AES-128 (*Nk*=4, *Nr*=10) Algorithm Validation

NIST VECTOR I (KNOWN ANSWER TEST)

```
PLAINTEXT:              00112233445566778899aabbccddeeff
KEY:                    000102030405060708090a0b0c0d0e0f

CYPHER (ENCRYPT):
round[ 0].input         00112233445566778899aabbccddeeff
round[ 0].k_sch         000102030405060708090a0b0c0d0e0f
round[ 1].start         00102030405060708090a0b0c0d0e0f0
round[ 1].s_box         63cab7040953d051cd60e0e7ba70e18c
round[ 1].s_row         6353e08c0960e104cd70b751bacad0e7
round[ 1].m_col         5f72641557f5bc92f7be3b291db9f91a
round[ 1].k_sch         d6aa74fdd2af72fadaa678f1d6ab76fe
round[ 2].start         89d810e8855ace682d1843d8cb128fe4
round[ 2].s_box         a761ca9b97be8b45d8ad1a611fc97369
round[ 2].s_row         a7be1a6997ad739bd8c9ca451f618b61
round[ 2].m_col         ff87968431d86a51645151fa773ad009
round[ 2].k_sch         b692cf0b643dbdf1be9bc5006830b3fe
round[ 3].start         4915598f55e5d7a0daca94fa1f0a63f7
round[ 3].s_box         3b59cb73fcd90ee05774222dc067fb68
round[ 3].s_row         3bd92268fc74fb735767cbe0c0590e2d
round[ 3].m_col         4c9c1e66f771f0762c3f868e534df256
round[ 3].k_sch         b6ff744ed2c2c9bf6c590cbf0469bf41
round[ 4].start         fa636a2825b339c940668a3157244d17
round[ 4].s_box         2dfb02343f6d12dd09337ec75b36e3f0
round[ 4].s_row         2d6d7ef03f33e334093602dd5bfb12c7
round[ 4].m_col         6385b79ffc538df997be478e7547d691
round[ 4].k_sch         47f7f7bc95353e03f96c32bcfd058dfd
round[ 5].start         247240236966b3fa6ed2753288425b6c
round[ 5].s_box         36400926f9336d2d9fb59d23c42c3950
round[ 5].s_row         36339d50f9b539269f2c092dc4406d23
round[ 5].m_col         f4bcd45432e554d075f1d6c51dd03b3c
round[ 5].k_sch         3caaa3e8a99f9deb50f3af57adf622aa
round[ 6].start         c81677bc9b7ac93b25027992b0261996
round[ 6].s_box         e847f56514dadde23f77b64fe7f7d490
round[ 6].s_row         e8dab6901477d4653ff7f5e2e747dd4f
round[ 6].m_col         9816ee7400f87f556b2c049c8e5ad036
round[ 6].k_sch         5e390f7df7a69296a7553dc10aa31f6b
round[ 7].start         c62fe109f75eedc3cc79395d84f9cf5d
round[ 7].s_box         b415f8016858552e4bb6124c5f998a4c
round[ 7].s_row         b458124c68b68a014b99f82e5f15554c
round[ 7].m_col         c57e1c159a9bd286f05f4be098c63439
round[ 7].k_sch         14f9701ae35fe28c440adf4d4ea9c026
round[ 8].start         d1876c0f79c4300ab45594add66ff41f
round[ 8].s_box         3e175076b61c04678dfc2295f6a8bfc0
round[ 8].s_row         3e1c22c0b6fcbf768da85067f6170495
round[ 8].m_col         baa03de7a1f9b56ed5512cba5f414d23
round[ 8].k_sch         47438735a41c65b9e016baf4aebf7ad2
round[ 9].start         fde3bad205e5d0d73547964ef1fe37f1
round[ 9].s_box         5411f4b56bd9700e96a0902fa1bb9aa1
round[ 9].s_row         54d990a16ba09ab596bbf40ea111702f
round[ 9].m_col         e9f74eec023020f61bf2ccf2353c21c7
round[ 9].k_sch         549932d1f08557681093ed9cbe2c974e
round[10].start         bd6e7c3df2b5779e0b61216e8b10b689
round[10].s_box         7a9f102789d5f50b2beffd9f3dca4ea7
round[10].s_row         7ad5fda789ef4e272bca100b3d9ff59f
round[10].k_sch         13111d7fe3944a17f307a78b4d2b30c5
round[10].output        69c4e0d86a7b0430d8cdb78070b4c55a
```

```
INVERSE CYPHER (DECRYPT):
round[ 0].iinput        69c4e0d86a7b0430d8cdb78070b4c55a
round[ 0].ik_sch        13111d7fe3944a17f307a78b4d2b30c5
round[ 1].istart        7ad5fda789ef4e272bca100b3d9ff59f
round[ 1].is_row        7a9f102789d5f50b2beffd9f3dca4ea7
round[ 1].is_box        bd6e7c3df2b5779e0b61216e8b10b689
round[ 1].ik_sch        549932d1f08557681093ed9cbe2c974e
round[ 1].ik_add        e9f74eec023020f61bf2ccf2353c21c7
round[ 2].istart        54d990a16ba09ab596bbf40ea111702f
round[ 2].is_row        5411f4b56bd9700e96a0902fa1bb9aa1
round[ 2].is_box        fde3bad205e5d0d73547964ef1fe37f1
round[ 2].ik_sch        47438735a41c65b9e016baf4aebf7ad2
