The following is an added requirement of the DES and TDES Validation tests. It should be used in conjunction with SP800-17 and SP800-20.

The Multi-block Message Test (MMT) for DES and TDES

The Multi-block Message Test (MMT) is designed to test the ability of the implementation to process multi-block messages, which require the chaining of information from one block to the next.

The test supplies the IUT with messages that are integral numbers of blocks in length. When testing DES and TDES implementations of the ECB, CBC, OFB and CFB64 modes of operation the block length is 64 bits, for the CFB1 mode of operation the block length is 1 bit, and for the CFB8 mode of operation the block length is 8 bits. For each of the above mentioned modes supported by an IUT, 10 messages are supplied with lengths of $i * blocklength$, where $1 \leq i \leq 10$.

In addition to the 4 modes of operation mentioned above, the TDES algorithm allows pipelined and interleaved modes of operation. When testing the CFB64-P mode of operation the block length is 64 bits, for the CFB1-P mode of operation the block length is 1 bit, and for the CFB8-P mode of operation the block length is 8 bits. For each of the pipelined modes of operation supported by an IUT, 10 messages are supplied with lengths of $i * blocklength$, where $1 \leq i \leq 10$.

The TDES interleaved modes of operation tripartite an input message into three plaintext substreams. Therefore, when testing TDES implementations of the CBC-I and OFB-I modes of operation, the test supplies the IUT with messages that are three times 64 bits (192 bits) to allow integral numbers of blocks to be tested in each of the substreams. For each of the interleaved modes of operation supported by an IUT, 10 messages are supplied with lengths of $\mathbf{3}*(i * blocklength)$, where $1 \leq i \leq 10$.

The REQUEST file for the MMT test contains a series of data sets consisting of three keys, an initialization vector (IV) (for all modes except ECB), and a plaintext for encryption (or a ciphertext for decryption). Following are two sample data sets:

```
KEY1=627f460e08104a10
KEY2=43cd265d5840eaf1
KEY3=313edf97df2a8a8c
IV=8e29f75ea77e5475
PLAINTEXT=326a494cd33fe756

KEY1=37ae5ebf46dff2dc
KEY2=0754b94f31cbb385
KEY3=5e7fd36dc870bfae
IV=3d1de3cc132e3b65
PLAINTEXT=84401f78fe6c10876d8ea23094ea5309
```

The RESPONSE file for the MMT test contains the same data as the REQUEST file with the addition of the ciphertext for encryption (or plaintext for decryption). Following are two sample data sets:

```
KEY1 = 627f460e08104a10
KEY2 = 43cd265d5840eaf1
KEY3 = 313edf97df2a8a8c
IV = 8e29f75ea77e5475
PLAINTEXT = 326a494cd33fe756
CIPHERTEXT = b22b8d66de970692

KEY1 = 37ae5ebf46dff2dc
KEY2 = 0754b94f31cbb385
KEY3 = 5e7fd36dc870bfae
IV = 3d1de3cc132e3b65
PLAINTEXT = 84401f78fe6c10876d8ea23094ea5309
CIPHERTEXT = 7b1f7c7e3b1c948ebd04a75ffba7d2f5
```