```
##############################################################
  Block Cipher Modes of Operation
      Methods for Key Wrapping
##############################################################

Method 1 - KW
##############################################################

Example 1.1

Wrap 128 bits with a 128-bit key

Key is      00010203 04050607 08090A0B 0C0D0E0F
PT is       00112233 44556677 8899AABB CCDDEEFF
--------------------------------------------------------------

Step         AES Encrypt                  A                  R[1]               R[2]
                                          A6A6A6A6A6A6A6A6   0011223344556677   8899AABBCCDDEEFF
t= 1   F4740052E82A225174CE86FBD7B805E7   F4740052E82A2250   8899AABBCCDDEEFF   74CE86FBD7B805E7
t= 2   06BA4EBDE7768D0BD132EE38147E76F8   06BA4EBDE7768D09   74CE86FBD7B805E7   D132EE38147E76F8
t= 3   FC967627BE937208FE6E8D679C5D3460   FC967627BE93720B   D132EE38147E76F8   FE6E8D679C5D3460
t= 4   5896EA9028EE203B07B2BD973E36A6FC   5896EA9028EE203F   FE6E8D679C5D3460   07B2BD973E36A6FC
t= 5   93AEA71B258D90C325F5A3ADC2195401   93AEA71B258D90C6   07B2BD973E36A6FC   25F5A3ADC2195401
t= 6   E3EE986344D878F7F14863BB1E9CA90A   E3EE986344D878F1   25F5A3ADC2195401   F14863BB1E9CA90A
t= 7   2BFC21B2C20E4006B556D35ED8CEF052   2BFC21B2C20E4001   F14863BB1E9CA90A   B556D35ED8CEF052
t= 8   4BE8CE99C0A43A7D64BAE5818D0570BB   4BE8CE99C0A43A75   B556D35ED8CEF052   64BAE5818D0570BB
t= 9   EBE1CE91067024F3BE114B343EB00981   EBE1CE91067024FA   64BAE5818D0570BB   BE114B343EB00981
t=10   5A9C7B1F5B1C3B464FD3D2B7D74FBB42   5A9C7B1F5B1C3B4C   BE114B343EB00981   4FD3D2B7D74FBB42
t=11   93B71967EED41FFCAEF34BD8FB5A7B82   93B71967EED41FF7   4FD3D2B7D74FBB42   AEF34BD8FB5A7B82
t=12   1FA68B0A8112B44B9D3E862371D2CFE5   1FA68B0A8112B447   AEF34BD8FB5A7B82   9D3E862371D2CFE5

CT is
    1FA68B0A 8112B447 AEF34BD8 FB5A7B82
    9D3E8623 71D2CFE5
==============================================================
Example 1.2

Wrap 128 bits with a 192-bit key

Key is
    00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617
PT is       00112233 44556677 8899AABB CCDDEEFF
--------------------------------------------------------------

Step         AES Encrypt                  A                  R[1]               R[2]
                                          A6A6A6A6A6A6A6A6   0011223344556677   8899AABBCCDDEEFF
t= 1   DFE8FD5D1A3786A7351D385096CCFB29   DFE8FD5D1A3786A6   8899AABBCCDDEEFF   351D385096CCFB29
t= 2   9D9B32B9ED742E0251F22F3286758A2D   9D9B32B9ED742E00   351D385096CCFB29   51F22F3286758A2D
t= 3   7B8E343CA51CF8ABBC164F51E20CC983   7B8E343CA51CF8A8   51F22F3286758A2D   BC164F51E20CC983
t= 4   02A97C589714059505FC2D8F8FF4B919   02A97C5897140591   BC164F51E20CC983   05FC2D8F8FF4B919
t= 5   15D4B63F66583817429487269D3A0016   15D4B63F66583812   05FC2D8F8FF4B919   429487269D3A0016
t= 6   AE2D0B76A6951EEA05A2D8FB4DD5BD7A   AE2D0B76A6951EEC   429487269D3A0016   05A2D8FB4DD5BD7A
t= 7   79F849444F4B8AA8D40B091CDBAC0340   79F849444F4B8AAF   05A2D8FB4DD5BD7A   D40B091CDBAC0340
t= 8   5933A9195B5F5E2189F0D6C06F8CA9B4   5933A9195B5F5E29   D40B091CDBAC0340   89F0D6C06F8CA9B4
t= 9   57ADA800299C2E854D5B3DFE7C04ABBA   57ADA800299C2E8C   89F0D6C06F8CA9B4   4D5B3DFE7C04ABBA
t=10   BF17BD6A9BC80163EB24CCFA52EA9078   BF17BD6A9BC80169   4D5B3DFE7C04ABBA   EB24CCFA52EA9078
t=11   B68BF270AE81544FF92B5B97C050AED2   B68BF270AE815444   EB24CCFA52EA9078   F92B5B97C050AED2
t=12   96778B25AE6CA439468AB8A17AD84E5D   96778B25AE6CA435   F92B5B97C050AED2   468AB8A17AD84E5D

CT is
    96778B25 AE6CA435 F92B5B97 C050AED2
    468AB8A1 7AD84E5D
==============================================================

Example 1.3

Wrap 128 bits with a 256-bit key

Key is
    00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C1D1E1F
PT is       00112233 44556677 8899AABB CCDDEEFF
--------------------------------------------------------------

Step         AES Encrypt                 A                  R[1]               R[2]
                                         A6A6A6A6A6A6A6A6   0011223344556677   8899AABBCCDDEEFF
t= 1   794314D454E3FDE1F661BD9F31FBFA31   794314D454E3FDE0   8899AABBCCDDEEFF   F661BD9F31FBFA31
