

Table C.3 shows 11 test vectors referred to as “case 10” through “case 0.” Case 1 tests XCB-AES-256, while the others test XCB-AES-128 with different combinations of plaintext and associated data lengths.

Table C.3—XCB-AES test cases

```

test_case_t case10 = {
    /* key */
    {
        0xa9, 0x55, 0xec, 0x89, 0xee, 0x6e, 0x0f, 0xf5,
        0xe5, 0x30, 0x34, 0xc5, 0x89, 0x1c, 0x4e, 0x97,
        0x68, 0x30, 0x31, 0x2a, 0x3a, 0x94, 0xb1, 0xe8,
        0x5e, 0x30, 0xeb, 0xc6, 0x34, 0x95, 0x97, 0xea,
    },
    /* bytes in key */
    32,
    /* plaintext */
    {
        0x6e, 0xc7, 0xe1, 0x66, 0x5f, 0x80, 0x6d, 0xf4,
        0xbc, 0xbd, 0x4a, 0x4c, 0x10, 0xa0, 0x6b, 0xd8,
        0x7b, 0xfb, 0x06, 0xf4, 0x17, 0x8a, 0xe5, 0x18,
        0x70, 0x6a, 0x1d, 0x71, 0x5f, 0x44, 0x8b
    },
    /* bytes in plaintext */
    31,
    /* associated data */
    { },
    /* bytes in associated data */
    0,
    /* ciphertext */
    {
        0xfb, 0x9c, 0x5b, 0xfb, 0x11, 0xc5, 0x75, 0x28,
        0x47, 0x64, 0xaa, 0x81, 0xba, 0x18, 0x90, 0x6f,
        0x2d, 0x66, 0xf5, 0x3a, 0x52, 0x3a, 0xd4, 0xfc,
        0x2f, 0x23, 0x53, 0xa4, 0x8f, 0x0b, 0x6f
    },
    NULL
};

test_case_t case9 = {
    /* key */
    {
        0xc9, 0x9a, 0xb8, 0x97, 0xad, 0xdd, 0xcc, 0xca,
        0xb8, 0x4e, 0x0d, 0xf4, 0xea, 0xfc, 0x93, 0xa4,
        0xf7, 0x60, 0xf3, 0x92, 0x69, 0x64, 0x1c, 0x19,
        0xe5, 0x92, 0x9b, 0x71, 0x2d, 0xd3, 0xd0, 0x79,
    },
    /* bytes in key */
    32,
    /* plaintext */
    {
        0xb1, 0x13, 0x50, 0x83, 0x81, 0x22, 0x96, 0x8d,
        0xbb, 0xf2, 0xaa, 0xe6, 0x9b, 0xfd, 0xf5, 0xdb,
        0x5b, 0xff, 0x16, 0x6f, 0xe7, 0x14, 0x03, 0x9b,
        0xd3
}

```

```
},
/* bytes in plaintext */
25,
/* associated data */
{
  0xb7, 0xd6, 0xbb, 0x6d, 0x90, 0x35, 0x22, 0x08,
  0x02, 0x69, 0xb3, 0xa5, 0x75, 0x61, 0x5a, 0xf8,
  0xc7, 0x5a, 0x52, 0xa4, 0x82, 0x86, 0xe3, 0x46,
  0x15, 0xfc, 0x6c, 0x28, 0x9b, 0x09, 0x57,
},
/* bytes in associated data */
31,
/* ciphertext */
{
  0x02, 0x15, 0x47, 0x5a, 0xec, 0xfc, 0xe0, 0x55,
  0x00, 0xc4, 0xcd, 0xc9, 0x06, 0x8c, 0xbb, 0x65,
  0xb6, 0x6b, 0x27, 0x0e, 0xff, 0xa2, 0xe3, 0x08,
  0x9d
},
&case10
};

test_case_t case8 = {
/* key */
{
  0x3b, 0xb9, 0x6b, 0xd5, 0x0b, 0x91, 0xa7, 0xd8,
