Table E3

An Example of the 64-bit Output Feedback Mode

Correction to Change Notice #2

The 64-bit OFB mode in the encrypt state has been selected.

Cryptographic Key = 0123456789abcdef

Initialization Vector = 1234567890abcdef

The plaintext is the ASCI code for:

"We the people of the United States, in order to "

These seven-bit characters are written in hexadecimal notation (0, b7, b6,...,b1). The XOR represents bit-by-bit, modulo 2 addition. Note that all 64 bits of the DES output block are exclusive-ORed with the 64 bits of plaintext.

TIME	DES INPUT BLOCK	DES OUTPUT BLOCK	XOR	P	= C
1	1234567890abcdef	bd661569ae874e25	XOR	5765207468652070	= ea03351dc6e26e55
2	bd661569ae874e25	5d976a504786581f	XOR	656f706c65206f66	= 38f81a3c22a63779
3	5d976a504786581f	5b0229c3443694e3	XOR	2074686520556e69	= 7b7641a66463fa8a
4	5b0229c3443694e3	78f87a8d6da572a3	XOR	7465642053746174	= 0c9d1ead3ed113d7
5	78f87a8d6da572a3	637b8945094103ab	XOR	65732c20696e206f	=0608a565602f23c4
6	637b8945094103ab	53ace61ca2b19f5b	XOR	7264657220746f20	= 21c8836e82c5f07b