SEED 128 Algorithm

Test Vectors

Key	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Plaintext	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
Ciphertext	5E BA C6 E0 05 4E 16 68 19 AF F1 CC 6D 34 6C DB

Round	Round Key		Round Input value			
	$K_{i,0}$	$K_{i,1}$	L0	L1	R0	R1
1	7C8F8C7E	C737A22C	00010203	04050607	08090A0B	0C0D0E0F
2	FF276CDB	A7CA684A	08090A0B	0C0D0E0F	8081BC57	C4EA8A1F
3	2F9D01A1	70049E41	8081BC57	C4EA8A1F	117A8B07	D7358C24
4	AE59B3C4	4245E90C	117A8B07	D7358C24	D1738C94	7326CAB0
5	A1D6400F	DBC1394E	D1738C94	7326CAB0	577ECE6D	1F8433EC
6	85963508	0C5F1FCB	577ECE6D	1F8433EC	910F62AB	DDA096C1
7	B684BDA7	61A4AEAE	910F62AB	DDA096C1	EA4D39B4	B17B1938
8	B684BDA7	61A4AEAE	EA4D39B4	B17B1938	B04E251F	97D7442C
9	76CC05D5	E97A7394	B04E251F	97D7442C	B86D31BF	A5988C06
10	50AC6F92	1B2666E5	B86D31BF	A5988C06	9008EABF	38DF7430
11	65B7904A	8EC3A7B3	9008EABF	38DF7430	33E47DE0	54EFF76C
12	2F7E2E22	A2B121B9	33E47DE0	54EFF76C	6BE9C434	BF3F378A
13	4D0BFDE4	4E888D9B	6BE9C434	BF3F378A	B8DC3842	03A02D33
14	631C8DDC	4378A6C4	B8DC3842	03A02D33	6679FCF7	9791DFCB
15	216AF65F	7878C031	6679FCF7	9791DFCB	1A415792	A02B8C54
16	71891150	98B255B0	1A415792	A02B8C54	19AFF1CC	6D346CDB

Key	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
Plaintext	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Ciphertext	C1 1F 22 F2 01 40 50 50 84 48 35 97 E4 37 0F 43

Round	Round Key		Round Input value			
	$K_{i,0}$	$K_{i,1}$	L0	L1	R0	R1
1	C119F584	5AE033A0	00000000	00000000	00000000	00000000
2	62947390	A600AD14	00000000	00000000	9D8DB62C	911F0C19
3	F6F6544E	596C4B49	9D8DB62C	911F0C19	21229A97	4AB4B7B8
4	C1A3DE02	CE483C49	21229A97	4AB4B7B8	5A27B404	899D7315
5	5E742E6D	7E25163D	5A27B404	899D7315	B8489E76	BA0EF3EA
6	8299D2B4	790A46CE	B8489E76	BA0EF3EA	04A3DF29	31A27FB4
7	EA67D836	55F354F2	04A3DF29	31A27FB4	EC9C17BF	81AA2AA0
8	C47329FB	F50DB634	EC9C17BF	81AA2AA0	4FA74E8D	CDB21BB8
9	2BD30235	51679CE6	4FA74E8D	CDB21BB8	D93492FE	4F71A4DA
10	FA8D6B76	A9F37E02	D93492FE	4F71A4DA	B14053D9	A911379B
11	8B99CC60	0F6092D4	B14053D9	A911379B	5A7024D6	3905668B
12	BDAEFCFA	489C2242	5A7024D6	3905668B	605C8C3A	73DFBB75
13	F6357C14	CFCCB126	605C8C3A	73DFBB75	40282F39	31CB8987
14	A0AA6D85	F8C10774	40282F39	31CB8987	E9F834A8	3B9586D4
15	47F4FEC5	353AE1BA	E9F834A8	3B9586D4	4B60324B	761C9958
16	FECCEA48	A4EF9F9B	4B60324B	761C9958	84483597	E4370F43

Key	47 06 48 08 51 E6 1B E8 5D 74 BF B3 FD 95 61 85
Plaintext	83 A2 F8 A2 88 64 1F B9 A4 E9 A5 CC 2F 13 1C 7D
Ciphertext	EE 54 D1 3E BC AE 70 6D 22 6B C3 14 2C D4 0D 4A