  0x37, 0x84, 0x45, 0x24, 0x26, 0x2f, 0xef, 0x97,
  0xe0, 0x41, 0x2c, 0xbd, 0x64, 0xa3, 0x91, 0xc1,
  0xd3, 0x93, 0xc1, 0x33, 0x11, 0xf1, 0x9f, 0x86,
},
/* bytes in key */
32,
/* plaintext */
{
  0xf0, 0xae, 0x13, 0x92, 0x99, 0xc1, 0xaf, 0x3d,
  0xd0, 0xe5, 0xa0, 0x4b, 0xe3, 0x2c, 0xd3, 0xe3,
  0x93
},
/* bytes in plaintext */
17,
/* associated data */
{
  0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
  0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
},
/* bytes in associated data */
16,
/* ciphertext */
{
  0x58, 0xe3, 0x6c, 0xeb, 0xc7, 0x41, 0x17, 0x28,
  0xc1, 0x5b, 0xe4, 0xaf, 0xad, 0x3d, 0xfd, 0x0f,
  0x18
},
&case9
};

test_case_t case7 = {
```

```
/* key */
{
    0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07,
    0x08, 0x09, 0x0a, 0x0b, 0x0c, 0x0d, 0x0e, 0x0f,
},
/* bytes in key */
16,
/* plaintext */
{
    0x08, 0x47, 0x1e, 0x46, 0x29, 0x45, 0xa7, 0x41,
    0x54, 0x0f, 0xaa, 0x16, 0xf0, 0x1e, 0x42, 0x1b,
    0x7f, 0xa4, 0x3e, 0x0d, 0x1f, 0x99, 0xf6, 0xa0,
    0x1f, 0x71, 0x26, 0xf9, 0x8a, 0x3f, 0xc9, 0x6a,
    0xd6, 0x8b, 0xf8, 0x6e, 0xa8, 0xd7, 0x2a, 0xab,
    0x5d, 0x98, 0x7d, 0x08, 0x54, 0xea, 0x72, 0xfe,
    0xa7, 0x64, 0x3c, 0x65, 0x84, 0x33, 0xdd, 0x5e,
    0x31, 0xb4, 0x06, 0x70, 0xc6, 0xd6, 0x9d, 0x1b,
    0x4c, 0xe3, 0xac, 0x9d, 0x9f, 0x5f, 0x73, 0xc6,
    0x91, 0x8a, 0xeb, 0x8d, 0x4c, 0x2d, 0xad, 0xbe,
    0x12, 0xe6, 0xd0, 0xc7, 0x2f, 0x4c, 0xa9, 0x1e,
    0x66, 0xc6, 0xbe, 0xbd, 0x32, 0xf0, 0x09, 0x48,
    0x65, 0x81, 0xda, 0x90, 0x18, 0xa7, 0x4b, 0x9c,
    0x7e, 0x28, 0x8f, 0xb1, 0x8f, 0xd6, 0x09, 0x00,
    0xa4, 0x44, 0x8f, 0xab, 0xea, 0xd7, 0x3d, 0x13,
    0xcb, 0x24, 0x83, 0xfb, 0xc8, 0xfb, 0xdf, 0xe9,
    0x30, 0xa1, 0x38, 0x90, 0x55, 0x5c, 0xaa, 0x88,
    0xf4, 0xac, 0xdd, 0x5a, 0x3e, 0x51, 0x59, 0xe5,
    0xa6, 0x46, 0x7e, 0xc7, 0xef, 0x05, 0x23, 0x95,
    0x30, 0x14, 0xe6, 0xde, 0x79, 0x6c, 0xce, 0x7d,
    0x4f, 0xcd, 0x14, 0xb0, 0x67, 0x7a, 0x2d, 0x8e,
    0x50, 0x9f, 0x55, 0xc8, 0x14, 0xed, 0x12, 0xcd,
    0x75, 0x5c, 0xd8, 0xac, 0xb7, 0xbb, 0x12, 0x66,
    0xb4, 0xd7, 0x25, 0xe2, 0x50, 0x55, 0xe4, 0xd3,
    0x60, 0xb7, 0xcd, 0x31, 0xab, 0xdd, 0x5f, 0x42,
    0x92, 0x7a, 0x4c, 0x11, 0x16, 0x30, 0x5f, 0xea,
    0x7e, 0xcb, 0xac, 0x5d, 0xc4, 0x7f, 0xf2, 0xf3,
    0x30, 0xef, 0x10, 0x8d, 0xc8, 0x93, 0xf7, 0xbe,
