

Triple DES Monte Carlo (Modes) Test Sample Results

This file contains a list of values that can be used in verifying the correctness of Monte Carlo (Modes) Test implementations. A list of values for every combination of mode of operation, state, and keying option supported by Triple DES is included.

Note the use of these values does not take the place of validation obtained through the Cryptographic Module Validation Program. To validate an implementation of Triple DES, a vendor must submit their implementation to one of the accredited validation laboratories. Upon successful validation, a validation certificate is issued for that implementation. (See Special Publication 800-20 *Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures* for details.)

Input File Format:

Included in this zip file are input files to be used for every mode of operation supported by Triple DES. The modes of operation, number of keys, and name of the file containing the input data is as follows:

MODE(S) OF OPERATION	NUMBER OF KEYS	FILE NAME
ECB	1	SAMPLEECB1.TXT
	2	SAMPLEECB2.TXT
	3	SAMPLEECB3.TXT
CBC, 64-bit CFB, 64-bit CFB-P, OFB, OFB-I	1	SAMPLE1.TXT
	2	SAMPLE2.TXT
	3	SAMPLE3.TXT
1-bit CFB, 1-bit CFBP	1	SAMPLECFB11.TXT
	2	SAMPLECFB12.TXT
	3	SAMPLECFB13.TXT
8-bit CFB, 8-bit CFBP	1	SAMPLECFB81.TXT
	2	SAMPLECFB82.TXT
	3	SAMPLECFB83.TXT

The input data used in these files is as follows:

Number of keys: 1, 2, or 3

If number of keys = 1:

Key 1: 0123456789abcdef
Key 2: 0123456789abcdef
Key 3: 0123456789abcdef

If number of keys = 2:

Key 1: 0123456789abcdef
Key 2: 23456789abcdef01
Key 3: 0123456789abcdef

If number of keys = 3:

Key 1: 0123456789abcdef
Key 2: 23456789abcdef01
Key 3: 456789abcdef0123

IV (if applicable): 1234567890abcdef

Input 1: 4e6f772069732074

Input 2(only for CBC-I):68652074696d6520

Input 3(only for CBC-I):666f7220616c6c20

If a mode of operation requires IV2 and IV3, these IVs are generated in the code and are based on the value of IV in the input data.

For example, SAMPLE1.TXT contains the following information. The 1 indicates one key value will be used for all three keys. These keys are shown on lines 2, 3, and 4. The IV is on line 5 and the DATA is on line 6:

```
1
0123456789abcdef
0123456789abcdef
0123456789abcdef
1234567890abcdef
4e6f772069732074
```

Output Results:

The following chart depicts the resulting values for iteration 1 and 2 of the Monte Carlo tests when using the indicated input data. The information is organized by mode of operation, state, number of keys, and results from iteration 1 and 2.

MODE	STATE	NUMBER OF KEYS	RESULTS FROM MONTE CARLO	
			ITERATION 0	ITERATION 1
ECB	ENCRYPT	1	KEY1 = 0123456789abcdef KEY2 = 0123456789abcdef KEY3 = 0123456789abcdef PLAINTEXT = 4e6f772069732074 CIPHERTEXT = 6a2a19f41eca854b	KEY1 = 6b085d92976149a4 KEY2 = 6b085d92976149a4 KEY3 = 6b085d92976149a4 PLAINTEXT = 6a2a19f41eca854b CIPHERTEXT = ce5d6c7b63177c18
		2	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 0123456789abcdef PLAINTEXT = 4e6f772069732074 CIPHERTEXT = 03e69f5bfa58eb42	KEY1 = 02c4da3d73f226ad KEY2 = 1cbce0f2bacd3b15 KEY3 = 02c4da3d73f226ad PLAINTEXT = 03e69f5bfa58eb42 CIPHERTEXT = 262a60f9743e1fd8
		3	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 456789abcdef0123 PLAINTEXT = 4e6f772069732074 CIPHERTEXT = dd17e8b8b437d232	KEY1 = dc34addf3d9dlfdc KEY2 = 976d456702cef4fd KEY3 = ad49c2ba0b2f975b PLAINTEXT = dd17e8b8b437d232 CIPHERTEXT = 3145bcfc1c19382f
ECB	DECRYPT	1	KEY1 = 0123456789abcdef KEY2 = 0123456789abcdef KEY3 = 0123456789abcdef CIPHERTEXT = 4e6f772069732074 PLAINTEXT = cdd64f2f9427c15d	KEY1 = cdf40b491c8c0db3 KEY2 = cdf40b491c8c0db3 KEY3 = cdf40b491c8c0db3 CIPHERTEXT = cdd64f2f9427c15d PLAINTEXT = 5bb675e3db3a7f3b
		2	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 0123456789abcdef CIPHERTEXT = 4e6f772069732074 PLAINTEXT = 6996c8fa47a2abeb	KEY1 = 68b58c9dce086704 KEY2 = 529dce3719e9e0da KEY3 = 68b58c9dce086704 CIPHERTEXT = 6996c8fa47a2abeb PLAINTEXT = 6b177e016e6ael2d
		3	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 456789abcdef0123 CIPHERTEXT = 4e6f772069732074 PLAINTEXT = 8325397644091a0a	KEY1 = 83077c10cda2d6e5 KEY2 = 296240fd8c834fcd KEY3 = 8fdac4fbe5ae978f CIPHERTEXT = 8325397644091a0a PLAINTEXT = c67901abdc008c89
CBC	ENCRYPT			