Round	Round Key		Round Input value			
	$K_{i,0}$	$K_{i,1}$	L0	L1	R0	R1
1	56BE4A0F	E9F62877	83A2F8A2	88641FB9	A4E9A5CC	2F131C7D
2	68BCB66C	078911DD	A4E9A5CC	2F131C7D	7CE5F012	47F8C1E6
3	5B82740B	FD24D09B	7CE5F012	47F8C1E6	AAC99520	609F4CB7
4	8D608015	A120E0BE	AAC99520	609F4CB7	3E126D1F	44FA99F0
5	810A75AE	1BF223E5	3E126D1F	44FA99F0	11716365	9BA775AC
6	F9C0D2D0	0F676C02	11716365	9BA775AC	32C9838F	BA5757CB
7	8F9B5C84	8A7C8DDD	32C9838F	BA5757CB	77E00C64	CF9F6B32
8	D4AB4896	18E93447	77E00C64	CF9F6B32	3F09B1F7	DE7D6D58
9	CF090F51	5A4C8202	3F09B1F7	DE7D6D58	300E5CAA	D0BF2345
10	4EC3196F	61B1A0DC	300E5CAA	D0BF2345	9574FDD7	4DF050D1
11	244E07C1	D0D10B12	9574FDD7	4DF050D1	A15EDA6F	624265FD
12	69917C6C	7FF94FB3	A15EDA6F	624265FD	9F39B682	D841C76F
13	9A7EB482	723B5738	9F39B682	D841C76F	EEBBAD8B	C1F488EF
14	B97522C5	39CC6349	EEBBAD8B	C1F488EF	45CF5D4E	BEEA4AA2
15	FFC2AFD5	1412E731	45CF5D4E	BEEA4AA2	43B7FE1B	BCF87781
16	A9AF7241	A3E67359	43B7FE1B	BCF87781	226BC314	2CD40D4A

Key	28 DB C3 BC 49 FF D8 7D CF A5 09 B1 1D 42 2B E7
Plaintext	B4 1E 6B E2 EB A8 4A 14 8E 2E ED 84 59 3C 5E C7
Ciphertext	9B 9B 7B FC D1 81 3C B9 5D 0B 36 18 F4 0F 51 22

Round	Round Key		Round Input value			
	$K_{i,0}$	$K_{i,1}$	L0	L1	R0	R1
1	B2B11B63	2EE9E2D1	B41E6BE2	EBA84A14	8E2EED84	593C5EC7
2	11967260	71A62F24	8E2EED84	593C5EC7	1B31F2F7	3DDE00BA
3	2E017A5A	35DAD7A7	1B31F2F7	3DDE00BA	35CC49C0	2AFB59EA
4	1B2AB5FF	A3ADA69F	35CC49C0	2AFB59EA	D7AB53AA	AE82F1C7
5	519C9903	DA90AAEE	D7AB53AA	AE82F1C7	24139958	B840E56F
6	29FD95AD	B94C3F13	24139958	B840E56F	24AB5291	544C9DBA
7	6F629D19	8ACE692F	24AB5291	544C9DBA	E8152994	75D0B424
8	30A26E73	2F22338E	E8152994	75D0B424	A2CD1153	F32BB23A
9	9721073A	98EE8DAE	A2CD1153	F32BB23A	C386008B	E3257731
10	C597A8A9	27DCDC97	C386008B	E3257731	98396BFD	814F8972
11	F5163A00	5FFD0003	98396BFD	814F8972	E74D2D0D	11D889D1
12	5CBE65DA	A73403E4	E74D2D0D	11D889D1	29D8C7B3	D1B71C0C
13	7D5CF070	1D3B8092	29D8C7B3	D1B71C0C	C4E692C2	D2F57F18
14	388C702B	1BAA4945	C4E692C2	D2F57F18	2FAFB300	5F0C4BFF
15	87D1AB5A	FA13FB5C	2FAFB300	5F0C4BFF	60E5F17C	5626BB68
16	C97D7EED	90724A6E	60E5F17C	5626BB68	5D0B3618	F40F5122