    0xcd, 0x6e, 0xea, 0xa3, 0x95, 0x74, 0xdb, 0x1e,
    0xe8, 0x42, 0xea, 0xab, 0x10, 0xf1, 0x7c, 0x29,
    0x93, 0x1f, 0x92, 0x52, 0xc1, 0x0c, 0x40, 0x2c,
    0xaa, 0x00, 0xe8, 0x77, 0x2d, 0x54, 0x11, 0x1a,
    0xba, 0x50, 0x6e, 0x4f, 0xef, 0x24, 0x7b, 0x58,
    0xcb, 0x6a, 0xa2, 0xfc, 0xbb, 0xc4, 0xef, 0x91,
    0xc4, 0x04, 0x5d, 0xde, 0x51, 0x32, 0xda, 0x81,
    0x12, 0x12, 0x7c, 0xa4, 0xb0, 0x0b, 0x9c, 0xa9,
    0xa4, 0x28, 0x29, 0xa4, 0xd3, 0x9a, 0xaf, 0x2b,
    0xc1, 0x27, 0xd9, 0xe6, 0x9e, 0x92, 0x4f, 0x01,
    0x69, 0x29, 0xf9, 0x5f, 0x54, 0x68, 0xbe, 0x6f,
    0xc7, 0x41, 0x58, 0xe7, 0x0d, 0xa7, 0x9c, 0x74,
    0x83, 0x54, 0xab, 0x11, 0x81, 0xee, 0xbd, 0x77,
    0x47, 0xf8, 0xfb, 0x44, 0x08, 0x72, 0xd4, 0xb4,
    0xfb, 0xa2, 0x11, 0xfb, 0x4c, 0x00, 0x9a, 0xf0,
    0xd4, 0x1a, 0xc8, 0x13, 0x44, 0x11, 0x20, 0xb9,
    0x62, 0xde, 0x53, 0x01, 0xdd, 0x54, 0x4e, 0x0c,
    0x0b, 0x1a, 0xd4, 0x3f, 0x82, 0x9f, 0x76, 0xa5,
    0x1b, 0x33, 0x1c, 0xd4, 0x26, 0x51, 0xb6, 0xa2,
    0x26, 0x28, 0x42, 0xb9, 0x0c, 0xd2, 0x93, 0x24,
```

```

0x18, 0xd8, 0xb6, 0x70, 0x75, 0x2a, 0x99, 0x25,
0xd2, 0xfb, 0x80, 0xfa, 0x25, 0x23, 0xb4, 0x22,
0x21, 0x21, 0xd0, 0x09, 0x99, 0x7e, 0xf2, 0x22,
0x3a, 0xca, 0x4b, 0x12, 0xe6, 0x28, 0x05, 0x0d,
0xce, 0x8d, 0xa, 0x6b, 0xdc, 0xd5, 0x47, 0x49,
0xe0, 0xda, 0x58, 0xf3, 0xfc, 0xa5, 0x63, 0x91,
0xb5, 0x60, 0x2b, 0x5b, 0xbb, 0x13, 0xd0, 0xf1,
0x2b, 0x1c, 0xd3, 0x0b, 0x45, 0xb6, 0xa7, 0x62,
0x32, 0xdc, 0x27, 0xab, 0x81, 0x97, 0x1f, 0xab,
0xdc, 0xc7, 0x5a, 0xee, 0x7b, 0xb6, 0x8b, 0xf9,
0x35, 0x95, 0x55, 0xe2, 0x04, 0x8c, 0xd4, 0x4b,
0x8e, 0x7a, 0xdb, 0x89, 0x52, 0xe2, 0xf0, 0xfa,
0x3b, 0xda, 0x38, 0xbc, 0xa6, 0x49, 0x72, 0x4a,
0x5f, 0x1d, 0xa, 0xac, 0x41, 0x31, 0x0d, 0x75,
0x78, 0xa6, 0x17, 0x48, 0x88, 0x82, 0xab, 0x66,
0x3f, 0x46, 0x26, 0x19, 0x11, 0xe4, 0xb8, 0x41,
0x27, 0xf3, 0x70, 0x62, 0x3b, 0x9f, 0xf6, 0x2e,
},
/* bytes in plaintext */
520,
/* associated data */
{
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
},
/* bytes in associated data */
16,
/* ciphertext */
{
    0x28, 0xb0, 0xec, 0x43, 0x2f, 0x39, 0x7f, 0x1b,
    0x1a, 0xe9, 0x8e, 0x45, 0x86, 0xd2, 0x92, 0x66,
    0xae, 0x7e, 0x59, 0x78, 0x7c, 0x2d, 0x8e, 0x8b,
    0x3f, 0x3f, 0x1c, 0x10, 0xda, 0xfc, 0x7e, 0x63,
    0x13, 0x21, 0xec, 0x09, 0xe7, 0xa4, 0x7a, 0x04,
