Table 5

Resulting Ciphertext from the Variable Plaintext Known Answer Test for Skipjack

(NOTE: KEY = 00 00 00 00 00 00 00 00 00 00)

ROUND	PLAINTEXT or IV (depending on mode)	CIPHERTEXT
00	80 00 00 00 00 00 00 00	9A 90 BC 0B 75 C7 37 03
01	40 00 00 00 00 00 00 00	CC 68 43 59 8C 73 2B BE
02	20 00 00 00 00 00 00 00	13 72 95 35 09 B3 C1 4C
03	10 00 00 00 00 00 00 00	70 AA AA 84 18 E4 89 30
04	08 00 00 00 00 00 00 00	E4 B0 B4 A1 39 E8 54 6E
05	04 00 00 00 00 00 00 00	70 18 F7 13 66 14 6E AF
06	02 00 00 00 00 00 00 00	B3 8F 3D 7E 4F 2D 25 3D
07	01 00 00 00 00 00 00 00	D6 4B A2 06 51 13 D9 1E
08	00 80 00 00 00 00 00 00	F9 5B 92 2F 14 27 A9 F2
09	00 40 00 00 00 00 00 00	6B 64 2F DE 40 85 85 86
10	00 20 00 00 00 00 00 00	6C F5 2D 5E 61 69 52 17
11	00 10 00 00 00 00 00 00	BC 0F 6B CA 62 E1 39 A6
12	00 08 00 00 00 00 00 00	6A D5 03 DC 2A B0 BF E2
13	00 04 00 00 00 00 00 00	AF AD D7 CA B6 72 35 16
14	00 02 00 00 00 00 00 00	00 42 1B 89 5A F5 C0 0A
15	00 01 00 00 00 00 00 00	CA D0 45 6C F8 6C D5 98
16	00 00 80 00 00 00 00 00	16 F4 1C 8F 8A 6A 5B 79
17	00 00 40 00 00 00 00 00	4C E7 71 C7 51 BA 27 60
18	00 00 20 00 00 00 00 00	72 C9 02 E5 8C E5 5B 87
19	00 00 10 00 00 00 00 00	6D 37 8C 66 64 D0 01 10
20	00 00 08 00 00 00 00 00	AC 27 B8 5B 0A 75 E8 BA
21	00 00 04 00 00 00 00 00	54 DF 3A 75 5B 00 63 D2
22	00 00 02 00 00 00 00 00	31 4F 4D 28 6D B4 90 58
23	00 00 01 00 00 00 00 00	88 AE 06 66 B2 A0 78 46

ROUND	PLAINTEXT or IV (depending on mode)	CIPHERTEXT
24	00 00 00 80 00 00 00 00	D8 60 A8 D9 A0 2C BC E8
25	00 00 00 40 00 00 00 00	37 CE 5E EA 53 13 53 5D
26	00 00 00 20 00 00 00 00	73 3A F9 2D A1 C1 80 26
27	00 00 00 10 00 00 00 00	34 1C 23 5F 6E 32 98 1D
28	00 00 00 08 00 00 00 00	C6 A6 56 14 47 D9 E0 96
29	00 00 00 04 00 00 00 00	C5 50 66 A8 D8 39 E5 FA
30	00 00 00 02 00 00 00 00	65 86 4B 48 79 11 A1 0C
31	00 00 00 01 00 00 00 00	87 29 07 E2 D3 36 33 2A
32	00 00 00 00 80 00 00 00	AF 03 76 88 E7 A5 24 9C
33	00 00 00 00 40 00 00 00	C1 FC D1 B4 DC C2 AC BB
34	00 00 00 00 20 00 00 00	40 48 48 80 2D 69 3D DA
35	00 00 00 00 10 00 00 00	B2 DC CE E3 3B 15 6D B6
36	00 00 00 00 08 00 00 00	E6 20 F4 2A 7F A9 01 0B
37	00 00 00 00 04 00 00 00	7C F0 67 F3 BD 3E C3 53
38	00 00 00 00 02 00 00 00	06 37 78 1F 1A 34 72 81
39	00 00 00 00 01 00 00 00	47 41 F1 46 4B 71 70 8E
40	00 00 00 00 00 80 00 00	ED AD 33 F4 56 F5 14 DF
41	00 00 00 00 00 40 00 00	ED 81 27 48 B7 F5 23 E9
42	00 00 00 00 00 20 00 00	83 8C 9C C3 83 D4 62 97
43	00 00 00 00 00 10 00 00	FB 2B C0 FC C9 2F 9B 24
44	00 00 00 00 00 08 00 00	E5 9A A1 12 2A 65 44 32
45	00 00 00 00 00 04 00 00	D4 C8 EF 7E 06 43 12 53
46	00 00 00 00 00 02 00 00	32 ED 63 28 14 C2 A8 56
47	00 00 00 00 00 01 00 00	5D C2 9F 7D E9 6E E5 2C
48	00 00 00 00 00 00 80 00	68 A0 7C 7E 8E AD D5 61
49	00 00 00 00 00 00 40 00	B2 70 68 F2 D6 B3 37 E2
50	00 00 00 00 00 00 20 00	1A F5 1E 9C 29 BF DC 7B
51	00 00 00 00 00 00 10 00	92 1D BD 9B 1C 6B EA EB