MODE	STATE	NUMBER OF KEYS	RESULTS FROM MONTE CARLO	
			ITERATION 0	ITERATION 1
		1	KEY1 = 0123456789abcdef KEY2 = 0123456789abcdef KEY3 = 0123456789abcdef CV = 1234567890abcdef PLAINTEXT = 4e6f772069732074 CIPHERTEXT = 54f15af6ebe3a4b4	KEY1 = 54d31f916249685b KEY2 = 54d31f916249685b KEY3 = 54d31f916249685b CV = 54f15af6ebe3a4b4 PLAINTEXT = 9452b69f6d1c6aec CIPHERTEXT = b99d8d2036c7f871
		2	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 0123456789abcdef CV = 1234567890abcdef PLAINTEXT = 4e6f772069732074 CIPHERTEXT = 357611565fa18e4d	KEY1 = 34545431d60b43a2 KEY2 = 10675129c8832c34 KEY3 = 34545431d60b43a2 CV = 357611565fa18e4d PLAINTEXT = 332237a1624fc335 CIPHERTEXT = 8474ec4db00b7ee3
		3	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 456789abcdef0123 CV = 1234567890abcdef PLAINTEXT = 4e6f772069732074 CIPHERTEXT = cb191f85d1ed8439	KEY1 = cb3b5be3584649d6 KEY2 = 0198949bda6eb97c KEY3 = e3ad6d028c2557ec CV = cb191f85d1ed8439 PLAINTEXT = 22dcf21270a2577c CIPHERTEXT = 3d3bad4173e6c47e
CBC	DECRYPT	1	KEY1 = 0123456789abcdef KEY2 = 0123456789abcdef KEY3 = 0123456789abcdef CV = 1234567890abcdef CIPHERTEXT = 4e6f772069732074 PLAINTEXT = 129f40b9d20056b3	KEY1 = 13bc04df5bab9b5d KEY2 = 13bc04df5bab9b5d KEY3 = 13bc04df5bab9b5d CV = f2190c0db43efd11 CIPHERTEXT = 129f40b9d20056b3 PLAINTEXT = afeled3bfcacd83b
		2	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 0123456789abcdef CV = 1234567890abcdef CIPHERTEXT = 4e6f772069732074 PLAINTEXT = 470efc9a6b8ee393	KEY1 = 462cb9fde3252f7c KEY2 = 108f0bdaa77f7c9d KEY3 = 462cb9fde3252f7c CV = 33cb6d520db2929d CIPHERTEXT = 470efc9a6b8ee393 PLAINTEXT = eeaca70ale0f7f69
		3	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 456789abcdef0123 CV = 1234567890abcdef CIPHERTEXT = 4e6f772069732074 PLAINTEXT = c5cecf63ecec514c	KEY1 = c4ec8a0464469da2 KEY2 = f7ce1cdcc14619b6 KEY3 = 971fe3d6406b80a4 CV = d48a7b546b8af7b6 CIPHERTEXT = c5cecf63ecec514c PLAINTEXT = 211b21752925fbce