    0x92, 0xf1, 0xfb, 0x52, 0xff, 0x11, 0x23, 0xd4,
    0x96, 0xaf, 0xf0, 0xad, 0xbc, 0xb9, 0x32, 0x1c,
    0x9b, 0xd2, 0x91, 0x74, 0xc4, 0x78, 0x2b, 0x28,
    0xb1, 0x18, 0x92, 0x77, 0x72, 0x96, 0xd3, 0x0c,
    0xbc, 0xf0, 0x4f, 0x6e, 0x4f, 0x7a, 0xe6, 0x1a,
    0xc0, 0xa8, 0x6a, 0x06, 0x4c, 0xe9, 0xec, 0xe8,
    0x8b, 0x3a, 0x6d, 0x32, 0xd1, 0x79, 0xba, 0xca,
    0x91, 0x66, 0xcd, 0x15, 0xc5, 0xf1, 0x68, 0x7e,
    0x88, 0x9a, 0x1e, 0xe4, 0x0b, 0x32, 0x78, 0x3b,
    0x02, 0xdd, 0xfd, 0x50, 0x0b, 0x6c, 0xd4, 0x96,
    0xba, 0x1f, 0x5d, 0x7b, 0x6e, 0xd6, 0xfd, 0xee,
    0xfd, 0xc8, 0xc3, 0x6c, 0xa3, 0x81, 0x8b, 0x51,
    0x60, 0xb5, 0x58, 0x82, 0xc6, 0x16, 0x58, 0x03,
    0xdb, 0xbe, 0xe9, 0x5e, 0x12, 0xb5, 0xe2, 0xfd,
    0x4a, 0xa, 0xfd, 0x5d, 0x84, 0x50, 0xd0, 0x98,
    0x3e, 0x30, 0xdb, 0x63, 0x18, 0x1f, 0x9a, 0x2a,
    0x3c, 0xc5, 0x16, 0xf2, 0x07, 0x59, 0x6e, 0xf5,
    0xee, 0x92, 0x7a, 0xfb, 0xf1, 0x41, 0xf0, 0xc5,
    0x5b, 0x0b, 0x08, 0x13, 0xe2, 0x99, 0x5b, 0x7c,
    0x4c, 0x13, 0xc0, 0x22, 0xe0, 0xba, 0x00, 0x42,
    0x27, 0x8b, 0x13, 0x32, 0x39, 0x1d, 0xb8, 0x9c,
    0x5d, 0xec, 0x68, 0x2f, 0xcd, 0xba, 0xdf, 0xba,
    0x6c, 0x01, 0x83, 0x25, 0x48, 0x47, 0x8f, 0x60,
}

```

```

0x06, 0x21, 0x98, 0xa9, 0x5c, 0x85, 0xa3, 0xc8,
0xf6, 0x33, 0x75, 0x3d, 0xc1, 0xe2, 0x9a, 0xc5,
0x60, 0xf5, 0xf5, 0xf8, 0x1d, 0x9e, 0xaa, 0x24,
0x00, 0x76, 0x65, 0x6b, 0x84, 0xe1, 0xd9, 0x20,
0xb9, 0xd9, 0x68, 0xee, 0xb8, 0x4c, 0x74, 0x1a,
0x22, 0x54, 0xe5, 0x11, 0x2c, 0x33, 0x92, 0xfb,
0xd4, 0xf9, 0xb2, 0xdd, 0x30, 0x75, 0x2b, 0xf2,
0x69, 0xef, 0x30, 0xa3, 0xca, 0x5c, 0x67, 0x35,
0x6e, 0x4e, 0x53, 0xd9, 0xda, 0x6a, 0x1b, 0x99,
0x55, 0x38, 0x1f, 0x85, 0x49, 0x1e, 0x52, 0xaa,
0xdc, 0x38, 0xd8, 0x69, 0x61, 0xec, 0x53, 0x47,
0xa7, 0x24, 0x04, 0xfc, 0x50, 0xd7, 0x33, 0x11,
0xd8, 0x20, 0x00, 0x86, 0x98, 0x3e, 0x50, 0x35,
0xff, 0x02, 0xb1, 0xf8, 0xf1, 0x44, 0xea, 0xef,
0x31, 0x75, 0x12, 0x3a, 0xf4, 0x97, 0x0f, 0xc7,
0x7e, 0x76, 0x91, 0xce, 0xe4, 0x50, 0x1d, 0x94,
0x90, 0x69, 0xd6, 0x11, 0x6b, 0xf1, 0xb3, 0x01,
0x2e, 0xac, 0x51, 0x07, 0x36, 0xc0, 0x9c, 0xfc,
0x63, 0x6d, 0x01, 0x64, 0xf6, 0x9f, 0x52, 0x53,
0xf4, 0xb4, 0x16, 0x2c, 0x5e, 0x55, 0x98, 0xcb,
0x7b, 0x0f, 0x95, 0xff, 0xe4, 0xc0, 0x78, 0x97,
0x1b, 0xe5, 0x49, 0x52, 0x0d, 0xec, 0x65, 0x5d,