round[ 2].ik_add        baa03de7a1f9b56ed5512cba5f414d23
round[ 3].istart        3e1c22c0b6fcbf768da85067f6170495
round[ 3].is_row        3e175076b61c04678dfc2295f6a8bfc0
round[ 3].is_box        d1876c0f79c4300ab45594add66ff41f
round[ 3].ik_sch        14f9701ae35fe28c440adf4d4ea9c026
round[ 3].ik_add        c57e1c159a9bd286f05f4be098c63439
round[ 4].istart        b458124c68b68a014b99f82e5f15554c
round[ 4].is_row        b415f8016858552e4bb6124c5f998a4c
round[ 4].is_box        c62fe109f75eedc3cc79395d84f9cf5d
round[ 4].ik_sch        5e390f7df7a69296a7553dc10aa31f6b
round[ 4].ik_add        9816ee7400f87f556b2c049c8e5ad036
round[ 5].istart        e8dab6901477d4653ff7f5e2e747dd4f
round[ 5].is_row        e847f56514dadde23f77b64fe7f7d490
round[ 5].is_box        c81677bc9b7ac93b25027992b0261996
round[ 5].ik_sch        3caaa3e8a99f9deb50f3af57adf622aa
round[ 5].ik_add        f4bcd45432e554d075f1d6c51dd03b3c
round[ 6].istart        36339d50f9b539269f2c092dc4406d23
round[ 6].is_row        36400926f9336d2d9fb59d23c42c3950
round[ 6].is_box        247240236966b3fa6ed2753288425b6c
round[ 6].ik_sch        47f7f7bc95353e03f96c32bcfd058dfd
round[ 6].ik_add        6385b79ffc538df997be478e7547d691
round[ 7].istart        2d6d7ef03f33e334093602dd5bfb12c7
round[ 7].is_row        2dfb02343f6d12dd09337ec75b36e3f0
round[ 7].is_box        fa636a2825b339c940668a3157244d17
round[ 7].ik_sch        b6ff744ed2c2c9bf6c590cbf0469bf41
round[ 7].ik_add        4c9c1e66f771f0762c3f868e534df256
round[ 8].istart        3bd92268fc74fb735767cbe0c0590e2d
round[ 8].is_row        3b59cb73fcd90ee05774222dc067fb68
round[ 8].is_box        4915598f55e5d7a0daca94fa1f0a63f7
round[ 8].ik_sch        b692cf0b643dbdf1be9bc5006830b3fe
round[ 8].ik_add        ff87968431d86a51645151fa773ad009
round[ 9].istart        a7be1a6997ad739bd8c9ca451f618b61
round[ 9].is_row        a761ca9b97be8b45d8ad1a611fc97369
round[ 9].is_box        89d810e8855ace682d1843d8cb128fe4
round[ 9].ik_sch        d6aa74fdd2af72fadaa678f1d6ab76fe
round[ 9].ik_add        5f72641557f5bc92f7be3b291db9f91a
round[10].istart        6353e08c0960e104cd70b751bacad0e7
round[10].is_row        63cab7040953d051cd60e0e7ba70e18c
round[10].is_box        00102030405060708090a0b0c0d0e0f0
round[10].ik_sch        000102030405060708090a0b0c0d0e0f
round[10].ioutput       00112233445566778899aabbccddeeff
```

NIST VECTOR II (KNOWN ANSWER TEST)

```
PLAINTEXT:              3243f6a8885a308d313198a2e0370734
KEY:                    2b7e151628aed2a6abf7158809cf4f3c

CYPHER (ENCRYPT):
round[ 0].input         3243f6a8885a308d313198a2e0370734
round[ 0].k_sch         2b7e151628aed2a6abf7158809cf4f3c
round[ 1].start         193de3bea0f4e22b9ac68d2ae9f84808
round[ 1].s_box         d42711aee0bf98f1b8b45de51e415230
round[ 1].s_row         d4bf5d30e0b452aeb84111f11e2798e5
round[ 1].m_col         046681e5e0cb199a48f8d37a2806264c
round[ 1].k_sch         a0fafe1788542cb123a339392a6c7605
round[ 2].start         a49c7ff2689f352b6b5bea43026a5049
round[ 2].s_box         49ded28945db96f17f39871a7702533b
round[ 2].s_row         49db873b453953897f02d2f177de961a
round[ 2].m_col         584dcaf11b4b5aacdbe7caa81b6bb0e5
round[ 2].k_sch         f2c295f27a96b9435935807a7359f67f
round[ 3].start         aa8f5f0361dde3ef82d24ad26832469a
round[ 3].s_box         ac73cf7befc111df13b5d6b545235ab8
round[ 3].s_row         acc1d6b8efb55a7b1323cfdf457311b5
round[ 3].m_col         75ec0993200b633353c0cf7cbb25d0dc
round[ 3].k_sch         3d80477d4716fe3e1e237e446d7a883b
round[ 4].start         486c4eee671d9d0d4de3b138d65f58e7
round[ 4].s_box         52502f2885a45ed7e311c807f6cf6a94
round[ 4].s_row         52a4c89485116a28e3cf2fd7f6505e07
round[ 4].m_col         0fd6daa9603138bf6fc0106b5eb31301
round[ 4].k_sch         ef44a541a8525b7fb671253bdb0bad00
round[ 5].start         e0927fe8c86363c0d9b1355085b8be01