t= 2   D450EA5C5BBCB561F60E0CDB7F429FE8   D450EA5C5BBCB563   F661BD9F31FBFA31   F60E0CDB7F429FE8
t= 3   85DBDF1879D5C0A55602001BFA07AD8B   85DBDF1879D5C0A6   F60E0CDB7F429FE8   5602001BFA07AD8B
t= 4   738C291128B7226D58924F777C3F678C   738C291128B72269   5602001BFA07AD8B   58924F777C3F678C
t= 5   2656A02DFFF054DCF4DF378183E3D5B2   2656A02DFFF054D9   58924F777C3F678C   F4DF378183E3D5B2
t= 6   DDFD0C0E8B52A63A91AC1D36A964F41B   DDFD0C0E8B52A63C   F4DF378183E3D5B2   91AC1D36A964F41B
t= 7   39AB00D4AE4399EA5271D5CED80F34ED   39AB00D4AE4399ED   91AC1D36A964F41B   5271D5CED80F34ED
t= 8   4CE414878463EAAC67D8ED899E7929B8   4CE414878463EAA4   5271D5CED80F34ED   67D8ED899E7929B8
t= 9   FBB44DB106AA07890DF7E50829123648   FBB44DB106AA0780   67D8ED899E7929B8   0DF7E50829123648
t=10   877112A7308ADCC53472D5993D318FD2   877112A7308ADCCF   0DF7E50829123648   3472D5993D318FD2
t=11   78E40190807CC15163E9777905818A2A   78E40190807CC15A   3472D5993D318FD2   63E9777905818A2A
t=12   64E8C3F9CE0F5BAE93C8191E7D6E8AE7   64E8C3F9CE0F5BA2   63E9777905818A2A   93C8191E7D6E8AE7

CT is
    64E8C3F9 CE0F5BA2 63E97779 05818A2A
    93C8191E 7D6E8AE7
==============================================================

Example 1.4

Wrap 192 bits with a 192-bit key

Key is
    00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617
PT is
    00112233 44556677 8899AABB CCDDEEFF
    00010203 04050607
--------------------------------------------------------------
```

```
Step         AES Encrypt                  A                  R[1]               R[2]
R[3]
                                          A6A6A6A6A6A6A6A6   0011223344556677   8899AABBCCDDEEFF
0001020304050607
t= 1   DFE8FD5D1A3786A7351D385096CCFB29   DFE8FD5D1A3786A6   8899AABBCCDDEEFF   0001020304050607
351D385096CCFB29
t= 2   9D9B32B9ED742E0251F22F3286758A2D   9D9B32B9ED742E00   0001020304050607   351D385096CCFB29
51F22F3286758A2D
t= 3   2C8E19A519025B7CFF540E514DE120A3   2C8E19A519025B7F   351D385096CCFB29   51F22F3286758A2D
FF540E514DE120A3
t= 4   E727C7BDF822602EA08DAA041D17BBBA   E727C7BDF822602A   51F22F3286758A2D   FF540E514DE120A3
A08DAA041D17BBBA
t= 5   15B61F7B25D51700AE82BC1118A5DEA4   15B61F7B25D51705   FF540E514DE120A3   A08DAA041D17BBBA
AE82BC1118A5DEA4
t= 6   A187755AEA64719CD1E708FD13778787   A187755AEA64719A   A08DAA041D17BBBA   AE82BC1118A5DEA4
D1E708FD13778787
t= 7   5A994895D81644B7926ED65A9E853FD9   5A994895D81644B0   AE82BC1118A5DEA4   D1E708FD13778787
926ED65A9E853FD9
t= 8   864F408C8AB8CDCF552A09E141D08AE3   864F408C8AB8CDC7   D1E708FD13778787   926ED65A9E853FD9
552A09E141D08AE3
t= 9   53F4373F575EB7A4ED5E8456E61BD295   53F4373F575EB7AD   926ED65A9E853FD9   552A09E141D08AE3
ED5E8456E61BD295
t=10   9EAA4CDA0B1BA5FF98883EDC6B080FB5   9EAA4CDA0B1BA5F5   552A09E141D08AE3   ED5E8456E61BD295
98883EDC6B080FB5
t=11   B1B9902C68E0EB5263F6D88A0663FEF9   B1B9902C68E0EB59   ED5E8456E61BD295   98883EDC6B080FB5
63F6D88A0663FEF9
t=12   FCE591D77709A6E0463437433A93EFE5   FCE591D77709A6EC   98883EDC6B080FB5   63F6D88A0663FEF9
463437433A93EFE5
t=13   428428D2BD88CF58C46965F34EFB2261   428428D2BD88CF55   63F6D88A0663FEF9   463437433A93EFE5
C46965F34EFB2261
t=14   6AC861AB961DA57856E3CEE892BBEFC4   6AC861AB961DA576   463437433A93EFE5   C46965F34EFB2261
56E3CEE892BBEFC4
t=15   E80DB49CC9A1EA6184943C8C67FCFD53   E80DB49CC9A1EA6E   C46965F34EFB2261   56E3CEE892BBEFC4
84943C8C67FCFD53
t=16   ABEE3534AC465C2C68F24EC260743EDC   ABEE3534AC465C3C   56E3CEE892BBEFC4   84943C8C67FCFD53
68F24EC260743EDC
```

```
t=17   E7CC8D8CEDE62BF7E1C6C7DDEE725A93   E7CC8D8CEDE62BE6   84943C8C67FCFD53   68F24EC260743EDC
E1C6C7DDEE725A93
t=18   031D33264E15D3206BA814915C6762D2   031D33264E15D332   68F24EC260743EDC   E1C6C7DDEE725A93
6BA814915C6762D2

CT is
    031D3326 4E15D332 68F24EC2 60743EDC
    E1C6C7DD EE725A93 6BA81491 5C6762D2
==============================================================

Example 1.5

Wrap 192 bits with a 256-bit key

Key is
    00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C1D1E1F
PT is
    00112233 44556677 8899AABB CCDDEEFF
    00010203 04050607
--------------------------------------------------------------

Step         AES Encrypt                  A                  R[1]               R[2]
R[3]