0xd6, 0x1d, 0x36, 0xcc, 0xa9, 0xd2, 0x6b, 0xaa,
0x02, 0xb1, 0x8c, 0xed, 0x48, 0xfb, 0xee, 0xb4,
0xb8, 0x42, 0xc0, 0x45, 0xc3, 0xc1, 0x18, 0x81,
0xdc, 0x83, 0x76, 0xc5, 0xda, 0xfc, 0x82, 0xac,
0xc6, 0xda, 0x45, 0x3a, 0xd3, 0xa1, 0x21, 0x39,
0xab, 0x0f, 0x0f, 0x6d, 0xd7, 0xdf, 0x3b, 0x1e,
0xe4, 0xaa, 0x71, 0x42, 0x8a, 0x19, 0xff, 0x97,
0x31, 0x92, 0xeb, 0xd6, 0x0d, 0x6d, 0xe6, 0x98,
0x84, 0xff, 0x99, 0xe9, 0x0d, 0xea, 0x4e, 0x5f,
0xc0, 0xab, 0xa0, 0xa6, 0x0d, 0x96, 0x7d, 0x60,
0x0b, 0xdd, 0x25, 0x9d, 0x5d, 0x63, 0xb3, 0xb9,
0xd4, 0x85, 0x9e, 0xf7, 0x5d, 0x3d, 0xbd, 0xe2,
0xd1, 0x4f, 0x17, 0x66, 0x07, 0xff, 0x3c, 0x1d,
0xe5, 0xf6, 0x28, 0xc2, 0xfc, 0x65, 0x5f, 0x33,
0x32, 0x29, 0xf7, 0x48, 0x12, 0x27, 0x98, 0xe3
},
&case8
};

test_case_t case6 = {
/* key */
{
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x16, 0x16, 0xdd, 0xa6
},
/* bytes in key */
16,
/* plaintext */
{
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00
},
/* bytes in plaintext */
}

```

```
24,
/* associated data */
{
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
},
/* bytes in associated data */
16,
/* ciphertext */
{
    0x70, 0x13, 0xfd, 0xe3, 0xc3, 0x9f, 0xa1, 0xa4,
    0x3f, 0x5a, 0xb4, 0x34, 0x5a, 0xbf, 0xe5, 0xd9,
    0xcf, 0x80, 0x85, 0xf8, 0x7e, 0xb3, 0x11, 0x89,
},
&case7
};

test_case_t case5 = {
/* key */
{
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x16, 0x16, 0xdd, 0xa6
},
/* bytes in key */
16,
/* plaintext */
{
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00
},
20,
/* associated data */
{
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00
},
/* bytes in associated data */
16,
/* ciphertext */
{
    0x70, 0x13, 0xfd, 0xe3, 0xdb, 0x56, 0x19, 0xbf,
    0xa4, 0xed, 0x25, 0x6d, 0xb4, 0x44, 0x15, 0x68,
    0x7a, 0xa4, 0x50, 0x3f
},
&case6
};

test_case_t case4 = {
/* key */
{
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0xf3, 0x24, 0x6b, 0x19
},
/* bytes in key */
16,
/* plaintext */
{
```

```

0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
},
/* bytes in plaintext */
16,
/* associated data */
{
    0x80, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
},
/* bytes in associated data */
16,
/* ciphertext */
{
    0x28, 0x2a, 0x71, 0x43, 0x39, 0xae, 0x66, 0x8c,
    0x3c, 0x20, 0x2a, 0xca, 0x9c, 0x71, 0xe0, 0xb,