round[ 5].s_box         e14fd29be8fbfbba35c89653976cae7c
round[ 5].s_row         e1fb967ce8c8ae9b356cd2ba974ffb53
round[ 5].m_col         25d1a9adbd11d168b63a338e4c4cc0b0
round[ 5].k_sch         d4d1c6f87c839d87caf2b8bc11f915bc
round[ 6].start         f1006f55c1924cef7cc88b325db5d50c
round[ 6].s_box         a163a8fc784f29df10e83d234cd503fe
round[ 6].s_row         a14f3dfe78e803fc10d5a8df4c632923
round[ 6].m_col         4b868d6d2c4a8980339df4e837d218d8
round[ 6].k_sch         6d88a37a110b3efddbf98641ca0093fd
round[ 7].start         260e2e173d41b77de86472a9fdd28b25
round[ 7].s_box         f7ab31f02783a9ff9b4340d354b53d3f
round[ 7].s_row         f783403f27433df09bb531ff54aba9d3
round[ 7].m_col         1415b5bf461615ec274656d7342ad843
round[ 7].k_sch         4e54f70e5f5fc9f384a64fb24ea6dc4f
round[ 8].start         5a4142b11949dc1fa3e019657a8c040c
round[ 8].s_box         be832cc8d43b86c00ae1d44dda64f2fe
round[ 8].s_row         be3bd4fed4e1f2c80a642cc0da83864d
round[ 8].m_col         00512fd1b1c889ff54766dcdfa1b99ea
round[ 8].k_sch         ead27321b58dbad2312bf5607f8d292f
round[ 9].start         ea835cf00445332d655d98ad8596b0c5
round[ 9].s_box         87ec4a8cf26ec3d84d4c46959790e7a6
round[ 9].s_row         876e46a6f24ce78c4d904ad897ecc395
round[ 9].m_col         473794ed40d4e4a5a3703aa64c9f42bc
round[ 9].k_sch         ac7766f319fadc2128d12941575c006e
round[10].start         eb40f21e592e38848ba113e71bc342d2
round[10].s_box         e9098972cb31075f3d327d94af2e2cb5
round[10].s_row         e9317db5cb322c723d2e895faf090794
round[10].k_sch         d014f9a8c9ee2589e13f0cc8b6630ca6
round[10].output        3925841d02dc09fbdc118597196a0b32
```

```
INVERSE CYPHER (DECRYPT):
round[ 0].iinput        3925841d02dc09fbdc118597196a0b32
round[ 0].ik_sch        d014f9a8c9ee2589e13f0cc8b6630ca6
round[ 1].istart        e9317db5cb322c723d2e895faf090794
round[ 1].is_row        e9098972cb31075f3d327d94af2e2cb5
round[ 1].is_box        eb40f21e592e38848ba113e71bc342d2
round[ 1].ik_sch        ac7766f319fadc2128d12941575c006e
round[ 1].ik_add        473794ed40d4e4a5a3703aa64c9f42bc
round[ 2].istart        876e46a6f24ce78c4d904ad897ecc395
round[ 2].is_row        87ec4a8cf26ec3d84d4c46959790e7a6
round[ 2].is_box        ea835cf00445332d655d98ad8596b0c5
round[ 2].ik_sch        ead27321b58dbad2312bf5607f8d292f
round[ 2].ik_add        00512fd1b1c889ff54766dcdfa1b99ea
round[ 3].istart        be3bd4fed4e1f2c80a642cc0da83864d
round[ 3].is_row        be832cc8d43b86c00ae1d44dda64f2fe
round[ 3].is_box        5a4142b11949dc1fa3e019657a8c040c
round[ 3].ik_sch        4e54f70e5f5fc9f384a64fb24ea6dc4f
round[ 3].ik_add        1415b5bf461615ec274656d7342ad843
round[ 4].istart        f783403f27433df09bb531ff54aba9d3
round[ 4].is_row        f7ab31f02783a9ff9b4340d354b53d3f
round[ 4].is_box        260e2e173d41b77de86472a9fdd28b25
round[ 4].ik_sch        6d88a37a110b3efddbf98641ca0093fd
round[ 4].ik_add        4b868d6d2c4a8980339df4e837d218d8
round[ 5].istart        a14f3dfe78e803fc10d5a8df4c632923
round[ 5].is_row        a163a8fc784f29df10e83d234cd503fe
round[ 5].is_box        f1006f55c1924cef7cc88b325db5d50c
round[ 5].ik_sch        d4d1c6f87c839d87caf2b8bc11f915bc
round[ 5].ik_add        25d1a9adbd11d168b63a338e4c4cc0b0
round[ 6].istart        e1fb967ce8c8ae9b356cd2ba974ffb53
round[ 6].is_row        e14fd29be8fbfbba35c89653976cae7c
round[ 6].is_box        e0927fe8c86363c0d9b1355085b8be01
round[ 6].ik_sch        ef44a541a8525b7fb671253bdb0bad00
round[ 6].ik_add        0fd6daa9603138bf6fc0106b5eb31301
round[ 7].istart        52a4c89485116a28e3cf2fd7f6505e07
round[ 7].is_row        52502f2885a45ed7e311c807f6cf6a94
round[ 7].is_box        486c4eee671d9d0d4de3b138d65f58e7
round[ 7].ik_sch        3d80477d4716fe3e1e237e446d7a883b
round[ 7].ik_add        75ec0993200b633353c0cf7cbb25d0dc
round[ 8].istart        acc1d6b8efb55a7b1323cfdf457311b5