                                          A6A6A6A6A6A6A6A6   0011223344556677   8899AABBCCDDEEFF
0001020304050607
t= 1   794314D454E3FDE1F661BD9F31FBFA31   794314D454E3FDE0   8899AABBCCDDEEFF   0001020304050607
F661BD9F31FBFA31
t= 2   D450EA5C5BBCB561F60E0CDB7F429FE8   D450EA5C5BBCB563   0001020304050607   F661BD9F31FBFA31
F60E0CDB7F429FE8
t= 3   9DF8F5405FBC00C16CA405593A3B5154   9DF8F5405FBC00C2   F661BD9F31FBFA31   F60E0CDB7F429FE8
6CA405593A3B5154
t= 4   F1D28EA6295891EC0CC86A4D9B9C6A31   F1D28EA6295891E8   F60E0CDB7F429FE8   6CA405593A3B5154
0CC86A4D9B9C6A31
t= 5   BF213BFD04E8A24FAEBE2D5C8BF747A9   BF213BFD04E8A24A   6CA405593A3B5154   0CC86A4D9B9C6A31
AEBE2D5C8BF747A9
```

```
t= 6   6F85BFBDB7E880E339EBC1A1A53FF55B   6F85BFBDB7E880E5   0CC86A4D9B9C6A31   AEBE2D5C8BF747A9
39EBC1A1A53FF55B
t= 7   D532789E4E79D819444F92BF78E77BB1   D532789E4E79D81E   AEBE2D5C8BF747A9   39EBC1A1A53FF55B
444F92BF78E77BB1
t= 8   2A5FFCEF1F1916D8C6874607903270CD   2A5FFCEF1F1916D0   39EBC1A1A53FF55B   444F92BF78E77BB1
C6874607903270CD
t= 9   01271BA91D9804F6740A273461ED82C6   01271BA91D9804FF   444F92BF78E77BB1   C6874607903270CD
740A273461ED82C6
t=10   A3223BD7237F7033FB1611A83BEB567F   A3223BD7237F7039   C6874607903270CD   740A273461ED82C6
FB1611A83BEB567F
t=11   B50C330616E7B1C773EDC8CB9322C34E   B50C330616E7B1CC   740A273461ED82C6   FB1611A83BEB567F
73EDC8CB9322C34E
t=12   FB8AFF3F083E12CE0B08CFDF48020F0D   FB8AFF3F083E12C2   FB1611A83BEB567F   73EDC8CB9322C34E
0B08CFDF48020F0D
t=13   82F597607784A33CFB1F2965FCE1E783   82F597607784A331   73EDC8CB9322C34E   0B08CFDF48020F0D
FB1F2965FCE1E783
t=14   D48E5E83B7C906DBD36F4FFBA2C82ED9   D48E5E83B7C906D5   0B08CFDF48020F0D   FB1F2965FCE1E783
D36F4FFBA2C82ED9
t=15   1BF2B1CD947311B6C490C33642717146   1BF2B1CD947311B9   FB1F2965FCE1E783   D36F4FFBA2C82ED9
C490C33642717146
t=16   C9F5F26A378011DEF6E6F4FBE30E71E4   C9F5F26A378011CE   D36F4FFBA2C82ED9   C490C33642717146
F6E6F4FBE30E71E4
t=17   39128CE5E435F3A0769C8B80A32CB895   39128CE5E435F3B1   C490C33642717146   F6E6F4FBE30E71E4
769C8B80A32CB895
t=18   A8F9BC1612C68B2D8CD5D17D6B254DA1   A8F9BC1612C68B3F   F6E6F4FBE30E71E4   769C8B80A32CB895
8CD5D17D6B254DA1

CT is
    A8F9BC16 12C68B3F F6E6F4FB E30E71E4
    769C8B80 A32CB895 8CD5D17D 6B254DA1
==============================================================
```

Example 1.6

Wrap 256 bits with a 256-bit key

```
Key is
    00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C1D1E1F
PT is
    00112233 44556677 8899AABB CCDDEEFF
    00010203 04050607 08090A0B 0C0D0E0F
--------------------------------------------------------------

Step         AES Encrypt                 A                  R[1]               R[2]
R[3]               R[4]
                                          A6A6A6A6A6A6A6A6   0011223344556677   8899AABBCCDDEEFF
0001020304050607   08090A0B0C0D0E0F
t= 1   794314D454E3FDE1F661BD9F31FBFA31   794314D454E3FDE0   8899AABBCCDDEEFF   0001020304050607
08090A0B0C0D0E0F   F661BD9F31FBFA31
t= 2   D450EA5C5BBCB561F60E0CDB7F429FE8   D450EA5C5BBCB563   0001020304050607   08090A0B0C0D0E0F
F661BD9F31FBFA31   F60E0CDB7F429FE8
t= 3   9DF8F5405FBC00C16CA405593A3B5154   9DF8F5405FBC00C2   08090A0B0C0D0E0F   F661BD9F31FBFA31
F60E0CDB7F429FE8   6CA405593A3B5154
t= 4   564408FDD0DD2EA4E5923CB9FDB56FBC   564408FDD0DD2EA0   F661BD9F31FBFA31   F60E0CDB7F429FE8
6CA405593A3B5154   E5923CB9FDB56FBC
t= 5   4EF02EDD3146AFBBE7D1194D853E53F8   4EF02EDD3146AFBE   F60E0CDB7F429FE8   6CA405593A3B5154
E5923CB9FDB56FBC   E7D1194D853E53F8
t= 6   963AAFFD96B223ECEFD48BA304945576   963AAFFD96B223EA   6CA405593A3B5154   E5923CB9FDB56FBC
E7D1194D853E53F8   EFD48BA304945576
t= 7   66D7A8ADD086B9DDC365B66943E2D760   66D7A8ADD086B9DA   E5923CB9FDB56FBC   E7D1194D853E53F8
EFD48BA304945576   C365B66943E2D760
t= 8   C58B9D3AC6D5B94E73E3B6CBE5D05D74   C58B9D3AC6D5B946   E7D1194D853E53F8   EFD48BA304945576
C365B66943E2D760   73E3B6CBE5D05D74
t= 9   1A681354E84C41F8D6AE29ECE7192D43   1A681354E84C41F1   EFD48BA304945576   C365B66943E2D760
73E3B6CBE5D05D74   D6AE29ECE7192D43
t=10   DBA417FB51F9E3CBFBEC169FA5C0F6BA   DBA417FB51F9E3C1   C365B66943E2D760   73E3B6CBE5D05D74
D6AE29ECE7192D43   FBEC169FA5C0F6BA
