is referred to [3] for the official specification of these parameters.

6. Appendix B: The Gram-Schmidt Algorithm

Given an arbitrary set $k_1, k_2, k_3, \ldots$ of n-dimensional vectors, we will construct a maximal linearly-independent subset of vectors using the Gram-Schmidt process. The method is to assume that the vectors k_i are linearly independent and to use the Gram-Schmidt process to construct an orthogonal set as follows. We will use the notation $\langle x|$ for a row vector and $|x\rangle$ for a column vector, $\langle x|y\rangle$ for inner product and $|x|$ for the norm of a vector. Let

$$u_1 = k_1$$

$$u_2 = k_2 - \langle u_1|k_2\rangle/|u_1|^2 \, u_1$$

$$u_3 = k_3 - \langle u_1|k_3\rangle/|u_1|^2 \, u_1 - \langle u_2|k_3\rangle/|u_2|^2 \, u_2$$

$$u_4 = \ldots$$

etc.

If at any stage in this process u_i is equal to zero then omit k_i and continue. This process will construct a linearly independent subset of the original set, which may not necessarily be maximal, but if the original set is sufficiently large the process will terminate after n vectors have been selected, and the subset is thus maximal.

The required theorem is as follows.

Theorem. $u_i = 0$ if and only if k_i is dependent on the k_j for $j<i$.

Proof. Suppose $u_i = 0$, then k_i is a linear combination of u_j for $j<i$. Since each u_j is a linear combination of k_l for $l<j$, we have that k_i is a linear combination of k_j for $j<i$.

Conversely, if k_i depends on the k_j for $j<i$, then k_i also depends on the u_j for $j<i$. Hence each $\langle u_j|k_i\rangle$ is the coefficient of u_j in the expansion of k_i in the vectors u_j. Thus the sum of the terms subtracted from k_i in the Gram-Schmidt process actually equals k_i, so $u_i = 0$.

In this form the Gram-Schmidt test is used to ensure that sufficiently many pseudo-random vectors have been presented to each linear element of the DES to guarantee complete testing. Appendix C addresses the question of how many random vectors must be examined on the average in order to ensure that we have a maximal linearly independent set.

7. Appendix C: Pseudo-random Testing of Linear Devices

A Markov-chain model is used to compute the mean and standard deviation of the number of pseudo-random input vectors that must be presented to a linear device to ensure that a basis has been presented to the device, thus testing it completely.

The first block of input may be either a zero or a non-zero block. In the second case the block will be in the set, while in the first we repeat until we obtain a non-zero block. Once we have a non-zero block, we repeat until we obtain another one, in which case we have two vectors in the set. However we may also obtain the same block again, or the zero block. With two vectors in the set a new situation arises, since the next vector may be zero, or a repeat of a vector already in the set or a new vector in the span of those already in the set. In general, a k-dimensional problem will be represented by a k+1 state Markov chain. This is a finite, ergodic absorbing Markov process, so must terminate [7; theorem 3.3.5], hence, in due course, we obtain a basis.

Theorem 1. For the Markov chain described above, the transition probability state i to state i is

$$1/2^{(k-i)}.$$

Proof. Let N(i) denote the number of vectors not in the linearly independent set and not zero, but in the span of the set. It suffices to show that $N(i) = 2^1 - i - 1$. It's immediate that

$$N(i) = 1 + SUM(j=2,\ i-1)\ (),$$

where () denotes the number of combinations of i things taken j at a time, and the argument follows by induction on i. The inductive step uses the additive formula [10; 1.2.6D(9)].

In the next theorem we compute the mean number of transitions for this Markov chain to be absorbed.

Theorem 2. The expected number of transitions to absorption for the above Markov chain is, for k>1,

$$E_k = S_k + [1/(2^k - 1)] + 1,$$

where S_k = SUM(i=1, k-1)[$2^i/(2^i - 1)$].