},
&case5
};

test_case_t case3 = {
/* key */
{
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x16, 0x16, 0xdd, 0xa6,
},
/* bytes in key */
16,
/* plaintext */
{
    0x80, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, /* 32 */
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, /* 64 */
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, /* 96 */
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, /* 128 */
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, /* 160 */
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, /* 192 */
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00
}

```

```

0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, /* 224 */
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, /* 256 */
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, /* 288 */
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, /* 320 */
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, /* 352 */
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, /* 384 */
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, /* 416 */
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, /* 448 */
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, /* 480 */
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, /* 512 */
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00
},
/* bytes in plaintext */
512,
/* associated data */
{
    0x80, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
},
/* bytes in associated data */
16,
/* ciphertext */
{
    0xbf, 0x2c, 0x04, 0x93, 0xbb, 0xb4, 0xbd, 0x55,
    0xcc, 0x11, 0xc0, 0x3d, 0xd9, 0x25, 0x1b, 0xe5,
    0x83, 0x79, 0x9f, 0x9d, 0xba, 0xcf, 0x23, 0x16,
    0x7a, 0x4c, 0x5e, 0xf0, 0x3e, 0x0d, 0xb9, 0x40,
    0x4e, 0x4e, 0xee, 0xb3, 0x5d, 0xdf, 0x15, 0x1d,
    0x23, 0x9e, 0x8b, 0x78, 0xc2, 0x64, 0x08, 0x24,
    0xce, 0x1f, 0x10, 0x6e, 0xab, 0x1c, 0x01, 0x9a,
    0xca, 0xd3, 0x98, 0x56, 0x31, 0xc7, 0x0c, 0x36,
}

```

```

0x3f, 0x30, 0x15, 0xf5, 0xec, 0x41, 0xc8, 0x82,
0x5e, 0xc4, 0xf4, 0x7f, 0x9e, 0xa0, 0x4d, 0x7e,
0xdc, 0x17, 0x34, 0x1f, 0x5c, 0x41, 0x98, 0x9c,
0x56, 0x3c, 0x6a, 0xc2, 0xac, 0x4e, 0xd8, 0xac,
0x6b, 0xa4, 0x61, 0xfc, 0xaf, 0xb0, 0xb4, 0x1e,
0x64, 0x4b, 0x00, 0x3c, 0xa3, 0xcf, 0x52, 0x60,
0x73, 0xa1, 0xef, 0x97, 0x21, 0x7d, 0xf0, 0x3e,