t=11   0629EB29A42E4FD9F56701DAF0388216   0629EB29A42E4FD2   73E3B6CBE5D05D74   D6AE29ECE7192D43
FBEC169FA5C0F6BA   F56701DAF0388216
t=12   F9ED8A14295156653CF149E90E8C04D9   F9ED8A1429515669   D6AE29ECE7192D43   FBEC169FA5C0F6BA
F56701DAF0388216   3CF149E90E8C04D9
```

```
t=13   2E8E2B6BB20166964745856AF333F01F   2E8E2B6BB201669B   FBEC169FA5C0F6BA   F56701DAF0388216
3CF149E90E8C04D9   4745856AF333F01F
t=14   15342443CB95ADB1BCA418BBF7DCE60B   15342443CB95ADBF   F56701DAF0388216   3CF149E90E8C04D9
4745856AF333F01F   BCA418BBF7DCE60B
t=15   33FE29365885C4B7C272E9466AAE98F9   33FE29365885C4B8   3CF149E90E8C04D9   4745856AF333F01F
BCA418BBF7DCE60B   C272E9466AAE98F9
t=16   5075496800978B4A40F68C91DB49702C   5075496800978B5A   4745856AF333F01F   BCA418BBF7DCE60B
C272E9466AAE98F9   40F68C91DB49702C
t=17   A5382A26B47551F11BB8C765A84195E7   A5382A26B47551E0   BCA418BBF7DCE60B   C272E9466AAE98F9
40F68C91DB49702C   1BB8C765A84195E7
t=18   F19D80D437EFE8F9F7EDAD518C960D36   F19D80D437EFE8EB   C272E9466AAE98F9   40F68C91DB49702C
1BB8C765A84195E7   F7EDAD518C960D36
t=19   B422B444B87A190B1CFBF6B4C24CB982   B422B444B87A1918   40F68C91DB49702C   1BB8C765A84195E7
F7EDAD518C960D36   1CFBF6B4C24CB982
t=20   D058823360F88A3707DFE775B9687E73   D058823360F88A23   1BB8C765A84195E7   F7EDAD518C960D36
1CFBF6B4C24CB982   07DFE775B9687E73
t=21   C89A96CA7B163ECCCBCCB35CFB87F826   C89A96CA7B163ED9   F7EDAD518C960D36   1CFBF6B4C24CB982
07DFE775B9687E73   CBCCB35CFB87F826
t=22   39D02FE7435870ED3F5786E2D80ED326   39D02FE7435870FB   1CFBF6B4C24CB982   07DFE775B9687E73
CBCCB35CFB87F826   3F5786E2D80ED326
t=23   0AEB82AE3146A91BCBC7F0E71A99F43B   0AEB82AE3146A90C   07DFE775B9687E73   CBCCB35CFB87F826
3F5786E2D80ED326   CBC7F0E71A99F43B
t=24   28C9F404C4B810ECFB988B9B7A02DD21   28C9F404C4B810F4   CBCCB35CFB87F826   3F5786E2D80ED326
CBC7F0E71A99F43B   FB988B9B7A02DD21

CT is
    28C9F404 C4B810F4 CBCCB35C FB87F826
    3F5786E2 D80ED326 CBC7F0E7 1A99F43B
    FB988B9B 7A02DD21
==============================================================

Method 2 - KWP
##############################################################

Example 2.1
```

```
Wrap 56 bits with a 128-bit key

Key is      00010203 04050607 08090A0B 0C0D0E0F
PT is       00112233 445566
--------------------------------------------------------------

CT is       1B1D4BC2 A90B1FA3 89412B3D 40FECB20
==============================================================

Example 2.2

Wrap 56 bits with a 192-bit key

Key is
    00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617
PT is       00112233 445566
--------------------------------------------------------------

CT is       87CE2C5C 2D7196E0 9381056B 319D91E9
==============================================================

Example 2.3

Wrap 56 bits with a 256-bit key

Key is
    00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C1D1E1F
PT is       00112233 445566
--------------------------------------------------------------

CT is       809BB186 4A189385 29E97EFC D9544E9A
==============================================================

Example 2.4
```

```
Wrap 112 bits with a 128-bit key

Key is      00010203 04050607 08090A0B 0C0D0E0F
PT is       00112233 44556677 8899AABB CCDD
--------------------------------------------------------------

Step         AES Encrypt                 A                  R[1]               R[2]
                                          A65959A60000000E   0011223344556677   8899AABBCCDD0000
t= 1   4058C1D625722F4C14E0005268BC93E7   4058C1D625722F4D   8899AABBCCDD0000   14E0005268BC93E7
t= 2   F946A0306E90726984AAB4C72549F399   F946A0306E90726B   14E0005268BC93E7   84AAB4C72549F399
t= 3   D25B1C0084AAD3A2FB2B655EDF3E1880   D25B1C0084AAD3A1   84AAB4C72549F399   FB2B655EDF3E1880
t= 4   FA25A426694570C0F32948B2EC6D448D   FA25A426694570C4   FB2B655EDF3E1880   F32948B2EC6D448D
t= 5   B728AD17CBFBDEC5A200F5FC2CECAD46   B728AD17CBFBDEC0   F32948B2EC6D448D   A200F5FC2CECAD46
t= 6   8F11EB437175B0723F12D02B361BDD37   8F11EB437175B074   A200F5FC2CECAD46   3F12D02B361BDD37
t= 7   4F4323AC06ABE87D86C7BCEC3D7648B1   4F4323AC06ABE87A   3F12D02B361BDD37   86C7BCEC3D7648B1
t= 8   ECA5045BC32BB60068BD4AA59A9FB71F   ECA5045BC32BB608   86C7BCEC3D7648B1   68BD4AA59A9FB71F