Proof. By induction on k. For the case k=2, we have

$$(I-Q)^{-1} = \begin{matrix} 4/3 & 2 \\ 0 & 2, \end{matrix}$$

so, assuming a start with a non-zero element, the expected number of transitions to absorption S_k is the sum of the last row of the fundamental matrix, or 2. The inductive step follows from the definition of the Markov chain. Now E_k is equal to one for the first state plus the probability of starting without a non-zero element times the mean number of transitions to absorption given a start without a non-zero element plus the probability of starting with a non-zero element times the mean number of transitions given a start with a non-zero element, or

$$E_k = S_k + [1/(2^k - 1)] + 1,$$

where all the states except the first are lumped to give a two state Markov chain with transition matrix

$$\begin{matrix} 1 & 0 \\ 1-1/2^k & 1/2^k \end{matrix}$$

with $Q = 1 - 1/2^k$, so the fundamental matrix is $2^k/(2^k-1)$. This is precisely the mean number of transitions required to get out of the zero state.

We now derive an asymptotic estimate to the above formula.

Theorem 4. The average number of vectors that must be examined to obtain a basis is asymptotically log n + c + O(1/n), where k is the number of non-zero vectors required to define the system, $n = 2^k$ and c is a constant.

Proof. Rewrite S_k as

$$S_k = \text{SUM}(i=1, k-1)\{1/[1- (1/2^i)]\},$$

to see that, apart from the first few terms, each new term just adds one as k increases, so asymptotically, for some constant c, we have S_k=c+k, and we see that the asymptotic value = log n + c + O(1/n). The value of c is given in [11;5.2.3(19)], the computation being attributed to J. W. Wrench, as approximately 1.606.

Hence if the dimension of the system is k, we need to look at k+2 random vectors on the average to obtain a maximal linearly independent set.

We now compute the standard deviation, realizing that the difference between the average and the minimum value of the parameter is just 1.606, so the standard deviation must be smaller than this. Reference to [7; theorem 3.3.5] shows that the standard deviation is approximately 1.414 for all values of k, as expected. Thus the distribution has a very small variance and we expect to examine about k+3 or k+4 vectors to obtain a k-dimensional basis in a set of k-dimensional random vectors, provided the dimension k is sufficiently large.

REFERENCES

1. Meyer, C., Enciphering Data for Secure Transmission, Computer Design, (April, 1974)129-34.

2. Meyer, C. and W. Tuchman, Pseudo-random Codes Can Be Cracked, Elect. Design, vol. 23(1972)74-6.

3. Data Encryption Standard, FIPS PUB 46, Jan. 15, 1977.

4. Grossman, E. and B. Tuckerman, Analysis of a Feistel-like Cipher Weakened by Having No Rotating Key, IBM Rpt c6375, 1977.

5. Gait, J., A New Non-Linear Pseudo-random Number Generator, IEEE Transactions on Software Engineering, Sept., 1977.

6. Bright, H. and R. Ennison, Cryptography Using Modular Software Elements, National Computer Conf., 1976, 113-23.

7. Kemeny, J. and J. Snell, Finite Markov Chains, Van Nostrand, Princeton, NJ, 1965.

8. Gait, J., Validating the Correctness of Hardware Implementations of the NBS Data Encryption Standard, NBS Special Pub. 500-20, 1977.

9. Gait, J., Encryption Standard: Validating Hardware Techniques, NBS Dimensions, July, 1978, 22-23.

10. Knuth, D., Fundamental Algorithms, Addison Wesley, 1968, Reading, Mass.

11. Knuth, D., Sorting and Searching, Addison Wesley, 1973, Reading, Mass.

NBS-114A (REV. 9-78)

U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET	1. PUBLICATION OR REPORT NO. NBS SP 500-61	2. Gov't. Accession No.	3. Recipient's Accession No.

4. TITLE AND SUBTITLE COMPUTER SCIENCE & TECHNOLOGY: MAINTENANCE TESTING FOR THE DATA ENCRYPTION STANDARD	5. Publication Date August 1980 6. Performing Organization Code
7. AUTHOR(S) Jason Gait	8. Performing Organ. Report No.
9. PERFORMING ORGANIZATION NAME AND ADDRESS NATIONAL BUREAU OF STANDARDS DEPARTMENT OF COMMERCE WASHINGTON, DC 20234	10. Project/Task/Work Unit No. 11. Contract/Grant No.
12. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (Street, City, State, ZIP) Same as above	13. Type of Report & Period Covered Final 14. Sponsoring Agency Code

15. SUPPLEMENTARY NOTES
Library of Congress Number: 80-600105

☐ Document describes a computer program; SF-185, FIPS Software Summary, is attached.