round[ 8].is_row        ac73cf7befc111df13b5d6b545235ab8
round[ 8].is_box        aa8f5f0361dde3ef82d24ad26832469a
round[ 8].ik_sch        f2c295f27a96b9435935807a7359f67f
round[ 8].ik_add        584dcaf11b4b5aacdbe7caa81b6bb0e5
round[ 9].istart        49db873b453953897f02d2f177de961a
round[ 9].is_row        49ded28945db96f17f39871a7702533b
round[ 9].is_box        a49c7ff2689f352b6b5bea43026a5049
round[ 9].ik_sch        a0fafe1788542cb123a339392a6c7605
round[ 9].ik_add        046681e5e0cb199a48f8d37a2806264c
round[10].istart        d4bf5d30e0b452aeb84111f11e2798e5
round[10].is_row        d42711aee0bf98f1b8b45de51e415230
round[10].is_box        193de3bea0f4e22b9ac68d2ae9f84808
round[10].ik_sch        2b7e151628aed2a6abf7158809cf4f3c
round[10].ioutput       3243f6a8885a308d313198a2e0370734
```

RANDOM VECTOR TEST I

```
PLAINTEXT:              d92233498ac75012fb9f6236bc9761ee
KEY:                    3d24038f3de17b9faf063f04fbf39ffc

CYPHER (ENCRYPT):
round[ 0].input         d92233498ac75012fb9f6236bc9761ee
round[ 0].k_sch         3d24038f3de17b9faf063f04fbf39ffc
round[ 1].start         e40630c6b7262b8d54995d324764fe12
round[ 1].s_box         696f04b4a9f7f15d20ee4c23a043bbc9
round[ 1].s_row         69f74cc9a9eebbb42043045da06ff123
round[ 1].m_col         558146896f0cedc6dcf78c9d38555323
round[ 1].k_sch         31ffb3800c1ec81fa318f71b58eb68e7
round[ 2].start         647ef509631225d97fef7b8660be3bc4
round[ 2].s_box         43f3e601fbc93f35d2df2144d0aee21c
round[ 2].s_row         43c9211cfbdfe201d2aee635d0f33f44
round[ 2].m_col         fbb5ec157462f8298591f44fce28912f
round[ 2].k_sch         daba27ead6a4eff575bc18ee2d577009
round[ 3].start         210fcbffa2c617dcf02deca1e37fe126
round[ 3].s_box         fd761f163ab4f0868cd8ce3211d2f8f7
round[ 3].s_row         fdb4cef73ad8f8168cd21f861176f032
round[ 3].m_col         1f30cc93e9943342f794f1557ac4cad1
round[ 3].k_sch         85eb2632534fc9c726f3d1290ba4a120
round[ 4].start         9adbeaa1badbfa85d167207c71606bf1
round[ 4].s_box         b8b98732f4b92d973e85b710a3d07fa1
round[ 4].s_row         b8b9b7a1f4857f323ed08797a3b92d10
round[ 4].m_col         adb28c842a56d99907805920b0ad704a
round[ 4].k_sch         c4d99119979658deb16589f7bac128d7
round[ 5].start         696b1d9dbdc08147b6e5d0d70a6c589d
round[ 5].s_box         f97fa45e7aba0ca04ed9700e67506a5e
round[ 5].s_row         f9ba705e7ad96a5e4e50a4a0677f0c0e
round[ 5].m_col         12584166b033958168b9b67d4d8312c6
round[ 5].k_sch         aced9fed3b7bc7338a1e4ec430df6613
round[ 6].start         beb5de8b8b4852b2e2a7f8b97d5c74d5
round[ 6].s_box         aed51d3d3d520037985c4156ff4a9203
round[ 6].s_row         ae5241033d5c923d984a1d37ffd50056
round[ 6].m_col         f3ca7bfc311519f3df1cb18ad718d063
round[ 6].k_sch         12dee2e929a525daa3bb6b1e93640d0d
round[ 7].start         e114991518b03c297ca7da94447cdd6e
round[ 7].s_box         f8faee59ade7eba5105c57221b10c19f
round[ 7].s_row         f8e7579fad5cc1591010eea51bfaeb22
round[ 7].m_col         114b0b863d1483c35bbc339feaf04a78
round[ 7].k_sch         1109353538ac10ef9b177bf1087376fc
round[ 8].start         00423eb305b8932cc0ab486ee2833c84
round[ 8].s_box         632cb26d6b6cdc71ba62529f98eceb5f
round[ 8].s_row         636c525f6b62eb6dbaecb271982cdc9f
round[ 8].m_col         7f124a25f6e473ee83c5ba691c20ad66
round[ 8].k_sch         1e318505269d95eabd8aee1bb5f998e7
round[ 9].start         6123cf20d079e6043e4f5472a9d93581
round[ 9].s_box         ef268ab770b68ef2b2842040d335960c
round[ 9].s_row         efb6200c708496b7b2358af2d3268e40
round[ 9].m_col         28f40da4567501f758af858d19563246
round[ 9].k_sch         9c7711d0baea843a07606a21b299f2c6
round[10].start         b4831c74ec9f85cd5fcfefacabcfc080
round[10].s_box         8dec9c92cedb97bdcf8adf91628abacd
round[10].s_row         8ddbdfcdce8aba92cf8a9cbd62ec9791