ROUND	PLAINTEXT or IV (depending on mode)	CIPHERTEXT
52	00 00 00 00 00 00 08 00	5B 6A 60 22 35 94 35 D2
53	00 00 00 00 00 00 04 00	D7 74 C6 23 74 B2 3B 09
54	00 00 00 00 00 00 02 00	FD 9F 05 27 59 4C E3 7B
55	00 00 00 00 00 00 01 00	67 86 01 C8 B3 64 A7 94
56	00 00 00 00 00 00 00 80	D5 18 22 8D 5B 0B E3 D7
57	00 00 00 00 00 00 00 40	A4 5F EE 6B DD 1F 73 4A
58	00 00 00 00 00 00 00 20	D1 BA 95 51 DF 7C D5 68
59	00 00 00 00 00 00 00 10	AE A3 3D 09 DC 9D 13 10
60	00 00 00 00 00 00 00 08	96 B4 91 C1 FE 44 3E 9A
61	00 00 00 00 00 00 00 04	D0 E0 14 CF EE 94 58 9D
62	00 00 00 00 00 00 00 02	0B 9E 44 B5 37 AF 28 79
63	00 00 00 00 00 00 00 01	22 F4 28 E3 EC 49 1E 60

Table 6

Resulting Ciphertext from the Variable Key Known Answer Test for Skipjack

((NOTE: Plaintext/text = 00 00 00 00 00 00 00 00 and, where applicable, IV = 00 00 00 00 00 00 00 00)

ROUND	KEY	CIPHERTEXT
0	80 00 00 00 00 00 00 00 00 00	7A 00 E4 94 41 46 1F 5A
1	40 00 00 00 00 00 00 00 00 00	A1 4F F8 BC D1 BC 9E F9
2	20 00 00 00 00 00 00 00 00 00	D7 E8 10 38 5A 42 AA EA
3	10 00 00 00 00 00 00 00 00 00	28 FE 2C 33 32 AA BD 35
4	08 00 00 00 00 00 00 00 00 00	3F C0 F0 5E E6 CE 78 8A
5	04 00 00 00 00 00 00 00 00 00	44 3D D0 CB 75 26 F7 4B
6	02 00 00 00 00 00 00 00 00 00	AD 81 9E 67 7C F9 03 05
7	01 00 00 00 00 00 00 00 00 00	98 91 75 5E 5E BA 5B 1D
8	00 80 00 00 00 00 00 00 00 00	0E 64 B4 94 63 3B F2 CB
9	00 40 00 00 00 00 00 00 00 00	63 38 1A 08 A4 7F C4 8D
10	00 20 00 00 00 00 00 00 00 00	F4 10 8B 09 9B 04 70 40
11	00 10 00 00 00 00 00 00 00 00	74 02 16 61 4E D0 E2 5B
12	00 08 00 00 00 00 00 00 00 00	80 00 91 7B 2E 16 B9 2A
13	00 04 00 00 00 00 00 00 00 00	A9 76 9B 62 B3 A0 BE 4E
14	00 02 00 00 00 00 00 00 00 00	42 FD B8 72 EA 31 41 21
15	00 01 00 00 00 00 00 00 00 00	1D 67 2B A0 15 6A B3 9D
16	00 00 80 00 00 00 00 00 00 00	F4 44 41 D7 C7 77 F0 57
17	00 00 40 00 00 00 00 00 00 00	EA 48 7D DC 36 0D 15 94
18	00 00 20 00 00 00 00 00 00 00	32 4B 0E 78 5F F2 B9 08
19	00 00 10 00 00 00 00 00 00 00	1A F5 9E C2 B9 D6 4C 4F
20	00 00 08 00 00 00 00 00 00 00	81 9B 7E 10 2E 76 A0 EE
21	00 00 04 00 00 00 00 00 00 00	0B 0B FE 0D 4A 37 AA 9E
22	00 00 02 00 00 00 00 00 00 00	12 B4 3E 37 60 D3 0D A6
23	00 00 01 00 00 00 00 00 00 00	31 77 25 6C 46 15 41 EE