MODE	STATE	NUMBER OF KEYS	RESULTS FROM MONTE CARLO	
			ITERATION 0	ITERATION 1
CBC-I	ENCRYPT	1	KEY1 = 0123456789abcdef KEY2 = 0123456789abcdef KEY3 = 0123456789abcdef CV1 = 1234567890abcdef CV2 = 6789abcde6012344 CV3 = bcdf01233b567899 PLAINTEXT1 = 4e6f772069732074 PLAINTEXT2 = 68652074696d6520 PLAINTEXT3 = 666f7220616c6c20 CIPHERTEXT1 = 54f15af6ebe3a4b4 CIPHERTEXT2 = 1830e4319fab94d0 CIPHERTEXT3 = c2679abf469c33eb	KEY1 = 54d31f916249685b KEY2 = 54d31f916249685b KEY3 = 54d31f916249685b CV1 = 54f15af6ebe3a4b4 CV2 = 1830e4319fab94d0 CV3 = c2679abf469c33eb PLAINTEXT1 = 9452b69f6d1c6aec PLAINTEXT2 = 5e38e47e7f6d8651 PLAINTEXT3 = d1ae483ee14559c8 CIPHERTEXT1 = b99d8d2036c7f871 CIPHERTEXT2 = 1f6e8cbd2d4bc4a0 CIPHERTEXT3 = 57395596cbe63c17
		2	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 0123456789abcdef CV1 = 1234567890abcdef CV2 = 6789abcde6012344 CV3 = bcdf01233b567899 PLAINTEXT1 = 4e6f772069732074 PLAINTEXT2 = 68652074696d6520 PLAINTEXT3 = 666f7220616c6c20 CIPHERTEXT1 = 357611565fa18e4d CIPHERTEXT2 = fa35cc03de95826a CIPHERTEXT3 = 26bc2165f0d6a717	KEY1 = 34545431d60b43a2 KEY2 = 52525e32a7340e32 KEY3 = 34545431d60b43a2 CV1 = 357611565fa18e4d CV2 = fa35cc03de95826a CV3 = 26bc2165f0d6a717 PLAINTEXT1 = 332237a1624fc335 PLAINTEXT2 = 711738ba0cf9e132 PLAINTEXT3 = 069bf645caa5544e CIPHERTEXT1 = 86e246fb8a652e27 CIPHERTEXT2 = acc76c3f2ba08206 CIPHERTEXT3 = 7a86c8b3eda83055
		3	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 456789abcdef0123 CV1 = 1234567890abcdef CV2 = 6789abcde6012344 CV3 = bcdf01233b567899 PLAINTEXT1 = 4e6f772069732074 PLAINTEXT2 = 68652074696d6520 PLAINTEXT3 = 666f7220616c6c20 CIPHERTEXT1 = cb191f85d1ed8439 CIPHERTEXT2 = 6d025f36b2e6241d CIPHERTEXT3 = a197fd91ba4497b8	KEY1 = cb3b5be3584649d6 KEY2 = 1ab3082ab579fedf KEY3 = 75ef0b91f2155b98 CV1 = cb191f85d1ed8439 CV2 = 6d025f36b2e6241d CV3 = a197fd91ba4497b8 PLAINTEXT1 = 22dcf21270a2577c PLAINTEXT2 = 39f66fa21fb410df PLAINTEXT3 = 5ac372eb1341b38f CIPHERTEXT1 = 5ae84dfc16fd7bb6 CIPHERTEXT2 = 19d0e0128abaa073 CIPHERTEXT3 = ed1ae2c4c48b091b

MODE	STATE	NUMBER OF KEYS	RESULTS FROM MONTE CARLO	
			ITERATION 0	ITERATION 1
CBC-I	DECRYPT	1	KEY1 = 0123456789abcdef KEY2 = 0123456789abcdef KEY3 = 0123456789abcdef CV1 = 1234567890abcdef CV2 = 6789abcde6012344 CV3 = bcdf01233b567899 CIPHERTEXT1 = 4e6f772069732074 CIPHERTEXT2 = 68652074696d6520 CIPHERTEXT3 = 666f7220616c6c20 PLAINTEXT1 = 129f40b9d20056b3 PLAINTEXT2 = 1de16f63aebb3102 PLAINTEXT3 = 9615f6c1777c77de	KEY1 = 13bc04df5bab9b5d KEY2 = 13bc04df5bab9b5d KEY3 = 13bc04df5bab9b5d CV1 = f2190c0db43efd11 CV2 = 94b263ee41bc4df9 CV3 = 8fb64c91c84ac1c3 CIPHERTEXT1 = 129f40b9d20056b3 CIPHERTEXT2 = 1de16f63aebb3102 CIPHERTEXT3 = 9615f6c1777c77de PLAINTEXT1 = afe1ed3bfcacd83b PLAINTEXT2 = b99a52984b86cb17 PLAINTEXT3 = e429ab9fbc833801
		2	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 0123456789abcdef CV1 = 1234567890abcdef CV2 = 6789abcde6012344 CV3 = bcdf01233b567899 CIPHERTEXT1 = 4e6f772069732074 CIPHERTEXT2 = 68652074696d6520 CIPHERTEXT3 = 666f7220616c6c20 PLAINTEXT1 = 470efc9a6b8ee393 PLAINTEXT2 = 33bc7c149d96088c PLAINTEXT3 = f7109214d3d8c276	KEY1 = 462cb9fde3252f7c KEY2 = aba8c832f7433bb6 KEY3 = 462cb9fde3252f7c CV1 = 33cb6d520db2929d CV2 = 89edafba5c8fd5b7 CV3 = f7fee0886b936582 CIPHERTEXT1 = 470efc9a6b8ee393 CIPHERTEXT2 = 33bc7c149d96088c CIPHERTEXT3 = f7109214d3d8c276 PLAINTEXT1 = 82eb6cb925baed22 PLAINTEXT2 = 8efe5c65c9c72bc8 PLAINTEXT3 = 437142e60331ab36
		3	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 456789abcdef0123 CV1 = 1234567890abcdef CV2 = 6789abcde6012344 CV3 = bcdf01233b567899 CIPHERTEXT1 = 4e6f772069732074 CIPHERTEXT2 = 68652074696d6520 CIPHERTEXT3 = 666f7220616c6c20 PLAINTEXT1 = c5cecf63ecec514c PLAINTEXT2 = e69d707f667a4477 PLAINTEXT3 = 7843cea950bc1e8f	KEY1 = c4ec8a0464469da2 KEY2 = 2ff88a1092b6b3b0 KEY3 = 7f454a1062c1b662 CV1 = d48a7b546b8af7b6 CV2 = 0dbded98387b5cb0 CV3 = 04e3f1d3c8b394ad CIPHERTEXT1 = c5cecf63ecec514c CIPHERTEXT2 = e69d707f667a4477 CIPHERTEXT3 = 7843cea950bc1e8f PLAINTEXT1 = cacf3278109cc6c0 PLAINTEXT2 = 053cf6df14a85379 PLAINTEXT3 = b6a934dbf2e76617
CFB 1-bit	ENCRYPT	1	KEY1 = 0123456789abcdef KEY2 = 0123456789abcdef KEY3 = 0123456789abcdef CV1 = 1234567890abcdef PLAINTEXT = 1 CIPHERTEXT = 1	KEY1 = 15400ecd4370d0e6 KEY2 = 15400ecd4370d0e6 KEY3 = 15400ecd4370d0e6 CV1 = 14634aabcdbd1d09 PLAINTEXT = 1 CIPHERTEXT = 0

