```
//XTEA
//k is a 16 byte key (128 bits)
//
//N=0
//encrypts an 8 byte plain text to an 8 byte cypher text
//
//N<>0
//decrypts an 8 byte cypher text to an 8 byte plain text
//
//long’s are 32bit unsigned integers

void XTEA(long * v, long * k, long N){

unsigned long y=v[0];
unsigned long z=v[1];
unsigned long DELTA=0x9E3779B9;

if (N>0)
    {
    unsigned long limit=DELTA*N;
    unsigned long sum=0;
    while (sum != limit)
        {
        y += ((z<<4 ^ z>>5) + z) ^ (sum + k[sum & 3]);
        sum += DELTA;
        z += ((y<<4 ^ y>>5) + y) ^ (sum + k[(sum>>11) & 3]);
        }
    }
else
    {
    while(sum)
        {
        z -= ((y<<4 ^ y>>5) + y) ^ (sum + k[(sum>>11) & 3]);
        sum -= DELTA;
        y -= ((z<<4 ^ z>>5) + z) ^ (sum + k[sum & 3]);
        }
    }

v[0]=y;
v[1]=z;

return;
}
```

```
//test vectors
//
//from K1,P1,C1
//
//Key data                             Plain text         Cypher text
//  k[3]     k[2]     k[1]     k[0]      v[1]     v[0]  >>  v[1]     v[0]
//-------------------------------------------------------------------------
//A6EB923D 60E2ACAA C1DA8993 27F917B1  547571AA AF20A390  0A202283 D26428AF
//

u32 k1[4]={0x27F917B1,0xC1DA8993,0x60E2ACAA,0xA6EB923D};
u32 p1[2]={0xAF20A390,0x547571AA};
u32 c1[2]={0xD26428AF,0x0A202283};

u32 k2[4]={0x31415926,0x53589793,0x23846264,0x33832795};
u32 p2[2]={0x02884197,0x16939937}; /* 48 digits of PI */
u32 c2[2]={0x46E2007D,0x58BBC2EA};

u32 k3[4]={0x1234ABC1,0x234ABC12,0x34ABC123,0x4ABC1234};
u32 p3[2]={0xABC1234A,0xBC1234AB};
u32 c3[2]={0x5C0754C1,0xF6F0BD9B};

u32 k4[4]={0xABC1234A,0xBC1234AB,0xC1234ABC,0x1234ABC1};
u32 p4[2]={0x234ABC12,0x34ABC123};
u32 c4[2]={0xCDFCC72C,0x24BC116B};

u32 k5[4]={0xDEADBEEF,0xDEADBEEF,0xDEADBEEF,0xDEADBEEF};
u32 p5[2]={0xDEADBEEF,0xDEADBEEF};
u32 c5[2]={0xFAF28CB5,0x0940C0E0};

u32 k6[4]={0xDEADBEEF,0xDEADBEEF,0xDEADBEEF,0xDEADBEEF};
u32 p6[2]={0x9647A918,0x9EC565D5};
u32 c6[2]={0xDEADBEEF,0xDEADBEEF};

u32 k7[4]={1234567890,1234567890,1234567890,1234567890};
u32 p7[2]={1234567890,1234567890}; /* DECIMAL, not HEX */
u32 c7[2]={1774989243,3795101296};

u32 k8[4]={1234567890,1234567890,1234567890,1234567890};
u32 p8[2]={1959019084,2694092002}; /* DECIMAL, not HEX */
u32 c8[2]={1234567890,1234567890};
```