ROUND	KEY	CIPHERTEXT
24	00 00 00 80 00 00 00 00 00 00	36 00 EB 92 83 6C A0 26
25	00 00 00 40 00 00 00 00 00 00	75 A4 35 AD 22 EC F7 93
26	00 00 00 20 00 00 00 00 00 00	71 90 AA 99 13 C1 F9 EC
27	00 00 00 10 00 00 00 00 00 00	AB A7 18 B1 85 A1 1D D0
28	00 00 00 08 00 00 00 00 00 00	40 F6 7A BF CC 3B 87 3C
29	00 00 00 04 00 00 00 00 00 00	38 A0 A5 8F B0 97 28 F2
30	00 00 00 02 00 00 00 00 00 00	CA 70 2E 49 BF 6F A6 45
31	00 00 00 01 00 00 00 00 00 00	45 5D 93 F0 39 EA 08 60
32	00 00 00 00 80 00 00 00 00 00	53 47 64 3F E8 03 88 3F
33	00 00 00 00 40 00 00 00 00 00	F4 0F F1 DC BA 2B C1 E5
34	00 00 00 00 20 00 00 00 00 00	57 4A 48 48 36 9D 41 2E
35	00 00 00 00 10 00 00 00 00 00	B2 BE 93 6E 36 67 06 36
36	00 00 00 00 08 00 00 00 00 00	5C 88 51 7D 27 42 E6 19
37	00 00 00 00 04 00 00 00 00 00	99 3C 89 D0 9A 2F E5 56
38	00 00 00 00 02 00 00 00 00 00	1A 3F 72 DA 69 4C 9F C7
39	00 00 00 00 01 00 00 00 00 00	96 59 D5 22 8F 4C B1 51
40	00 00 00 00 00 80 00 00 00 00	7C 13 F4 9E 75 0F 5C 30
41	00 00 00 00 00 40 00 00 00 00	35 00 BD 40 7B CD 01 F6
42	00 00 00 00 00 20 00 00 00 00	85 C5 8E 3C 49 44 20 28
43	00 00 00 00 00 10 00 00 00 00	84 13 84 0A 2D 48 AB EA
44	00 00 00 00 00 08 00 00 00 00	83 28 50 E6 E5 C4 AE 5A
45	00 00 00 00 00 04 00 00 00 00	29 E9 7F 0D 9F 0F DC 5F
46	00 00 00 00 00 02 00 00 00 00	2C 45 23 04 37 FF 2E 04
47	00 00 00 00 00 01 00 00 00 00	10 C4 09 FB 87 2A 98 4F
48	00 00 00 00 00 00 80 00 00 00	14 69 3B 30 C3 AF 74 70
49	00 00 00 00 00 00 40 00 00 00	91 3A 90 50 D5 85 BA B9
50	00 00 00 00 00 00 20 00 00 00	5B FB 0F 83 AB 0C 6E EA
51	00 00 00 00 00 00 10 00 00 00	6C 0C A7 28 4D 83 6A AE

ROUND	KEY	CIPHERTEXT
52	00 00 00 00 00 00 08 00 00 00	AC 57 27 D6 12 E1 85 E8
53	00 00 00 00 00 00 04 00 00 00	38 D7 D5 96 A3 D2 9D 90
54	00 00 00 00 00 00 02 00 00 00	78 BA DA D3 BC 43 6C A2
55	00 00 00 00 00 00 01 00 00 00	E4 05 77 87 41 B0 4B A0
56	00 00 00 00 00 00 00 80 00 00	72 FF E4 3D EA 02 AF A5
57	00 00 00 00 00 00 00 40 00 00	52 E9 31 DF 24 8C E4 C7
58	00 00 00 00 00 00 00 20 00 00	4B B1 65 FD B3 BF F6 5C
59	00 00 00 00 00 00 00 10 00 00	7C FA FA 68 61 D7 B4 7D
60	00 00 00 00 00 00 00 08 00 00	48 D1 75 52 31 F8 7A 2A
61	00 00 00 00 00 00 00 04 00 00	41 32 07 DA 1C 9B 6A B5
62	00 00 00 00 00 00 00 02 00 00	63 F8 18 E9 38 2A 27 78
63	00 00 00 00 00 00 00 01 00 00	ED AF 2B 85 FC 30 EB 09
64	00 00 00 00 00 00 00 00 80 00	11 FC 59 93 82 07 63 F7
65	00 00 00 00 00 00 00 00 40 00	E5 39 C3 96 99 15 09 2F
66	00 00 00 00 00 00 00 00 20 00	50 6F 6A 1E 83 4A D8 F7
67	00 00 00 00 00 00 00 00 10 00	8B 15 BA 30 47 FA 31 95
68	00 00 00 00 00 00 00 00 08 00	13 0B E1 5C 39 3E 4B 7A
69	00 00 00 00 00 00 00 00 04 00	88 95 EC 31 04 CA 10 41
70	00 00 00 00 00 00 00 00 02 00	E4 40 AC DF 4B 64 C9 C9
71	00 00 00 00 00 00 00 00 01 00	C2 32 80 EB E0 93 F0 02
72	00 00 00 00 00 00 00 00 00 80	52 64 A6 57 41 FE 78 E3
73	00 00 00 00 00 00 00 00 00 40	80 89 2E 76 85 47 CE 61
74	00 00 00 00 00 00 00 00 00 20	09 11 41 2D 72 09 34 75
75	00 00 00 00 00 00 00 00 00 10	9F 21 AA 76 47 83 E6 49
76	00 00 00 00 00 00 00 00 00 08	4C A9 FA BE AD 2C 02 C6
77	00 00 00 00 00 00 00 00 00 04	59 CE 10 97 3A 7B 1F D5
78	00 00 00 00 00 00 00 00 00 02	68 3B 29 34 E0 CC BE AA
79	00 00 00 00 00 00 00 00 00 01	74 D0 E7 C2 E3 B4 50 A8