t= 9   D43CA24FAC5CC32C4CEC5B7C5108E9B7   D43CA24FAC5CC325   68BD4AA59A9FB71F   4CEC5B7C5108E9B7
t=10   66E877757DA497AE8AA16C253AEE8FFD   66E877757DA497A4   4CEC5B7C5108E9B7   8AA16C253AEE8FFD
t=11   FFB3C11E1B9BB40A18E811A05D2A4C23   FFB3C11E1B9BB401   8AA16C253AEE8FFD   18E811A05D2A4C23
t=12   EA0BFDE8AF063E85A367B45315716B5B   EA0BFDE8AF063E89   18E811A05D2A4C23   A367B45315716B5B

CT is
    EA0BFDE8 AF063E89 18E811A0 5D2A4C23
    A367B453 15716B5B
==============================================================

Example 2.5

Wrap 112 bits with a 192-bit key

Key is
    00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617
PT is       00112233 44556677 8899AABB CCDD
--------------------------------------------------------------
```

```
Step         AES Encrypt                    A                  R[1]               R[2]
                                           A65959A60000000E   0011223344556677   8899AABBCCDD0000
t= 1   93D198AFFE64EE3CA4FBDDF1B3583B39   93D198AFFE64EE3D   8899AABBCCDD0000   A4FBDDF1B3583B39
t= 2   D90730292ACFD91180CD178F8818C2C2   D90730292ACFD913   A4FBDDF1B3583B39   80CD178F8818C2C2
t= 3   2F682260B8678B0FA9CFBC21AE72C43D   2F682260B8678B0C   80CD178F8818C2C2   A9CFBC21AE72C43D
t= 4   CECCD7B2F945CC6ADA7E26C24B6B9D44   CECCD7B2F945CC6E   A9CFBC21AE72C43D   DA7E26C24B6B9D44
t= 5   E4F87EA3B835846459FAAA61FF733D0C   E4F87EA3B8358461   DA7E26C24B6B9D44   59FAAA61FF733D0C
t= 6   C98ECE3AEA50353A8F8D74516807A362   C98ECE3AEA50353C   59FAAA61FF733D0C   8F8D74516807A362
t= 7   C53687B77F39DB992BAD3900697255D7   C53687B77F39DB9E   8F8D74516807A362   2BAD3900697255D7
t= 8   987B20808E81557C86CA8F99F65B9DE6   987B20808E815574   2BAD3900697255D7   86CA8F99F65B9DE6
t= 9   900DCAAA46DA2C202F24632E2CC21156   900DCAAA46DA2C29   86CA8F99F65B9DE6   2F24632E2CC21156
t=10   9BAE2D13D4FE56C8E1CB95DD17576050   9BAE2D13D4FE56C2   2F24632E2CC21156   E1CB95DD17576050
t=11   76354560986FC45AD74CE81DCDACA26E   76354560986FC451   E1CB95DD17576050   D74CE81DCDACA26E
t=12   900484950F84EB6272BB29D4A6F7AC74   900484950F84EB6E   D74CE81DCDACA26E   72BB29D4A6F7AC74

CT is
    90048495 0F84EB6E D74CE81D CDACA26E
    72BB29D4 A6F7AC74
==============================================================

Example 2.6

Wrap 112 bits with a 256-bit key

Key is
    00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C1D1E1F
PT is       00112233 44556677 8899AABB CCDD
--------------------------------------------------------------

Step         AES Encrypt                    A                  R[1]               R[2]
                                           A65959A60000000E   0011223344556677   8899AABBCCDD0000
t= 1   1859BA3F01507A4A196C6756191CE524   1859BA3F01507A4B   8899AABBCCDD0000   196C6756191CE524
t= 2   964A36563AB3FD6CE6D52F0DA8ACA68B   964A36563AB3FD6E   196C6756191CE524   E6D52F0DA8ACA68B
t= 3   8170BFB170B95F1CEA5B6071B2762B44   8170BFB170B95F1F   E6D52F0DA8ACA68B   EA5B6071B2762B44
```

```
t= 4   B0B771BE2B15178AB15B21D7496596BB   B0B771BE2B15178E   EA5B6071B2762B44   B15B21D7496596BB
t= 5   7EF8EA1C48C73744854E695ACB4DEC8A   7EF8EA1C48C73741   B15B21D7496596BB   854E695ACB4DEC8A
t= 6   D02F5216E4E37D64BBF529C513B8AAD5   D02F5216E4E37D62   854E695ACB4DEC8A   BBF529C513B8AAD5
t= 7   5485F8A07295E073C9DD50FB7EE480FA   5485F8A07295E074   BBF529C513B8AAD5   C9DD50FB7EE480FA
t= 8   4863B595E3F8996189945A3B607100C1   4863B595E3F89969   C9DD50FB7EE480FA   89945A3B607100C1
t= 9   E5E47D3AB398D462C802DC9B6F3B2595   E5E47D3AB398D46B   89945A3B607100C1   C802DC9B6F3B2595
t=10   E38FDC3D58A9BBE8163BADDBA6F112CA   E38FDC3D58A9BBE2   C802DC9B6F3B2595   163BADDBA6F112CA
t=11   ED6BB8B31280880F5767611574A94125   ED6BB8B312808804   163BADDBA6F112CA   5767611574A94125
t=12   C68168173F141E619090DA78D7DF9DF7   C68168173F141E6D   5767611574A94125   9090DA78D7DF9DF7

CT is
    C6816817 3F141E6D 57676115 74A94125
    9090DA78 D7DF9DF7
==============================================================

Example 2.7

Wrap 168 bits with a 192-bit key

Key is
    00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617
PT is
    00112233 44556677 8899AABB CCDDEEFF
    00010203 04
--------------------------------------------------------------