0x26, 0xbb, 0xd0, 0x22, 0xee, 0x27, 0x9f, 0x06,
0x95, 0x3c, 0xa3, 0xcd, 0xfd, 0xb4, 0x3d, 0x49,
0x20, 0xf3, 0x2e, 0xd6, 0x87, 0xd7, 0x81, 0x11,
0x32, 0x84, 0xb1, 0x7d, 0x34, 0x10, 0x72, 0x58,
0x1a, 0x3b, 0x38, 0xe7, 0x9f, 0x65, 0xd7, 0x54,
0x9f, 0x80, 0x39, 0x00, 0x74, 0x5f, 0x37, 0x94,
0xbf, 0x71, 0x75, 0xa8, 0xca, 0xeb, 0x62, 0xb7,
0x96, 0x6f, 0xf7, 0xa2, 0xb7, 0x0f, 0xdf, 0x1f,
0x12, 0x3f, 0x98, 0x26, 0x65, 0x2e, 0xda, 0x09,
0x7e, 0x7f, 0x39, 0x2d, 0xf8, 0xd0, 0xa9, 0xc4,
0xf4, 0x4b, 0xa4, 0x0e, 0x54, 0xb9, 0x71, 0xbe,
0x31, 0x87, 0x6f, 0x1e, 0x43, 0xaa, 0x1f, 0x65,
0xf5, 0xa6, 0x0e, 0xbf, 0x53, 0xf1, 0xea, 0x9b,
0x8f, 0x9b, 0xc6, 0x37, 0x31, 0xfa, 0xbb, 0xb4,
0xdf, 0xcb, 0xd2, 0xbc, 0xa9, 0x94, 0x70, 0x37,
0x8f, 0x5a, 0x91, 0xc2, 0xf1, 0xbc, 0xb0, 0x80,
0x10, 0xea, 0xfa, 0x3e, 0x32, 0xf3, 0xac, 0xe6,
0xd3, 0xc9, 0xe9, 0x1d, 0x12, 0xd7, 0x9a, 0x78,
0x3d, 0xb3, 0xf8, 0xdf, 0xec, 0xdd, 0xd8, 0x1a,
0xda, 0xb8, 0x79, 0x03, 0x75, 0x28, 0x8c, 0x5d,
0xf9, 0xee, 0xa4, 0xa6, 0x63, 0xb5, 0x45, 0x6a,
0x02, 0xdc, 0x4f, 0xe4, 0x4c, 0xd9, 0x82, 0x1c,
0x77, 0x3b, 0xdc, 0xfd, 0xf8, 0xc5, 0xe0, 0x68,
0x65, 0x22, 0xab, 0x40, 0x98, 0x50, 0x01, 0x0f,
0x34, 0xe9, 0xa, 0x64, 0x2c, 0xa, 0x96, 0xf2,
0xbd, 0xa3, 0xe9, 0x75, 0x8b, 0xfd, 0xd5, 0x18,
0x47, 0xa7, 0x15, 0xb0, 0xb8, 0xcf, 0x12, 0xc2,
0x29, 0xf4, 0x39, 0x3d, 0xa6, 0xc8, 0x49, 0x72,
0xf7, 0x3f, 0x2b, 0x2f, 0x72, 0xb7, 0x5d, 0x03,
0x23, 0xe5, 0x9a, 0x48, 0xe3, 0xf2, 0x08, 0xe6,
0x6d, 0xe7, 0x2f, 0x4d, 0x9a, 0x44, 0x04, 0x75,
0x2a, 0xc7, 0x0f, 0x04, 0xe6, 0x47, 0x25, 0x27,
0x1b, 0xd3, 0xff, 0xf2, 0x6c, 0xd7, 0xb4, 0x19,
0x1d, 0x0d, 0xe3, 0xf7, 0x19, 0x63, 0xd7, 0x6e,
0xf5, 0xda, 0x72, 0xbf, 0x7e, 0xf6, 0xd4, 0xdb,
0xd7, 0x87, 0xce, 0xa1, 0x8a, 0x13, 0x6f, 0x01,
0x2b, 0x2d, 0x8c, 0x8b, 0x50, 0x83, 0xdd, 0xcc,
0xf8, 0xc2, 0x86, 0x41, 0xb6, 0x25, 0x60, 0x17,
0x5f, 0x6d, 0x28, 0xea, 0xdd, 0xa5, 0xc9, 0xa1,
0x5b, 0xf1, 0x53, 0xa5, 0xfd, 0x01, 0x16, 0xdf,
0xd4, 0xf5, 0x62, 0x2a, 0x8f, 0x18, 0xd0, 0x7d,
0x55, 0x93, 0x03, 0xe2, 0xe8, 0xdd, 0x10, 0x1c,
0x17, 0x0f, 0xe8, 0x35, 0x88, 0xfb, 0xe2, 0x00,
0x5e, 0x90, 0x07, 0x1b, 0xb0, 0x70, 0x64, 0xcd,
0x36, 0x2e, 0x15, 0x32, 0x31, 0x1c, 0x06, 0x7e,
0xf4, 0xa7, 0xa5, 0x00, 0xe3, 0x5e, 0x20, 0xc5,
0x82, 0x05, 0x98, 0x18, 0xb3, 0x3e, 0xd0, 0x66,