round[10].k_sch         44fea5e7fe1421ddf9744bfc4bedb93a
round[10].output        c9257a2a309e9b4f36fed74129012eab
```

```
INVERSE CYPHER (DECRYPT):
round[ 0].iinput        c9257a2a309e9b4f36fed74129012eab
round[ 0].ik_sch        44fea5e7fe1421ddf9744bfc4bedb93a
round[ 1].istart        8ddbdfcdce8aba92cf8a9cbd62ec9791
round[ 1].is_row        8dec9c92cedb97bdcf8adf91628abacd
round[ 1].is_box        b4831c74ec9f85cd5fcfefacabcfc080
round[ 1].ik_sch        9c7711d0baea843a07606a21b299f2c6
round[ 1].ik_add        28f40da4567501f758af858d19563246
round[ 2].istart        efb6200c708496b7b2358af2d3268e40
round[ 2].is_row        ef268ab770b68ef2b2842040d335960c
round[ 2].is_box        6123cf20d079e6043e4f5472a9d93581
round[ 2].ik_sch        1e318505269d95eabd8aee1bb5f998e7
round[ 2].ik_add        7f124a25f6e473ee83c5ba691c20ad66
round[ 3].istart        636c525f6b62eb6dbaecb271982cdc9f
round[ 3].is_row        632cb26d6b6cdc71ba62529f98eceb5f
round[ 3].is_box        00423eb305b8932cc0ab486ee2833c84
round[ 3].ik_sch        1109353538ac10ef9b177bf1087376fc
round[ 3].ik_add        114b0b863d1483c35bbc339feaf04a78
round[ 4].istart        f8e7579fad5cc1591010eea51bfaeb22
round[ 4].is_row        f8faee59ade7eba5105c57221b10c19f
round[ 4].is_box        e114991518b03c297ca7da94447cdd6e
round[ 4].ik_sch        12dee2e929a525daa3bb6b1e93640d0d
round[ 4].ik_add        f3ca7bfc311519f3df1cb18ad718d063
round[ 5].istart        ae5241033d5c923d984a1d37ffd50056
round[ 5].is_row        aed51d3d3d520037985c4156ff4a9203
round[ 5].is_box        beb5de8b8b4852b2e2a7f8b97d5c74d5
round[ 5].ik_sch        aced9fed3b7bc7338a1e4ec430df6613
round[ 5].ik_add        12584166b033958168b9b67d4d8312c6
round[ 6].istart        f9ba705e7ad96a5e4e50a4a0677f0c0e
round[ 6].is_row        f97fa45e7aba0ca04ed9700e67506a5e
round[ 6].is_box        696b1d9dbdc08147b6e5d0d70a6c589d
round[ 6].ik_sch        c4d99119979658deb16589f7bac128d7
round[ 6].ik_add        adb28c842a56d99907805920b0ad704a
round[ 7].istart        b8b9b7a1f4857f323ed08797a3b92d10
round[ 7].is_row        b8b98732f4b92d973e85b710a3d07fa1
round[ 7].is_box        9adbeaa1badbfa85d167207c71606bf1
round[ 7].ik_sch        85eb2632534fc9c726f3d1290ba4a120
round[ 7].ik_add        1f30cc93e9943342f794f1557ac4cad1
round[ 8].istart        fdb4cef73ad8f8168cd21f861176f032
round[ 8].is_row        fd761f163ab4f0868cd8ce3211d2f8f7
round[ 8].is_box        210fcbffa2c617dcf02deca1e37fe126
round[ 8].ik_sch        daba27ead6a4eff575bc18ee2d577009
round[ 8].ik_add        fbb5ec157462f8298591f44fce28912f
round[ 9].istart        43c9211cfbdfe201d2aee635d0f33f44
round[ 9].is_row        43f3e601fbc93f35d2df2144d0aee21c
round[ 9].is_box        647ef509631225d97fef7b8660be3bc4
round[ 9].ik_sch        31ffb3800c1ec81fa318f71b58eb68e7
round[ 9].ik_add        558146896f0cedc6dcf78c9d38555323
round[10].istart        69f74cc9a9eebbb42043045da06ff123
round[10].is_row        696f04b4a9f7f15d20ee4c23a043bbc9
round[10].is_box        e40630c6b7262b8d54995d324764fe12
round[10].ik_sch        3d24038f3de17b9faf063f04fbf39ffc
round[10].ioutput       d92233498ac75012fb9f6236bc9761ee
```

RANDOM VECTOR TEST II

```
PLAINTEXT:              b40521450a07ac14bf82d8f22c83e133
KEY:                    566f10aee1b7f808c76048f58059ada3

CYPHER (ENCRYPT):
round[ 0].input         b40521450a07ac14bf82d8f22c83e133
round[ 0].k_sch         566f10aee1b7f808c76048f58059ada3
round[ 1].start         e26a31ebebb0541c78e29007acda4c90
round[ 1].s_box         9802c7e9e9e7209cbc9860c591572960
round[ 1].s_row         98e76060e99829e9bc57c79c910220c5
round[ 1].m_col         198d1ff4ba500358c1dcc16cda30871b
round[ 1].k_sch         9cfa1a637d4de26bba2daa9e3a74073d
round[ 2].start         85770597c71de1337bf16bf2e0448026
round[ 2].s_box         97f56b88c6a4f8c321a17f89e11bcdf7
round[ 2].s_row         97a47ff7c6a1cd88211b6bc3e1f5f889
