NAME

libmtp −

SYNOPSIS

```
#include 'config.h'
#include 'libmtp.h'
#include 'unicode.h'
#include 'ptp.h'
#include 'libusb-glue.h'
#include 'device-flags.h'
#include 'playlist-spl.h'
#include 'util.h'
#include 'mtpz.h'
#include <gcrypt.h>
#include <stdlib.h>
#include <unistd.h>
#include <string.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <time.h>
#include <errno.h>
```

Data Structures

struct **mtpz_rsa_struct**

Macros

#define **MTPZ_HASHSTATE_84** 5
#define **MTPZ_HASHSTATE_88** 6
#define **MTPZ_ENCRYPTIONLOBYTE**(val) (((val) >> 24) & 0xFF)
#define **MTPZ_ENCRYPTIONBYTE1**(val) (((val) >> 16) & 0xFF)
#define **MTPZ_ENCRYPTIONBYTE2**(val) (((val) >> 8) & 0xFF)
#define **MTPZ_ENCRYPTIONBYTE3**(val) (((val) >> 0) & 0xFF)
#define **MTPZ_SWAP**(x) mtpz_bswap32(x)

Typedefs

typedef struct **mtpz_rsa_struct mtpz_rsa_t**

Functions

int **mtpz_loaddata** ()
mtpz_rsa_t * **mtpz_rsa_init** (const unsigned char *modulus, const unsigned char *priv_key, const unsigned char *pub_exp)
void **mtpz_rsa_free** (**mtpz_rsa_t** *)
int **mtpz_rsa_decrypt** (int flen, unsigned char *from, int tlen, unsigned char *to, **mtpz_rsa_t** *rsa)
int **mtpz_rsa_sign** (int flen, unsigned char *from, int tlen, unsigned char *to, **mtpz_rsa_t** *rsa)
void **mtpz_encryption_cipher** (unsigned char *data, unsigned int len, char encrypt)
void **mtpz_encryption_cipher_advanced** (unsigned char *key, unsigned int key_len, unsigned char *data, unsigned int data_len, char encrypt)
unsigned char * **mtpz_encryption_expand_key** (unsigned char *constant, int key_len, int count, int *out_len)
void **mtpz_encryption_expand_key_inner** (unsigned char *constant, int key_len, unsigned char **out, int *out_len)
void **mtpz_encryption_inv_mix_columns** (unsigned char *expanded, int offset, int rounds)
void **mtpz_encryption_decrypt_custom** (unsigned char *data, unsigned char *seed, unsigned char *expanded)
void **mtpz_encryption_encrypt_custom** (unsigned char *data, unsigned char *seed, unsigned char *expanded)
void **mtpz_encryption_encrypt_mac** (unsigned char *hash, unsigned int hash_length, unsigned char *seed, unsigned int seed_len, unsigned char *out)
uint16_t **ptp_mtpz_handshake** (**PTPParams** *params)

Variables

unsigned char **mtpz_aes_rcon** []
unsigned char **mtpz_aes_sbox** []
unsigned char **mtpz_aes_invsbox** []
unsigned int **mtpz_aes_ft1** []
unsigned int **mtpz_aes_ft2** []
unsigned int **mtpz_aes_ft3** []
unsigned int **mtpz_aes_ft4** []
unsigned int **mtpz_aes_rt1** []
unsigned int **mtpz_aes_rt2** []
unsigned int **mtpz_aes_rt3** []
unsigned int **mtpz_aes_rt4** []
unsigned int **mtpz_aes_gb11** []
unsigned int **mtpz_aes_gb14** []
unsigned int **mtpz_aes_gb13** []
unsigned int **mtpz_aes_gb9** []

Detailed Description

This file provides mtp zune cryptographic setup interfaces. It is also used with Windows Phone 7, but Microsoft/Nokiad seem to have discontinued MTPZ on Windows Phone 8.