16. ABSTRACT *(A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here.)*

This publication describes the design of maintenance tests for the Federal Information Processing Data Encryption Standard (DES). The test consists of an iterative procedure that completely tests the operation of DES devices by using a small program and minimum data. The tests are designed to be independent of implementation and to be fast enough to test devices during actual operation. The tests are defined as four stopping points in a general testing process, and satisfy four testing requirements depending on the thoroughness of testing desired.

17. KEY WORDS *(six to twelve entries; alphabetical order; capitalize only the first letter of the first key word unless a proper name; separated by semicolons)*

Communications security; computer security; cryptography; data encryption standard; in-service testing; maintenance tests; Monte-Carlo testing; stuck-fault testing; test cases; validation vs maintenance

18. AVAILABILITY ☒ Unlimited ☐ For Official Distribution. Do Not Release to NTIS ☒ Order From Sup. of Doc., U.S. Government Printing Office, Washington, DC 20402 ☐ Order From National Technical Information Service (NTIS), Springfield, VA. 22161	19. SECURITY CLASS (THIS REPORT) UNCLASSIFIED 20. SECURITY CLASS (THIS PAGE) UNCLASSIFIED	21. NO. OF PRINTED PAGES 29 22. Price $2.00

USCOMM-DC

NBS TECHNICAL PUBLICATIONS

PERIODICALS

JOURNAL OF RESEARCH—The Journal of Research of the National Bureau of Standards reports NBS research and development in those disciplines of the physical and engineering sciences in which the Bureau is active. These include physics, chemistry, engineering, mathematics, and computer sciences. Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Bureau's technical and scientific programs. As a special service to subscribers each issue contains complete citations to all recent Bureau publications in both NBS and non-NBS media. Issued six times a year. Annual subscription: domestic $13; foreign $16.25. Single copy, $3 domestic; $3.75 foreign.

NOTE: The Journal was formerly published in two sections: Section A "Physics and Chemistry" and Section B "Mathematical Sciences."

DIMENSIONS/NBS—This monthly magazine is published to inform scientists, engineers, business and industry leaders, teachers, students, and consumers of the latest advances in science and technology, with primary emphasis on work at NBS. The magazine highlights and reviews such issues as energy research, fire protection, building technology, metric conversion, pollution abatement, health and safety, and consumer product performance. In addition, it reports the results of Bureau programs in measurement standards and techniques, properties of matter and materials, engineering standards and services, instrumentation, and automatic data processing. Annual subscription: domestic $11; foreign $13.75.

NONPERIODICALS

Monographs—Major contributions to the technical literature on various subjects related to the Bureau's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NBS, NBS annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a worldwide program coordinated by NBS under the authority of the National Standard Data Act (Public Law 90-396).

NOTE: The principal publication outlet for the foregoing data is the Journal of Physical and Chemical Reference Data (JPCRD) published quarterly for NBS by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements available from ACS, 1155 Sixteenth St., NW, Washington, DC 20056.

Building Science Series—Disseminates technical information developed at the Bureau on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NBS under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NBS administers this program as a supplement to the activities of the private sector standardizing organizations.

Consumer Information Series—Practical information, based on NBS research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

Order the **above** *NBS publications from: Superintendent of Documents, Government Printing Office, Washington, DC 20402.*

Order the **following** *NBS publications—FIPS and NBSIR's—from the National Technical Information Services, Springfield, VA 22161.*

Federal Information Processing Standards Publications (FIPS PUB)—Publications in this series collectively constitute the Federal Information Processing Standards Register. The Register serves as the official source of information in the Federal Government regarding standards issued by NBS pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NBS Interagency Reports (NBSIR)—A special series of interim or final reports on work performed by NBS for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Services, Springfield, VA 22161, in paper copy or microfiche form.

BIBLIOGRAPHIC SUBSCRIPTION SERVICES

The following current-awareness and literature-survey bibliographies are issued periodically by the Bureau:

Cryogenic Data Center Current Awareness Service. A literature survey issued biweekly. Annual subscription: domestic $35; foreign $45.

Liquefied Natural Gas. A literature survey issued quarterly. Annual subscription: $30.

Superconducting Devices and Materials. A literature survey issued quarterly. Annual subscription: $45. Please send subscription orders and remittances for the preceding bibliographic services to the National Bureau of Standards, Cryogenic Data Center (736) Boulder, CO 80303.