Step         AES Encrypt                 A                  R[1]               R[2]
R[3]
                                          A65959A600000015   0011223344556677   8899AABBCCDDEEFF
0001020304000000
t= 1   E37251138B7F1D94E8B689F276D1976B   E37251138B7F1D95   8899AABBCCDDEEFF   0001020304000000
E8B689F276D1976B
t= 2   1B37DEB725296472B982A38A5CCD26C0   1B37DEB725296470   0001020304000000   E8B689F276D1976B
B982A38A5CCD26C0
t= 3   7AAD0877BE15377A4500F8263F3F5768   7AAD0877BE153779   E8B689F276D1976B   B982A38A5CCD26C0
```

```
4500F8263F3F5768
t= 4   F4E12516F52D758991F58FE0E79FF139   F4E12516F52D758D   B982A38A5CCD26C0   4500F8263F3F5768
91F58FE0E79FF139
t= 5   C14F020726CFC94AAB13ED957046B73B   C14F020726CFC94F   4500F8263F3F5768   91F58FE0E79FF139
AB13ED957046B73B
t= 6   FBF76D1D1F4BC09BF38235745B4BAD13   FBF76D1D1F4BC09D   91F58FE0E79FF139   AB13ED957046B73B
F38235745B4BAD13
t= 7   62D496F4BC2278709B0EE0C574966920   62D496F4BC227877   AB13ED957046B73B   F38235745B4BAD13
9B0EE0C574966920
t= 8   FA9DEFFBB26AAAD75B914711D60CA97B   FA9DEFFBB26AAADF   F38235745B4BAD13   9B0EE0C574966920
5B914711D60CA97B
t= 9   9FC8B7221FEFD9DC1E9FF0B4A82D33DA   9FC8B7221FEFD9D5   9B0EE0C574966920   5B914711D60CA97B
1E9FF0B4A82D33DA
t=10   A79A122DA8BD7F34513D3679AA5A4B85   A79A122DA8BD7F3E   5B914711D60CA97B   1E9FF0B4A82D33DA
513D3679AA5A4B85
t=11   D9A22F82AC13D76F68A34DD84602722B   D9A22F82AC13D764   1E9FF0B4A82D33DA   513D3679AA5A4B85
68A34DD84602722B
t=12   15943A9050B6781CEE299A0EDA067212   15943A9050B67810   513D3679AA5A4B85   68A34DD84602722B
EE299A0EDA067212
t=13   295E430A8C55CB86D49E0C20ABA8DF46   295E430A8C55CB8B   68A34DD84602722B   EE299A0EDA067212
D49E0C20ABA8DF46
t=14   9EDEEEB863E7B6B97EA77CFED5CDBB1F   9EDEEEB863E7B6B7   EE299A0EDA067212   D49E0C20ABA8DF46
7EA77CFED5CDBB1F
t=15   C35A23152783F6435C36F57C756A20CF   C35A23152783F64C   D49E0C20ABA8DF46   7EA77CFED5CDBB1F
5C36F57C756A20CF
t=16   A3AB89067DFBDF168FDDFD8976420F9D   A3AB89067DFBDF06   7EA77CFED5CDBB1F   5C36F57C756A20CF
8FDDFD8976420F9D
t=17   0494BA67A4076DBEDEB7183CF16B91B0   0494BA67A4076DAF   5C36F57C756A20CF   8FDDFD8976420F9D
DEB7183CF16B91B0
t=18   A402348F1956DB84AEB74CAB196C343E   A402348F1956DB96   8FDDFD8976420F9D   DEB7183CF16B91B0
AEB74CAB196C343E

CT is
    A402348F 1956DB96 8FDDFD89 76420F9D
    DEB7183C F16B91B0 AEB74CAB 196C343E
===============================================================
Example 2.8

Wrap 168 bits with a 256-bit key

Key is
    00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C1D1E1F
PT is
    00112233 44556677 8899AABB CCDDEEFF
    00010203 04
--------------------------------------------------------------

Step         AES Encrypt                  A                  R[1]               R[2]
R[3]
                                          A65959A600000015   0011223344556677   8899AABBCCDDEEFF
0001020304000000
t= 1   92411F5F5C43C8F00E54A5621E9AF5CB   92411F5F5C43C8F1   8899AABBCCDDEEFF   0001020304000000
0E54A5621E9AF5CB
t= 2   B1E02AB9D2331014267BC3A60E118546   B1E02AB9D2331016   0001020304000000   0E54A5621E9AF5CB
267BC3A60E118546
t= 3   BE4AC9BFE7557D36E7A288B9A1204784   BE4AC9BFE7557D35   0E54A5621E9AF5CB   267BC3A60E118546
E7A288B9A1204784
t= 4   0DED948239BE7A4FE7AA6BFFEF170EB1   0DED948239BE7A4B   267BC3A60E118546   E7A288B9A1204784
E7AA6BFFEF170EB1
t= 5   CBAF178F5DA6D80EC4760C8F663C6B85   CBAF178F5DA6D80B   E7A288B9A1204784   E7AA6BFFEF170EB1
C4760C8F663C6B85
t= 6   0829AC869041EF4501B7A66625210DD6   0829AC869041EF43   E7AA6BFFEF170EB1   C4760C8F663C6B85
01B7A66625210DD6
t= 7   C2BFF3A062DFF01A05DF9F8294465C28   C2BFF3A062DFF01D   C4760C8F663C6B85   01B7A66625210DD6
05DF9F8294465C28
t= 8   1FA73D3F3FDFDE213894380B75977A16   1FA73D3F3FDFDE29   01B7A66625210DD6   05DF9F8294465C28
3894380B75977A16
t= 9   8C2083A0F321A12CC4DDCF1D3186BBAE   8C2083A0F321A125   05DF9F8294465C28   3894380B75977A16
C4DDCF1D3186BBAE
t=10   2B0B04623E6542F65FD591C77326B8E8   2B0B04623E6542FC   3894380B75977A16   C4DDCF1D3186BBAE
```

```
5FD591C77326B8E8
t=11   1F327228A1366E23527C06162C219740   1F327228A1366E28   C4DDCF1D3186BBAE   5FD591C77326B8E8
527C06162C219740
t=12   DE429D0FEAC8648ACF4646E43DBA5C79   DE429D0FEAC86486   5FD591C77326B8E8   527C06162C219740