round[ 2].m_col         4ab2cf8c2a5b6536c769b28eac8a7f3c
round[ 2].k_sch         0c3f3de37172df88cb5f7516f12b722b
round[ 3].start         468df26f5b29babe0c36c7985da10d17
round[ 3].s_box         5a5d89a839a5f4aefe05c6464c32d7f0
round[ 3].s_row         5aa5c6f03905d7a8fe3289ae4c5df446
round[ 3].m_col         76aa637602f96ad296b42ce5cdb728f1
round[ 3].k_sch         f97fcc42880d13ca435266dcb27914f7
round[ 4].start         8fd5af348af47918d5e64a397fce3c06
round[ 4].s_box         730379187ebfb6ad038ed612d28beb6f
round[ 4].s_row         73bfd66f7e8eeb18038b79add203b612
round[ 4].m_col         8518ca22864715d7542896b61e0790fc
round[ 4].k_sch         4785a475cf88b7bf8cdad1633ea3c594
round[ 5].start         c29d6e5749cfa268d8f247d520a45568
round[ 5].s_box         255e9f5b3b8a3a456189a003b749fc45
round[ 5].s_row         258aa0453b89fc5b61499f45b75e3a03
round[ 5].m_col         2a943bcf5176bc8ec30cc2ffae4698a0
round[ 5].k_sch         5d2386c792ab31781e71e01b20d2258f
round[ 6].start         77b7bd08c3dd8df6dd7d22e48e94bd2f
round[ 6].s_box         f5a97a302ec15d42c1ff936919227a15
round[ 6].s_row         f5c193152eff7a30c1227a4219a95d69
round[ 6].m_col         2fd7367c0c757597c749d184e6deb10d
round[ 6].k_sch         c81cf5705ab7c40844c624136414019c
round[ 7].start         e7cbc30c56c2b19f838ff59782cab091
round[ 7].s_box         941f2efeb125c8dbec73e6881374e781
round[ 7].s_row         9425e681b173e7feec742edb131fc888
round[ 7].m_col         3b6efe7df59b0ebbaaadb2d847e604e9
round[ 7].k_sch         72602b3328d7ef3b6c11cb280805cab4
round[ 8].start         490ed54edd4ce180c6bc79f04fe3ce5d
round[ 8].s_box         3bab032fc129f8cdb465b68c84118b4c
round[ 8].s_row         3b29b64cc1658b2fb41103cd84abf88c
round[ 8].m_col         f7e4b14a92a2d8e88e5eef5481564bc7
round[ 8].k_sch         9914a603b1c34938ddd28210d5d748a4
round[ 9].start         6ef01749236191d0538c6d4454810363
round[ 9].s_box         9f8cf03b26ef8170ed643c1b200c7bfb
round[ 9].s_row         9fef3cfb26647b3bed0cf070208c811b
round[ 9].m_col         c8e51e84a058f903558e8a3055a0985b
round[ 9].k_sch         8c46ef003d85a638e057242835806c8c
round[10].start         44a3f1849ddd5f3bb5d9ae186020f4d7
round[10].s_box         1b0aa15f5ec1cfe2d535e4add0b7bf0e
round[10].s_row         1bc1e40e5e35bf5fd5b7a1e2d00acfad
round[10].k_sch         77168b964a932daeaac409869f44650a
round[10].output        6cd76f9814a692f17f73a8644f4eaaa7
```

```
INVERSE CYPHER (DECRYPT):
round[ 0].iinput        6cd76f9814a692f17f73a8644f4eaaa7
round[ 0].ik_sch        77168b964a932daeaac409869f44650a
round[ 1].istart        1bc1e40e5e35bf5fd5b7a1e2d00acfad
round[ 1].is_row        1b0aa15f5ec1cfe2d535e4add0b7bf0e
round[ 1].is_box        44a3f1849ddd5f3bb5d9ae186020f4d7
round[ 1].ik_sch        8c46ef003d85a638e057242835806c8c
round[ 1].ik_add        c8e51e84a058f903558e8a3055a0985b
round[ 2].istart        9fef3cfb26647b3bed0cf070208c811b
round[ 2].is_row        9f8cf03b26ef8170ed643c1b200c7bfb
round[ 2].is_box        6ef01749236191d0538c6d4454810363
round[ 2].ik_sch        9914a603b1c34938ddd28210d5d748a4
round[ 2].ik_add        f7e4b14a92a2d8e88e5eef5481564bc7
round[ 3].istart        3b29b64cc1658b2fb41103cd84abf88c
round[ 3].is_row        3bab032fc129f8cdb465b68c84118b4c
round[ 3].is_box        490ed54edd4ce180c6bc79f04fe3ce5d
round[ 3].ik_sch        72602b3328d7ef3b6c11cb280805cab4
round[ 3].ik_add        3b6efe7df59b0ebbaaadb2d847e604e9
round[ 4].istart        9425e681b173e7feec742edb131fc888
round[ 4].is_row        941f2efeb125c8dbec73e6881374e781
round[ 4].is_box        e7cbc30c56c2b19f838ff59782cab091
round[ 4].ik_sch        c81cf5705ab7c40844c624136414019c
round[ 4].ik_add        2fd7367c0c757597c749d184e6deb10d
round[ 5].istart        f5c193152eff7a30c1227a4219a95d69
round[ 5].is_row        f5a97a302ec15d42c1ff936919227a15
round[ 5].is_box        77b7bd08c3dd8df6dd7d22e48e94bd2f