MODE	STATE	NUMBER OF KEYS	RESULTS FROM MONTE CARLO	
			ITERATION 0	ITERATION 1
		2	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 0123456789abcdef CV1 = 1234567890abcdef PLAINTEXT = 1 CIPHERTEXT = 0	KEY1 = d30d6dea7fab977a KEY2 = 0b4a1c021c100ec4 KEY3 = d30d6dea7fab977a CV1 = d32e288df7015b94 PLAINTEXT = 1 CIPHERTEXT = 1
		3	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 456789abcdef0123 CV1 = 1234567890abcdef PLAINTEXT = 1 CIPHERTEXT = 1	KEY1 = c4519e9710f1a7a7 KEY2 = 8ca1201310e5a4d6 KEY3 = a8311ada19f40bd5 CV1 = c472dbf0995b6b49 PLAINTEXT = 0 CIPHERTEXT = 0
CFB 1-bit	DECRYPT	1	KEY1 = 0123456789abcdef KEY2 = 0123456789abcdef KEY3 = 0123456789abcdef CV1 = 1234567890abcdef CIPHERTEXT = 1 PLAINTEXT = 1	KEY1 = 9d403d2a020dd657 KEY2 = 9d403d2a020dd657 KEY3 = 9d403d2a020dd657 CV1 = 7421d73b79620968 CIPHERTEXT = 1 PLAINTEXT = 0
		2	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 0123456789abcdef CV1 = 1234567890abcdef CIPHERTEXT = 1 PLAINTEXT = 1	KEY1 = 40f10189e5fe4f25 KEY2 = 0e20a454d0b54a62 KEY3 = 40f10189e5fe4f25 CV1 = 3f4ec3a5db3381b9 CIPHERTEXT = 0 PLAINTEXT = 1
		3	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 456789abcdef0123 CV1 = 1234567890abcdef CIPHERTEXT = 1 PLAINTEXT = 1	KEY1 = b30b9858ad2f6825 KEY2 = c868adb06ef7b02a KEY3 = 0b0edf02d5262680 CV1 = 6ee7b4ealc839c46 CIPHERTEXT = 1 PLAINTEXT = 0
CFB 8-bit	ENCRYPT	1	KEY1 = 0123456789abcdef KEY2 = 0123456789abcdef KEY3 = 0123456789abcdef CV1 = 1234567890abcdef PLAINTEXT = 7f CIPHERTEXT = a8	KEY1 = bf8fa7941f2c5846 KEY2 = bf8fa7941f2c5846 KEY3 = bf8fa7941f2c5846 CV1 = beace3f2968695a8 PLAINTEXT = 38 CIPHERTEXT = 5e