CF4646E43DBA5C79
t=13   7D86687464A92820ED8498F60E0963E5   7D86687464A9282D   527C06162C219740   CF4646E43DBA5C79
ED8498F60E0963E5
t=14   2BAD6CB1428FED3B2C8EDC503CE4DD7B   2BAD6CB1428FED35   CF4646E43DBA5C79   ED8498F60E0963E5
2C8EDC503CE4DD7B
t=15   A3A006039CD41BC0C27B14D60E8A1675   A3A006039CD41BCF   ED8498F60E0963E5   2C8EDC503CE4DD7B
C27B14D60E8A1675
t=16   ED770070D3E4C64A38D54BB4B9856335   ED770070D3E4C65A   2C8EDC503CE4DD7B   C27B14D60E8A1675
38D54BB4B9856335
t=17   07D82DDBE96E2B1E04237329964C76EB   07D82DDBE96E2B0F   C27B14D60E8A1675   38D54BB4B9856335
04237329964C76EB
t=18   308D49692B5F8CE4B3F669870A708DBC   308D49692B5F8CF6   38D54BB4B9856335   04237329964C76EB
B3F669870A708DBC

CT is
    308D4969 2B5F8CF6 38D54BB4 B9856335
    04237329 964C76EB B3F66987 0A708DBC
==============================================================

Example 2.9

Wrap 224 bits with a 256-bit key

Key is
    00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C1D1E1F
PT is
    00112233 44556677 8899AABB CCDDEEFF
    00010203 04050607 08090A0B
--------------------------------------------------------------

Step         AES Encrypt                        A                  R[1]               R[2]
```

```
R[3]               R[4]
                                          A65959A60000001C   0011223344556677   8899AABBCCDDEEFF
0001020304050607   08090A0B00000000
t= 1   BF601339874E4DC8A13CDC243B979EB4   BF601339874E4DC9   8899AABBCCDDEEFF   0001020304050607
08090A0B00000000   A13CDC243B979EB4
t= 2   3637FABE343C6EED3D84AD908D14D67B   3637FABE343C6EEF   0001020304050607   08090A0B00000000
A13CDC243B979EB4   3D84AD908D14D67B
t= 3   2C88585365D84DDDF2CBCF5C959950C0   2C88585365D84DDE   08090A0B00000000   A13CDC243B979EB4
3D84AD908D14D67B   F2CBCF5C959950C0
t= 4   3FD77560F0CAD7FD1BC080B28F086C9B   3FD77560F0CAD7F9   A13CDC243B979EB4   3D84AD908D14D67B
F2CBCF5C959950C0   1BC080B28F086C9B
t= 5   89FD32369923E40A04668F6DD8C89D5C   89FD32369923E40F   3D84AD908D14D67B   F2CBCF5C959950C0
1BC080B28F086C9B   04668F6DD8C89D5C
t= 6   C290EE12881D7C0F0D13959F552C13D2   C290EE12881D7C09   F2CBCF5C959950C0   1BC080B28F086C9B
04668F6DD8C89D5C   0D13959F552C13D2
t= 7   4A9BFB1AD6EB5941959F3DA33D357998   4A9BFB1AD6EB5946   1BC080B28F086C9B   04668F6DD8C89D5C
0D13959F552C13D2   959F3DA33D357998
t= 8   3AB13F71164E7759B8FF882896FEE7BB   3AB13F71164E7751   04668F6DD8C89D5C   0D13959F552C13D2
959F3DA33D357998   B8FF882896FEE7BB
t= 9   A3226157E186939C08489113DE97255E   A3226157E1869395   0D13959F552C13D2   959F3DA33D357998
B8FF882896FEE7BB   08489113DE97255E
t=10   C088B7379E3EBFE2D2127B2696DD73FA   C088B7379E3EBFE8   959F3DA33D357998   B8FF882896FEE7BB
08489113DE97255E   D2127B2696DD73FA
t=11   8FFDD2C41956006C193BA8B414421913   8FFDD2C419560067   B8FF882896FEE7BB   08489113DE97255E
D2127B2696DD73FA   193BA8B414421913
t=12   0A78F13B11F3B2C24469331D734429D1   0A78F13B11F3B2CE   08489113DE97255E   D2127B2696DD73FA
193BA8B414421913   4469331D734429D1
t=13   733D2728BAC2A168C5066A7868783DC1   733D2728BAC2A165   D2127B2696DD73FA   193BA8B414421913
4469331D734429D1   C5066A7868783DC1
t=14   56FD861083D6BB697260712BF7D7EF50   56FD861083D6BB67   193BA8B414421913   4469331D734429D1
C5066A7868783DC1   7260712BF7D7EF50
t=15   9B368D9D81F4E0BD58F796D9378EE3C1   9B368D9D81F4E0B2   4469331D734429D1   C5066A7868783DC1
7260712BF7D7EF50   58F796D9378EE3C1
t=16   D4CF4251FC74A92FAAE1E428B7B76BB1   D4CF4251FC74A93F   C5066A7868783DC1   7260712BF7D7EF50
58F796D9378EE3C1   AAE1E428B7B76BB1
t=17   9CF16D66E1AAEB342B643A972FC0CDB2   9CF16D66E1AAEB25   7260712BF7D7EF50   58F796D9378EE3C1
```

```
AAE1E428B7B76BB1   2B643A972FC0CDB2
t=18   5BC357DCEA34CDB7EF26EDFEB8D7AF05   5BC357DCEA34CDA5   58F796D9378EE3C1   AAE1E428B7B76BB1
2B643A972FC0CDB2   EF26EDFEB8D7AF05
t=19   9EB7BC517FCF18C65F3D605BAC655070   9EB7BC517FCF18D5   AAE1E428B7B76BB1   2B643A972FC0CDB2
EF26EDFEB8D7AF05   5F3D605BAC655070
t=20   FE09727F3CD78BF91C237F2CD1219628   FE09727F3CD78BED   2B643A972FC0CDB2   EF26EDFEB8D7AF05
5F3D605BAC655070   1C237F2CD1219628
t=21   08EC10262E5A74C7F04CDB2E7DE1CBA0   08EC10262E5A74D2   EF26EDFEB8D7AF05   5F3D605BAC655070
1C237F2CD1219628   F04CDB2E7DE1CBA0