0x3f, 0x7a, 0xe0, 0xa0, 0xb2, 0xc8, 0x87, 0xef,
0x72, 0x30, 0x91, 0x79, 0x9f, 0xaf, 0xfd, 0xbb,
},

```

```
&case4
};

test_case_t case2 = {
/* key */
{
    0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07,
    0x08, 0x09, 0x0a, 0x0b, 0x0c, 0x0d, 0x0e, 0x0f,
},
/* bytes in key */
16,
/* plaintext */
{
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00
},
/* bytes in plaintext */
48,
/* associated data */
{
    0x80, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
},
/* bytes in associated data */
16,
/* ciphertext */
{
    0x97, 0xc6, 0xb2, 0xb7, 0x19, 0xa9, 0x54, 0xe3,
    0x3b, 0xab, 0x39, 0xa, 0xf2, 0x57, 0xeb, 0x4c,
    0x59, 0x93, 0xdd, 0x9a, 0x1a, 0x36, 0x61, 0xd5,
    0xb1, 0x52, 0xf8, 0xd6, 0x5f, 0x35, 0x37, 0xb9,
    0x54, 0x34, 0xff, 0xf3, 0x35, 0x2d, 0xfe, 0xb6,
    0x61, 0x5e, 0xc1, 0xb1, 0xc6, 0x6d, 0x81, 0x5d,
},
&case3
};

test_case_t case1 = {
/* key */
{
    0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07,
    0x08, 0x09, 0x0a, 0x0b, 0x0c, 0x0d, 0x0e, 0x0f,
    0x10, 0x11, 0x12, 0x13, 0x14, 0x15, 0x16, 0x17,
    0x18, 0x19, 0x1a, 0x1b, 0x1c, 0x1d, 0x1e, 0x1f,
},
/* bytes in key */
32,
```

```

/* plaintext */
{
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00
},
/* bytes in plaintext */
32,
/* associated data */
{
    0x80, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00
},
/* bytes in associated data */
16,
/* ciphertext */
{
    0x0a, 0xa2, 0x7c, 0x16, 0x7b, 0x7a, 0x6f, 0x13,
    0x93, 0x23, 0x4c, 0xb1, 0x82, 0x8f, 0x73, 0x7c,
    0xe5, 0x3d, 0xa9, 0xf5, 0x05, 0x8e, 0xbd, 0x81,
    0xf4, 0x4b, 0xfb, 0x8a, 0xa6, 0x4a, 0xe6, 0xc1
},
&case2
};

test_case_t case0 = {
/* key */
{
    0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07,
    0x08, 0x09, 0xa, 0xb, 0xc, 0xd, 0xe, 0xf
},
/* bytes in key */
16,
/* plaintext */
{
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00
},
/* bytes in plaintext */
32,
/* associated data */
{
    0x80, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00
},
/* bytes in associated data */
16,
/* ciphertext */
{
    0xf7, 0x27, 0xd7, 0x48, 0xb8, 0x6e, 0x3b, 0x36,
    0x2f, 0x20, 0x81, 0x0e, 0xed, 0xbe, 0x37, 0x8a,
}

```

```
0x07, 0x76, 0x16, 0x31, 0xb9, 0x00, 0x94, 0x54,  
0xd5, 0x4d, 0x8d, 0x94, 0x9c, 0x35, 0x27, 0x19,  
,  
&case1  
};
```