```
/*****************************************************************************
  File name:    SM2_ENC.h
  Version:      SM2_ENC_V1.1
  Date:         Sep 27,2016
  Description:  implementation of SM2 encryption algorithm and decryption algorithm
  Function List:
        1.SM2_init                      //initiate SM2 curve
        2.SM2_ENC                       //SM2 encryption, calls SM3_KDF
        3.SM2_DEC                       //SM2 decryption, calls
SM2_KDF,Test_null,Test_Point,SM3_init,SM3_process,SM3_done
        4.SM2_ENC_SelfTest              //test whether the calculation is correct by comparing
the result with the standard data
        5.Test_Point                    //test if the given point is on SM2 curve
        6.Test_Pubkey                   //test if the given public key is valid
        7.Test_Null                     //test if the geiven array is all zero
        8.SM2_KeyGeneration             //calculate a pubKey out of a given priKey
        9.SM3_init                      //init SM3 state
        10.SM3_process                  //compress the the message
        11.SM3_done                     //compress the rest message and output the hash value
        12.SM3_KDF                      //key deviding function base on SM3, generates key
stream
 Notes:
    This SM2 implementation source code can be used for academic, non-profit making or
non-commercial use only.
    This SM2 implementation is created on MIRACL. SM2 implementation source code provider does
not provide MIRACL library, MIRACL license or any permission to use MIRACL library. Any commercial
use of MIRACL requires a license which may be obtained from Shamus Software Ltd.
*****************************************************************************/


#define ECC_WORDSIZE         8
#define SM2_NUMBITS         256
#define  SM2_NUMWORD        (SM2_NUMBITS/ECC_WORDSIZE)  //32

#define ERR_INFINITY_POINT              0x00000001
#define ERR_NOT_VALID_ELEMENT           0x00000002
#define ERR_NOT_VALID_POINT             0x00000003
#define ERR_ORDER                       0x00000004
#define ERR_ARRAY_NULL                  0x00000005
#define ERR_C3_MATCH                    0x00000006
#define ERR_ECURVE_INIT                 0x00000007
#define ERR_SELFTEST_KG                 0x00000008
#define ERR_SELFTEST_ENC                0x00000009
#define ERR_SELFTEST_DEC                0x0000000A
```

```
unsigned char SM2_p[32] =
{0xFF,0xFF,0xFF,0xFE,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,

0xFF,0xFF,0xFF,0xFF,0x00,0x00,0x00,0x00,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF};
unsigned char SM2_a[32] =
{0xFF,0xFF,0xFF,0xFE,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,

0xFF,0xFF,0xFF,0xFF,0x00,0x00,0x00,0x00,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFC};
unsigned char SM2_b[32] =
{0x28,0xE9,0xFA,0x9E,0x9D,0x9F,0x5E,0x34,0x4D,0x5A,0x9E,0x4B,0xCF,0x65,0x09,0xA7,

0xF3,0x97,0x89,0xF5,0x15,0xAB,0x8F,0x92,0xDD,0xBC,0xBD,0x41,0x4D,0x94,0x0E,0x93};
unsigned char SM2_n[32] =
{0xFF,0xFF,0xFF,0xFE,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,

0x72,0x03,0xDF,0x6B,0x21,0xC6,0x05,0x2B,0x53,0xBB,0xF4,0x09,0x39,0xD5,0x41,0x23};
unsigned char SM2_Gx[32]=
{0x32,0xC4,0xAE,0x2C,0x1F,0x19,0x81,0x19,0x5F,0x99,0x04,0x46,0x6A,0x39,0xC9,0x94,

0x8F,0xE3,0x0B,0xBF,0xF2,0x66,0x0B,0xE1,0x71,0x5A,0x45,0x89,0x33,0x4C,0x74,0xC7};
unsigned char SM2_Gy[32]=
{0xBC,0x37,0x36,0xA2,0xF4,0xF6,0x77,0x9C,0x59,0xBD,0xCE,0xE3,0x6B,0x69,0x21,0x53,

0xD0,0xA9,0x87,0x7C,0xC6,0x2A,0x47,0x40,0x02,0xDF,0x32,0xE5,0x21,0x39,0xF0,0xA0};
unsigned char SM2_h[32]=
{0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,

0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x01};

big para_p,para_a,para_b,para_n,para_Gx,para_Gy,para_h;
epoint *G;
miracl *mip;



int Test_Point(epoint* point);
int Test_PubKey(epoint *pubKey);
int Test_Null(unsigned char array[],int len);
int SM2_Init();
int SM2_KeyGeneration(big priKey,epoint *pubKey);
int SM2_Encrypt(unsigned char* randK,epoint *pubKey,unsigned char M[],int klen,unsigned char
C[]);
int SM2_Decrypt(big dB,unsigned char C[],int Clen,unsigned char M[]);
```

```
int SM2_ENC_SelfTest();
```