MODE	STATE	NUMBER OF KEYS	RESULTS FROM MONTE CARLO	
			ITERATION 0	ITERATION 1
		2	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 0123456789abcdef CV1 = 1234567890abcdef PLAINTEXT = 7f CIPHERTEXT = 21	KEY1 = 8aa8765e6eb662ce KEY2 = 20cead29e65831f4 KEY3 = 8aa8765e6eb662ce CV1 = 8a8b3238e71cae21 PLAINTEXT = f4 CIPHERTEXT = d3
		3	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 456789abcdef0123 CV1 = 1234567890abcdef PLAINTEXT = 7f CIPHERTEXT = 24	KEY1 = 6723fe76addafdcdb KEY2 = 949b587591bc984a KEY3 = 7c4380ece67fd6cd CV1 = 6701bb1124713024 PLAINTEXT = 4a CIPHERTEXT = 40
CFB 8-bit	DECRYPT	1	KEY1 = 0123456789abcdef KEY2 = 0123456789abcdef KEY3 = 0123456789abcdef CV1 = 1234567890abcdef CIPHERTEXT = 7f PLAINTEXT = c9	KEY1 = 045bd07025406226 KEY2 = 045bd07025406226 KEY3 = 045bd07025406226 CV1 = 6c691085933ed57b CIPHERTEXT = b2 PLAINTEXT = 86
		2	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 0123456789abcdef CV1 = 1234567890abcdef CIPHERTEXT = 7f PLAINTEXT = 92	KEY1 = 43fde5325223ef7c KEY2 = a4758fb9315eba0e KEY3 = 43fde5325223ef7c CV1 = 0b49963763b93013 CIPHERTEXT = 81 PLAINTEXT = 5d
		3	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 456789abcdef0123 CV1 = 1234567890abcdef CIPHERTEXT = 7f PLAINTEXT = 1a	KEY1 = 0b340b3792d3fef4 KEY2 = f208cbc4570b08ef KEY3 = d32926d6370ec7f8 CV1 = d6ddca85d4ceb784 CIPHERTEXT = 9e PLAINTEXT = 56
CFB 64-bit	ENCRYPT	1	KEY1 = 0123456789abcdef KEY2 = 0123456789abcdef KEY3 = 0123456789abcdef CV1 = 1234567890abcdef PLAINTEXT = 4e6f772069732074 CIPHERTEXT = 15db41a26f22840d	KEY1 = 15f804c4e68949e3 KEY2 = 15f804c4e68949e3 KEY3 = 15f804c4e68949e3 CV1 = 15db41a26f22840d PLAINTEXT = 3e14565551353165 CIPHERTEXT = d58136876016c161

MODE	STATE	NUMBER OF KEYS	RESULTS FROM MONTE CARLO	
			ITERATION 0	ITERATION 1
		2	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 0123456789abcdef CV1 = 1234567890abcdef PLAINTEXT = 4e6f772069732074 CIPHERTEXT = 67f8369d10d093ac	KEY1 = 67da73fb987a5e43 KEY2 = 62155701450bf49d KEY3 = 67da73fb987a5e43 CV1 = 67f8369d10d093ac PLAINTEXT = 41513189eec61b9c CIPHERTEXT = e44542717420f99c
		3	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 456789abcdef0123 CV1 = 1234567890abcdef PLAINTEXT = 4e6f772069732074 CIPHERTEXT = 83c4778e887756c9	KEY1 = 83e632e901dc9b26 KEY2 = 7afb2a8c3da7646b KEY3 = a2570b61ef54ae73 CV1 = 83c4778e887756c9 PLAINTEXT = 59be4d04976a8b6a CIPHERTEXT = b28e2baaf0a992e7
CFB 64- bit	DECRYPT	1	KEY1 = 0123456789abcdef KEY2 = 0123456789abcdef KEY3 = 0123456789abcdef CV1 = 1234567890abcdef CIPHERTEXT = 4e6f772069732074 PLAINTEXT = 897f9df7c00b7e02	KEY1 = 895dd99149alb3ec KEY2 = 895dd99149alb3ec KEY3 = 895dd99149alb3ec CV1 = d9c2868fed1aele CIPHERTEXT = 50bd1b782d11901c PLAINTEXT = 325839b43eeca651
		2	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 0123456789abcdef CV1 = 1234567890abcdef CIPHERTEXT = 4e6f772069732074 PLAINTEXT = 299fdc474911f8c7	KEY1 = 29bc9820c1ba3429 KEY2 = fb402004322f16c8 KEY3 = 29bc9820c1ba3429 CV1 = 8a327cdb386f1364 CIPHERTEXT = a3ada09c717eeba3 PLAINTEXT = 451e85cd8bde2221
		3	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 456789abcdef0123 CV1 = 1234567890abcdef CIPHERTEXT = 4e6f772069732074 PLAINTEXT = 68ae9637c6bcdeb4	KEY1 = 688cd3514f16135b KEY2 = 9d466ec1ba047ae6 KEY3 = 26c25d57b3f27a19 CV1 = 5617b637a5436c12 CIPHERTEXT = 3eb9200063ffb2a6 PLAINTEXT = b9e279d28ebc2f70
CFB-P 1-bit	ENCRYPT	1	KEY1 = 0123456789abcdef KEY2 = 0123456789abcdef KEY3 = 0123456789abcdef CV1 = 1234567890abcdef CV2 = 6789abcde6012344 CV3 = bcdf01233b567899 TEXT = 1 RESULT = 1	KEY1 = 08fd4698dce0a8b9 KEY2 = 08fd4698dce0a8b9 KEY3 = 08fd4698dce0a8b9 CV1 = c23780ff95129955 CV2 = 178cd654ea67eeaa CV3 = 6ce22baa3fbd43ff TEXT = 0 RESULT = 0