round[ 5].ik_sch        5d2386c792ab31781e71e01b20d2258f
round[ 5].ik_add        2a943bcf5176bc8ec30cc2ffae4698a0
round[ 6].istart        258aa0453b89fc5b61499f45b75e3a03
round[ 6].is_row        255e9f5b3b8a3a456189a003b749fc45
round[ 6].is_box        c29d6e5749cfa268d8f247d520a45568
round[ 6].ik_sch        4785a475cf88b7bf8cdad1633ea3c594
round[ 6].ik_add        8518ca22864715d7542896b61e0790fc
round[ 7].istart        73bfd66f7e8eeb18038b79add203b612
round[ 7].is_row        730379187ebfb6ad038ed612d28beb6f
round[ 7].is_box        8fd5af348af47918d5e64a397fce3c06
round[ 7].ik_sch        f97fcc42880d13ca435266dcb27914f7
round[ 7].ik_add        76aa637602f96ad296b42ce5cdb728f1
round[ 8].istart        5aa5c6f03905d7a8fe3289ae4c5df446
round[ 8].is_row        5a5d89a839a5f4aefe05c6464c32d7f0
round[ 8].is_box        468df26f5b29babe0c36c7985da10d17
round[ 8].ik_sch        0c3f3de37172df88cb5f7516f12b722b
round[ 8].ik_add        4ab2cf8c2a5b6536c769b28eac8a7f3c
round[ 9].istart        97a47ff7c6a1cd88211b6bc3e1f5f889
round[ 9].is_row        97f56b88c6a4f8c321a17f89e11bcdf7
round[ 9].is_box        85770597c71de1337bf16bf2e0448026
round[ 9].ik_sch        9cfa1a637d4de26bba2daa9e3a74073d
round[ 9].ik_add        198d1ff4ba500358c1dcc16cda30871b
round[10].istart        98e76060e99829e9bc57c79c910220c5
round[10].is_row        9802c7e9e9e7209cbc9860c591572960
round[10].is_box        e26a31ebebb0541c78e29007acda4c90
round[10].ik_sch        566f10aee1b7f808c76048f58059ada3
round[10].ioutput       b40521450a07ac14bf82d8f22c83e133
```

RANDOM VECTOR TEST III

```
PLAINTEXT:              fad2afb142b327854d3f1082ee51bfe4
KEY:                    8bc3d92b722e49570b7d0961d15a72fb

CYPHER (ENCRYPT):
round[ 0].input         fad2afb142b327854d3f1082ee51bfe4
round[ 0].k_sch         8bc3d92b722e49570b7d0961d15a72fb
round[ 1].start         7111769a309d6ed2464219e33f0bcd1f
round[ 1].s_box         a38238b8045e9fb55a2cd411752bbdc0
round[ 1].s_row         a35ed4c0042cbdb85a2b38b575829f11
round[ 1].m_col         abb815ef79389af644f1c58cf9c1e1a0
round[ 1].k_sch         3483d61546ad9f424dd096239c8ae4d8
round[ 2].start         9f3bc3fa3f9505b4092153af654b0578
round[ 2].s_box         dbe22e2d752a6b8d01fded794db36bbc
round[ 2].s_row         db2aedbc75fd6b2d01b32e8d4de26b79
round[ 2].m_col         821fefd2b00429536f83629fb556f2ac
round[ 2].k_sch         48eab7cb0e4728894397beaadf1d5a72
round[ 3].start         caf55819be4301da2c14dc356a4ba8de
round[ 3].s_box         74e66ad4ae1a7c5771fa869602b3c21d
round[ 3].s_row         741a861daefac2d471b36a5702e67c96
round[ 3].m_col         5dcc5e3a44c8ac6211e5efe4dfc7bdab
round[ 3].k_sch         e854f755e613dfdca58461767a993b04
round[ 4].start         b598a96fa2db73beb4618e92a55e86af
round[ 4].s_box         d546d3a83ab98fae8def194f06584479
round[ 4].s_row         d5b919793aef44a88d58d3ae06468f4f
round[ 4].m_col         01eed536b29bbeae94fd8140064f945d
round[ 4].k_sch         0eb6058fe8a5da534d21bb2537b88021
round[ 5].start         0f58d0b95a3e64fdd9dc3a6531f7147c
round[ 5].s_box         766a7056beb243543586804dc768fa10
round[ 5].s_row         76b28010be86fa5635687054c76a434d
round[ 5].m_col         b182ef885aea2d09f62141ef259bfce1
round[ 5].k_sch         727bf8159ade2246d7ff9963e0471942
round[ 6].start         c3f9179dc0340f4f21ded88cc5dce5a3
round[ 6].s_box         2e99f05eba187684fd1d6164a686d90a
round[ 6].s_row         2e18610aba1dd95efd86f084a6997664
round[ 6].m_col         1fb7ea1fcfaeecad04651779f5717fd6
round[ 6].k_sch         f2afd4f46871f6b2bf8e6fd15fc97693
round[ 7].start         ed183eeba7df1a1fbbeb78a8aab80945
round[ 7].s_box         55adb2e95c9ea2c0eae9bcc2ac6c016e
round[ 7].s_row         559ebc6e5ce901e9ea6cb2c0acada2c2
round[ 7].m_col         c1c31a01707f97c5093fa260cfd2037f
round[ 7].k_sch         6f97083b07e6fe89b8689158e7a1e7cb