t=22   1D4CB9CF9823FA6438F92BC355393AE9   1D4CB9CF9823FA72   5F3D605BAC655070   1C237F2CD1219628
F04CDB2E7DE1CBA0   38F92BC355393AE9
t=23   0C356C66401A65BCA0E4AE8C901912AC   0C356C66401A65AB   1C237F2CD1219628   F04CDB2E7DE1CBA0
38F92BC355393AE9   A0E4AE8C901912AC
t=24   0942747DB07032BB3D3AF0F16D240607   0942747DB07032A3   F04CDB2E7DE1CBA0   38F92BC355393AE9
A0E4AE8C901912AC   3D3AF0F16D240607

CT is
    0942747D B07032A3 F04CDB2E 7DE1CBA0
    38F92BC3 55393AE9 A0E4AE8C 901912AC
    3D3AF0F1 6D240607
==============================================================

Method 3 - TKW
##############################################################

Example 3.1

Wrap 64 bits with 3-key TDES

Key1 is     00010203 04050607
Key2 is     08090A0B 0C0D0E0F
Key3 is     10111213 14151617
PT is       00112233 44556677
--------------------------------------------------------------

Step    TDES Encrypt      A          R[1]       R[2]
```

```
                          A6A6A6A6   00112233   44556677
t= 1   7BA94C3C0A1FD001   7BA94C3D   44556677   0A1FD001
t= 2   268ACDE66CB62750   268ACDE4   0A1FD001   6CB62750
t= 3   D828E3F4D9DD0E9E   D828E3F7   6CB62750   D9DD0E9E
t= 4   C26ED963EDBCBAEB   C26ED967   D9DD0E9E   EDBCBAEB
t= 5   7AAB634843AE4B4B   7AAB634D   EDBCBAEB   43AE4B4B
t= 6   3B14C1A5A9395F3D   3B14C1A3   43AE4B4B   A9395F3D
t= 7   3DAEECFAACA4B062   3DAEECFD   A9395F3D   ACA4B062
t= 8   55291D77E2D070C1   55291D7F   ACA4B062   E2D070C1
t= 9   56DB3DA69588AC9F   56DB3DAF   E2D070C1   9588AC9F
t=10   CF560CDAF358E957   CF560CD0   9588AC9F   F358E957
t=11   F19D0E06B80D82A7   F19D0E0D   F358E957   B80D82A7
t=12   16277D116DE53A76   16277D1D   B80D82A7   6DE53A76

CT is       16277D1D B80D82A7 6DE53A76
==============================================================

Wrap 128 bits with 3-key TDES

Key1 is     00010203 04050607
Key2 is     08090A0B 0C0D0E0F
Key3 is     10111213 14151617
PT is       00112233 44556677 8899AABB CCDDEEFF
--------------------------------------------------------------

Step    TDES Encrypt      A          R[1]       R[2]       R[3]       R[4]
                          A6A6A6A6   00112233   44556677   8899AABB   CCDDEEFF
t= 1   7BA94C3C0A1FD001   7BA94C3D   44556677   8899AABB   CCDDEEFF   0A1FD001
t= 2   268ACDE66CB62750   268ACDE4   8899AABB   CCDDEEFF   0A1FD001   6CB62750
t= 3   BEE0441373E916D1   BEE04410   CCDDEEFF   0A1FD001   6CB62750   73E916D1
t= 4   7FE207EB5EE91330   7FE207EF   0A1FD001   6CB62750   73E916D1   5EE91330
t= 5   8BD1C6F558FEA0C7   8BD1C6F0   6CB62750   73E916D1   5EE91330   58FEA0C7
t= 6   9D3774B823D80E07   9D3774BE   73E916D1   5EE91330   58FEA0C7   23D80E07
t= 7   1B424F514053C308   1B424F56   5EE91330   58FEA0C7   23D80E07   4053C308
t= 8   2C6DCEFC8F1EADC2   2C6DCEF4   58FEA0C7   23D80E07   4053C308   8F1EADC2
t= 9   349BFFF9C30BE982   349BFFF0   23D80E07   4053C308   8F1EADC2   C30BE982
```

```
t=10   D03C77C039BA6E44   D03C77CA   4053C308   8F1EADC2   C30BE982   39BA6E44
t=11   472907DAC5E177A7   472907D1   8F1EADC2   C30BE982   39BA6E44   C5E177A7
t=12   DE2BF0BBCB335117   DE2BF0B7   C30BE982   39BA6E44   C5E177A7   CB335117
t=13   274C0D320CAA0D3E   274C0D3F   39BA6E44   C5E177A7   CB335117   0CAA0D3E
t=14   846A99B1E46BDD1D   846A99BF   C5E177A7   CB335117   0CAA0D3E   E46BDD1D
t=15   3791C7F7C4428FBF   3791C7F8   CB335117   0CAA0D3E   E46BDD1D   C4428FBF
t=16   DFBD77379F99AF78   DFBD7727   0CAA0D3E   E46BDD1D   C4428FBF   9F99AF78
t=17   44FCF75DB4A88880   44FCF74C   E46BDD1D   C4428FBF   9F99AF78   B4A88880
t=18   C32528F4518A879E   C32528E6   C4428FBF   9F99AF78   B4A88880   518A879E
t=19   0F271CEF4EE11034   0F271CFC   9F99AF78   B4A88880   518A879E   4EE11034
t=20   6C430DCD39FF9D67   6C430DD9   B4A88880   518A879E   4EE11034   39FF9D67
t=21   4DD4D2A321D739BA   4DD4D2B6   518A879E   4EE11034   39FF9D67   21D739BA
t=22   AB1194EA33F9619B   AB1194FC   4EE11034   39FF9D67   21D739BA   33F9619B
t=23   FC0A617752D2AB0D   FC0A6160   39FF9D67   21D739BA   33F9619B   52D2AB0D
t=24   75F5F27D29822081   75F5F265   21D739BA   33F9619B   52D2AB0D   29822081

CT is
    75F5F265 21D739BA 33F9619B 52D2AB0D
    29822081
==============================================================
```