MODE	STATE	NUMBER OF KEYS	RESULTS FROM MONTE CARLO	
			ITERATION 0	ITERATION 1
		2	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 0123456789abcdef CV1 = 1234567890abcdef CV2 = 6789abcde6012344 CV3 = bcdf01233b567899 TEXT = 1 RESULT = 0	KEY1 = 07861fdc32025738 KEY2 = 3201e68f07df2692 KEY3 = 07861fdc32025738 CV1 = c1a956aeaaaa66b4 CV2 = 16feac04443fbc09 CV3 = 6c5401599995115e TEXT = 0 RESULT = 1
		3	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 456789abcdef0123 CV1 = 1234567890abcdef CV2 = 6789abcde6012344 CV3 = bcdf01233b567899 TEXT = 1 RESULT = 0	KEY1 = b001b3bfd5cda80b KEY2 = 2f51eccdc794b5f7 KEY3 = 491a3ecd1a4cda98 CV1 = ec08fdb65759d938 CV2 = 415e530bacaf2e8d CV3 = 96b3a861020483e2 TEXT = 1 RESULT = 1
CFB-P 1-bit	DECRYPT	1	KEY1 = 0123456789abcdef KEY2 = 0123456789abcdef KEY3 = 0123456789abcdef CV1 = 1234567890abcdef CV2 = 6789abcde6012344 CV3 = bcdf01233b567899 TEXT = 1 RESULT = 0	KEY1 = 2f191a6b515d7016 KEY2 = 2f191a6b515d7016 KEY3 = 2f191a6b515d7016 CV1 = 06858d412deb5aea CV2 = 5bdae2968340b03f CV3 = b13037ebd8960594 TEXT = 0 RESULT = 0
		2	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 0123456789abcdef CV1 = 1234567890abcdef CV2 = 6789abcde6012344 CV3 = bcdf01233b567899 TEXT = 1 RESULT = 0	KEY1 = 800d0bbfae453bea KEY2 = 106d7f79572601ec KEY3 = 800d0bbfae453bea CV1 = e006b16df8a96b7e CV2 = 355c06c34dfec0d3 CV3 = 8ab15c18a3541628 TEXT = 0 RESULT = 1
		3	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 456789abcdef0123 CV1 = 1234567890abcdef CV2 = 6789abcde6012344 CV3 = bcdf01233b567899 TEXT = 1 RESULT = 0	KEY1 = 29941316346d9ba2 KEY2 = 38f4fb801692974c KEY3 = 7fa451ece6f7e3b6 CV1 = c61b4c8bdaef7370 CV2 = 1b70a1e13044c8c5 CV3 = 70c5f736859a1e1a TEXT = 0 RESULT = 1