round[ 8].start         ae54123a7799694cb15733382873e4b4
round[ 8].s_box         e420c980f5eef929c85bc307348f698d
round[ 8].s_row         e4eec38df55b6980c88fc9293420f907
round[ 8].m_col         b4f01b1bf578e72de1a4b557f663f48b
round[ 8].k_sch         dd0317afdae5e926628d787e852c9fb5
round[ 9].start         69f30cb42f9d0e0b8329cd29734f6b3e
round[ 9].s_box         f90dfe8d155eab2beca5bda58f847fb2
round[ 9].s_row         f95ebdb215a57f8dec84fe2b8f0daba5
round[ 9].m_col         042b0b8c2c48c2e481cdf2031cd63b7d
round[ 9].k_sch         b7d8c2386d3d2b1e0fb053608a9cccd5
round[10].start         b3f3c9b44175e9fa8e7da163964af7a8
round[10].s_box         6d0ddd8d839d1e2d19ff32fb90d668c2
round[10].s_row         6d9d32c283ff688d19d6dd2d900d1efb
round[10].k_sch         5f93c14632aeea583d1eb938b78275ed
round[10].output        320ef384b15182d524c86415278f6b16
```

```
INVERSE CYPHER (DECRYPT):
round[ 0].iinput        320ef384b15182d524c86415278f6b16
round[ 0].ik_sch        5f93c14632aeea583d1eb938b78275ed
round[ 1].istart        6d9d32c283ff688d19d6dd2d900d1efb
round[ 1].is_row        6d0ddd8d839d1e2d19ff32fb90d668c2
round[ 1].is_box        b3f3c9b44175e9fa8e7da163964af7a8
round[ 1].ik_sch        b7d8c2386d3d2b1e0fb053608a9cccd5
round[ 1].ik_add        042b0b8c2c48c2e481cdf2031cd63b7d
round[ 2].istart        f95ebdb215a57f8dec84fe2b8f0daba5
round[ 2].is_row        f90dfe8d155eab2beca5bda58f847fb2
round[ 2].is_box        69f30cb42f9d0e0b8329cd29734f6b3e
round[ 2].ik_sch        dd0317afdae5e926628d787e852c9fb5
round[ 2].ik_add        b4f01b1bf578e72de1a4b557f663f48b
round[ 3].istart        e4eec38df55b6980c88fc9293420f907
round[ 3].is_row        e420c980f5eef929c85bc307348f698d
round[ 3].is_box        ae54123a7799694cb15733382873e4b4
round[ 3].ik_sch        6f97083b07e6fe89b8689158e7a1e7cb
round[ 3].ik_add        c1c31a01707f97c5093fa260cfd2037f
round[ 4].istart        559ebc6e5ce901e9ea6cb2c0acada2c2
round[ 4].is_row        55adb2e95c9ea2c0eae9bcc2ac6c016e
round[ 4].is_box        ed183eeba7df1a1fbbeb78a8aab80945
round[ 4].ik_sch        f2afd4f46871f6b2bf8e6fd15fc97693
round[ 4].ik_add        1fb7ea1fcfaeecad04651779f5717fd6
round[ 5].istart        2e18610aba1dd95efd86f084a6997664
round[ 5].is_row        2e99f05eba187684fd1d6164a686d90a
round[ 5].is_box        c3f9179dc0340f4f21ded88cc5dce5a3
round[ 5].ik_sch        727bf8159ade2246d7ff9963e0471942
round[ 5].ik_add        b182ef885aea2d09f62141ef259bfce1
round[ 6].istart        76b28010be86fa5635687054c76a434d
round[ 6].is_row        766a7056beb243543586804dc768fa10
round[ 6].is_box        0f58d0b95a3e64fdd9dc3a6531f7147c
round[ 6].ik_sch        0eb6058fe8a5da534d21bb2537b88021
round[ 6].ik_add        01eed536b29bbeae94fd8140064f945d
round[ 7].istart        d5b919793aef44a88d58d3ae06468f4f
round[ 7].is_row        d546d3a83ab98fae8def194f06584479
round[ 7].is_box        b598a96fa2db73beb4618e92a55e86af
round[ 7].ik_sch        e854f755e613dfdca58461767a993b04
round[ 7].ik_add        5dcc5e3a44c8ac6211e5efe4dfc7bdab
round[ 8].istart        741a861daefac2d471b36a5702e67c96
round[ 8].is_row        74e66ad4ae1a7c5771fa869602b3c21d
round[ 8].is_box        caf55819be4301da2c14dc356a4ba8de
round[ 8].ik_sch        48eab7cb0e4728894397beaadf1d5a72
round[ 8].ik_add        821fefd2b00429536f83629fb556f2ac
round[ 9].istart        db2aedbc75fd6b2d01b32e8d4de26b79
round[ 9].is_row        dbe22e2d752a6b8d01fded794db36bbc
round[ 9].is_box        9f3bc3fa3f9505b4092153af654b0578
round[ 9].ik_sch        3483d61546ad9f424dd096239c8ae4d8
round[ 9].ik_add        abb815ef79389af644f1c58cf9c1e1a0
round[10].istart        a35ed4c0042cbdb85a2b38b575829f11
round[10].is_row        a38238b8045e9fb55a2cd411752bbdc0
round[10].is_box        7111769a309d6ed2464219e33f0bcd1f
round[10].ik_sch        8bc3d92b722e49570b7d0961d15a72fb
round[10].ioutput       fad2afb142b327854d3f1082ee51bfe4
```