DISCLAIMER:

The intention of this implementation is for users to be able to interoperate with their devices, i.e. copy music to them in operating systems other than Microsoft Windows, so it can be played back on the device. We do not provide encryption keys and constants in libmtp, we never will. You have to have these on file in your home directory in $HOME/.mtpz-data, and we suggest that you talk to Microsoft about providing the proper numbers if you want to use this facility.

Variable Documentation

unsigned char mtpz_aes_invsbox

Initial value:

=
{
0x52, 0x09, 0x6A, 0xD5, 0x30, 0x36, 0xA5, 0x38, 0xBF, 0x40, 0xA3, 0x9E, 0x81, 0xF3, 0xD7, 0xFB, 0x7C, 0xE3, 0x39, 0x82, 0x9B, 0x2F, 0xFF, 0x87, 0x34, 0x8E, 0x43, 0x44, 0xC4, 0xDE, 0xE9, 0xCB, 0x54, 0x7B, 0x94, 0x32, 0xA6, 0xC2, 0x23, 0x3D, 0xEE, 0x4C, 0x95, 0x0B, 0x42, 0xFA, 0xC3, 0x4E, 0x08, 0x2E, 0xA1, 0x66, 0x28, 0xD9, 0x24, 0xB2, 0x76, 0x5B, 0xA2, 0x49, 0x6D, 0x8B, 0xD1, 0x25, 0x72, 0xF8, 0xF6, 0x64, 0x86, 0x68, 0x98, 0x16, 0xD4, 0xA4, 0x5C, 0xCC, 0x5D, 0x65, 0xB6, 0x92, 0x6C, 0x70, 0x48, 0x50, 0xFD, 0xED, 0xB9, 0xDA, 0x5E, 0x15, 0x46, 0x57, 0xA7, 0x8D, 0x9D, 0x84, 0x90, 0xD8, 0xAB, 0x00, 0x8C, 0xBC, 0xD3, 0x0A, 0xF7, 0xE4, 0x58, 0x05, 0xB8, 0xB3, 0x45, 0x06, 0xD0, 0x2C, 0x1E, 0x8F, 0xCA, 0x3F, 0x0F, 0x02, 0xC1, 0xAF, 0xBD, 0x03, 0x01, 0x13, 0x8A, 0x6B, 0x3A, 0x91, 0x11, 0x41, 0x4F, 0x67, 0xDC, 0xEA, 0x97, 0xF2, 0xCF, 0xCE, 0xF0, 0xB4, 0xE6, 0x73, 0x96, 0xAC, 0x74, 0x22, 0xE7, 0xAD, 0x35, 0x85, 0xE2, 0xF9, 0x37, 0xE8, 0x1C, 0x75, 0xDF, 0x6E, 0x47, 0xF1, 0x1A, 0x71, 0x1D, 0x29, 0xC5, 0x89, 0x6F, 0xB7, 0x62, 0x0E, 0xAA, 0x18, 0xBE, 0x1B, 0xFC, 0x56, 0x3E, 0x4B, 0xC6, 0xD2, 0x79, 0x20, 0x9A, 0xDB, 0xC0, 0xFE, 0x78, 0xCD, 0x5A, 0xF4, 0x1F, 0xDD, 0xA8, 0x33, 0x88, 0x07, 0xC7, 0x31, 0xB1, 0x12, 0x10, 0x59, 0x27, 0x80, 0xEC, 0x5F, 0x60, 0x51, 0x7F, 0xA9, 0x19, 0xB5, 0x4A, 0x0D, 0x2D, 0xE5, 0x7A, 0x9F, 0x93, 0xC9, 0x9C, 0xEF, 0xA0, 0xE0, 0x3B, 0x4D, 0xAE, 0x2A, 0xF5, 0xB0, 0xC8, 0xEB, 0xBB, 0x3C, 0x83, 0x53, 0x99, 0x61,

0x17, 0x2B, 0x04, 0x7E, 0xBA, 0x77, 0xD6, 0x26, 0xE1, 0x69, 0x14, 0x63, 0x55, 0x21, 0x0C, 0x7D
}

unsigned char mtpz_aes_rcon

Initial value:

=
{
0x01, 0x02, 0x04, 0x08, 0x10, 0x20, 0x40, 0x80, 0x1b, 0x36, 0x6c, 0xd8, 0xab, 0x4d, 0x9a
}

unsigned char mtpz_aes_sbox

Initial value:

=
{
0x63, 0x7c, 0x77, 0x7b, 0xf2, 0x6b, 0x6f, 0xc5, 0x30, 0x01,
0x67, 0x2b, 0xfe, 0xd7, 0xab, 0x76, 0xca, 0x82, 0xc9, 0x7d,
0xfa, 0x59, 0x47, 0xf0, 0xad, 0xd4, 0xa2, 0xaf, 0x9c, 0xa4,
0x72, 0xc0, 0xb7, 0xfd, 0x93, 0x26, 0x36, 0x3f, 0xf7, 0xcc,
0x34, 0xa5, 0xe5, 0xf1, 0x71, 0xd8, 0x31, 0x15, 0x04, 0xc7,
0x23, 0xc3, 0x18, 0x96, 0x05, 0x9a, 0x07, 0x12, 0x80, 0xe2,
0xeb, 0x27, 0xb2, 0x75, 0x09, 0x83, 0x2c, 0x1a, 0x1b, 0x6e,
0x5a, 0xa0, 0x52, 0x3b, 0xd6, 0xb3, 0x29, 0xe3, 0x2f, 0x84,
0x53, 0xd1, 0x00, 0xed, 0x20, 0xfc, 0xb1, 0x5b, 0x6a, 0xcb,
0xbe, 0x39, 0x4a, 0x4c, 0x58, 0xcf, 0xd0, 0xef, 0xaa, 0xfb,
0x43, 0x4d, 0x33, 0x85, 0x45, 0xf9, 0x02, 0x7f, 0x50, 0x3c,
0x9f, 0xa8, 0x51, 0xa3, 0x40, 0x8f, 0x92, 0x9d, 0x38, 0xf5,
0xbc, 0xb6, 0xda, 0x21, 0x10, 0xff, 0xf3, 0xd2, 0xcd, 0x0c,
0x13, 0xec, 0x5f, 0x97, 0x44, 0x17, 0xc4, 0xa7, 0x7e, 0x3d,
0x64, 0x5d, 0x19, 0x73, 0x60, 0x81, 0x4f, 0xdc, 0x22, 0x2a,
0x90, 0x88, 0x46, 0xee, 0xb8, 0x14, 0xde, 0x5e, 0x0b, 0xdb,
0xe0, 0x32, 0x3a, 0x0a, 0x49, 0x06, 0x24, 0x5c, 0xc2, 0xd3,
0xac, 0x62, 0x91, 0x95, 0xe4, 0x79, 0xe7, 0xc8, 0x37, 0x6d,
0x8d, 0xd5, 0x4e, 0xa9, 0x6c, 0x56, 0xf4, 0xea, 0x65, 0x7a,
0xae, 0x08, 0xba, 0x78, 0x25, 0x2e, 0x1c, 0xa6, 0xb4, 0xc6,
0xe8, 0xdd, 0x74, 0x1f, 0x4b, 0xbd, 0x8b, 0x8a, 0x70, 0x3e,
0xb5, 0x66, 0x48, 0x03, 0xf6, 0x0e, 0x61, 0x35, 0x57, 0xb9,
0x86, 0xc1, 0x1d, 0x9e, 0xe1, 0xf8, 0x98, 0x11, 0x69, 0xd9,
0x8e, 0x94, 0x9b, 0x1e, 0x87, 0xe9, 0xce, 0x55, 0x28, 0xdf,
0x8c, 0xa1, 0x89, 0x0d, 0xbf, 0xe6, 0x42, 0x68, 0x41, 0x99,
0x2d, 0x0f, 0xb0, 0x54, 0xbb, 0x16
}

Author

Generated automatically by Doxygen for libmtp from the source code.