MODE	STATE	NUMBER OF KEYS	RESULTS FROM MONTE CARLO	
			ITERATION 0	ITERATION 1
CFB-P 8-bit	ENCRYPT	1	KEY1 = 0123456789abcdef KEY2 = 0123456789abcdef KEY3 = 0123456789abcdef CV1 = 1234567890abcdef CV2 = 6789abcde6012344 CV3 = bcdf01233b567899 TEXT = 7f RESULT = d0	KEY1 = e95b766b644a3d3e KEY2 = e95b766b644a3d3e KEY3 = e95b766b644a3d3e CV1 = 8982e879330cedd0 CV2 = ded83dce88624325 CV3 = 342d9323ddb7987a TEXT = 5f RESULT = 15
		2	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 0123456789abcdef CV1 = 1234567890abcdef CV2 = 6789abcde6012344 CV3 = bcdf01233b567899 TEXT = 7f RESULT = d2	KEY1 = b5d3a2e5b91a133d KEY2 = a2bf25026740648c KEY3 = b5d3a2e5b91a133d CV1 = 8a8cb4f0e68230d2 CV2 = dfe20a463bd78627 CV3 = 35375f9b912cdb7c TEXT = 8c RESULT = ca
		3	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 456789abcdef0123 CV1 = 1234567890abcdef CV2 = 6789abcde6012344 CV3 = bcdf01233b567899 TEXT = 7f RESULT = ba	KEY1 = 5867fd1c19584a54 KEY2 = 85f770e9a729f1b6 KEY3 = 45259b0e23ce40da CV1 = 1fb75845b87b90ba CV2 = 750cad9b0dd0e60f CV3 = ca6202f063263b64 TEXT = e5 RESULT = ff
CFB-P 8-bit	DECRYPT	1	KEY1 = 0123456789abcdef KEY2 = 0123456789abcdef KEY3 = 0123456789abcdef CV1 = 1234567890abcdef CV2 = 6789abcde6012344 CV3 = bcdf01233b567899 TEXT = 7f RESULT = a8	KEY1 = 5b231a0bf8167946 KEY2 = 5b231a0bf8167946 KEY3 = 5b231a0bf8167946 CV1 = fe88c59e9ec0add4 CV2 = 53de1af3f4160329 CV3 = a9337049496b587e TEXT = 7c RESULT = c9
		2	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 0123456789abcdef CV1 = 1234567890abcdef CV2 = 6789abcde6012344 CV3 = bcdf01233b567899 TEXT = 7f RESULT = c3	KEY1 = 6b4cea25d0152c2c KEY2 = 31a8a8c44fb36162 KEY3 = 6b4cea25d0152c2c CV1 = ad23412a44eba9ae CV2 = 0278967f9a40fff03 CV3 = 57cdebd4ef965458 TEXT = 6d RESULT = d5

MODE	STATE	NUMBER OF KEYS	RESULTS FROM MONTE CARLO	
			ITERATION 0	ITERATION 1
		3	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 456789abcdef0123 CV1 = 1234567890abcdef CV2 = 6789abcde6012344 CV3 = bcdf01233b567899 TEXT = 7f RESULT = 09	KEY1 = fd493246c76e68e6 KEY2 = 6dd6ae1934df89ba KEY3 = 98bc79491aa10b9e CV1 = 0562d8244e391836 CV2 = 5ab82d79a38e6d8b CV3 = b00d82cef8e3c2e0 TEXT = 3f RESULT = 04
CFB-P 64-bit	ENCRYPT	1	KEY1 = 0123456789abcdef KEY2 = 0123456789abcdef KEY3 = 0123456789abcdef CV1 = 1234567890abcdef CV2 = 6789abcde6012344 CV3 = bcdf01233b567899 TEXT = 4e6f772069732074 RESULT = 8a8ed551fe56ee1e	KEY1 = 8aad913776fd23f1 KEY2 = 8aad913776fd23f1 KEY3 = 8aad913776fd23f1 CV1 = 8a8ed551fe56ee1e CV2 = dfe42aa753ac4373 CV3 = 35397ffca90198c8 TEXT = 0b8675e3d7c1a572 RESULT = e01ca1f01713fea6
		2	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 0123456789abcdef CV1 = 1234567890abcdef CV2 = 6789abcde6012344 CV3 = bcdf01233b567899 TEXT = 4e6f772069732074 RESULT = c5eeb999abcf6d27	KEY1 = c4cdfdfe2364a1c8 KEY2 = 26760bd6aebce389 KEY3 = c4cdfdfe2364a1c8 CV1 = c5eeb999abcf6d27 CV2 = 1b440eef0124c27c CV3 = 70996444567a17d1 TEXT = 9414a399805058dc RESULT = 00c9a5a8d59c39d1
		3	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 456789abcdef0123 CV1 = 1234567890abcdef CV2 = 6789abcde6012344 CV3 = bcdf01233b567899 TEXT = 4e6f772069732074 RESULT = e363fcfb112fdcf1	KEY1 = e340b99d9885101f KEY2 = 38daad8f29615815 KEY3 = 8f9e51c194a7547a CV1 = e363fcfb112fdcf1 CV2 = 38b9525066853246 CV3 = 8e0ea7a5bbda879b TEXT = fdfa8443e56b49ca RESULT = 2f02b9ddab5a770c
CFB-P 64-bit	DECRYPT	1	KEY1 = 0123456789abcdef KEY2 = 0123456789abcdef KEY3 = 0123456789abcdef CV1 = 1234567890abcdef CV2 = 6789abcde6012344 CV3 = bcdf01233b567899 TEXT = 4e6f772069732074 RESULT = 5bda341645ad4eda	KEY1 = 5bf87070cd078334 KEY2 = 5bf87070cd078334 KEY3 = 5bf87070cd078334 CV1 = 792a0652434e2903 CV2 = ce7f5ba798a37e58 CV3 = 23d4b0fcedf8d3ad TEXT = 22f0324406e367d9 RESULT = 675e6fbdd51c32c5

MODE	STATE	NUMBER OF KEYS	RESULTS FROM MONTE CARLO	
			ITERATION 0	ITERATION 1
		2	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 0123456789abcdef CV1 = 1234567890abcdef CV2 = 6789abcde6012344 CV3 = bcdf01233b567899 TEXT = 4e6f772069732074 RESULT = 4253c75b94830738	KEY1 = 4370833d1c29cbd6 KEY2 = b3cef725f4dfbf3b KEY3 = 4370833d1c29cbd6 CV1 = 2f5eeef6572f596 CV2 = 84b44404bac84aeb CV3 = da09995a101da040 TEXT = 6d0d29f4f1f1f2ae RESULT = 915992a3870c45f3
		3	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 456789abcdef0123 CV1 = 1234567890abcdef CV2 = 6789abcde6012344 CV3 = bcdf01233b567899 TEXT = 4e6f772069732074 RESULT = b99b723b9bc82bf9	KEY1 = b9b9375d1362e616 KEY2 = 1364c10d5df4a458 KEY3 = d5aef151e979efda CV1 = 34297c48c966cb43 CV2 = 897ed19elebc2098 CV3 = ded426f3741175ed TEXT = 8db20e7352aee0ba RESULT = b44203bb5fd2aef4
OFB	ENCRYPT AND DECRYPT	1	KEY1 = 0123456789abcdef KEY2 = 0123456789abcdef KEY3 = 0123456789abcdef CV = 1234567890abcdef TEXT = 4e6f772069732074 RESULT = 09543701651f9ad2	KEY1 = 08767367ecb5573d KEY2 = 08767367ecb5573d KEY3 = 08767367ecb5573d CV = 934648d64eb7689b TEXT = 21fe5836f364bf2a RESULT = d044aed4a9a27c03
		2	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 0123456789abcdef CV = 1234567890abcdef TEXT = 4e6f772069732074 RESULT = d9592a51bc14e5bd	KEY1 = d97a6e3734bf2952 KEY2 = 796407c79ed0b51c KEY3 = d97a6e3734bf2952 CV = 94fc404db0aa7794 TEXT = c46443a368204c05 RESULT = bbaea7b44cd9c833
		3	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 456789abcdef0123 CV = 1234567890abcdef TEXT = 4e6f772069732074 RESULT = b0bc3ed52644783c	KEY1 = b09e7ab3aeefb5d3 KEY2 = f492458fdca45e9e KEY3 = 4ad3e075ea802040 CV = ad04690f0faa681c TEXT = 61b9698cb0071a9f RESULT = 6222999807d7ff76

MODE	STATE	NUMBER OF KEYS	RESULTS FROM MONTE CARLO	
			ITERATION 0	ITERATION 1
OFB-I	ENCRYPT AND DECRYPT	1	KEY1 = 0123456789abcdef KEY2 = 0123456789abcdef KEY3 = 0123456789abcdef CV1 = 1234567890abcdef CV2 = 6789abcde6012344 CV3 = bcdf01233b567899 TEXT = 4e6f772069732074 RESULT = 0442a5208f527285	KEY1 = 0461e04607f8bf6b KEY2 = 0461e04607f8bf6b KEY3 = 0461e04607f8bf6b CV1 = 776df5c54094da89 CV2 = ccc34bla95ea2fde CV3 = 2218a06feb3f8533 TEXT = bb8edbaaea154f88 RESULT = 6650d0b01db5f473
		2	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 0123456789abcdef CV1 = 1234567890abcdef CV2 = 6789abcde6012344 CV3 = bcdf01233b567899 TEXT = 4e6f772069732074 RESULT = 3e075b0ceb332e01	KEY1 = 3e251f6b6298e3ef KEY2 = 4fcef4f83d25d6bc KEY3 = 3e251f6b6298e3ef CV1 = c5d28d4ab71acd0e CV2 = 1b27e2a00c702263 CV3 = 707d37f561c577b8 TEXT = 5f5ddc29a2cfef7a RESULT = acfd10a333044267
		3	KEY1 = 0123456789abcdef KEY2 = 23456789abcdef01 KEY3 = 456789abcdef0123 CV1 = 1234567890abcdef CV2 = 6789abcde6012344 CV3 = bcdf01233b567899 TEXT = 4e6f772069732074 RESULT = 22d33530d6a016fd	KEY1 = 23f170575e0bda13 KEY2 = 736820e6b9201a62 KEY3 = 70aeb56dc207a7a4 CV1 = 6812aa1b9066927c CV2 = bd67ff70e5bbe7d1 CV3 = 12bd54c63b113d26 TEXT = cddda4829547a485 RESULT = f86a08679bdc09ab