MATH EN INFO

MODULE SBOX

Phase 1

1 Présentation

Ce fichier contient quelques indications sur la SBox utilisée dans la fonction non-linéaire F du système de cryptage ainsi que des indications sur la phase 2 du module SBox.

2 Indications sur la SBox

La SBox utilisée est un tableau de 2^8 longs (numérotée de 0 à $2^8 - 1$). La notation SBox(i) désigne la i-ième case de ce tableau. Le contenu de la SBox est le suivant :

0xe93d5a68,0x948140f7,0xf64c261c,0x94692934,0x411520f7,0x7602d4f7,
0xbcf46b2e,0xd4a20068,0xd4082471,0x3320f46a,0x43b7d4b7,0x500061af,
0x1e39f62e,0x97244546,0x14214f74,0xbf8b8840,0x4d95fc1d,0x96b591af,
0x70f4ddd3,0x66a02f45,0xbfbc09ec,0x03bd9785,0x7fac6dd0,0x31cb8504,
0x96eb27b3,0x55fd3941,0xda2547e6,0xabca0a9a,0x28507825,0x530429f4,
0x0a2c86da,0xe9b66dfb,0x68dc1462,0xd7486900,0x680ec0a4,0x27a18dee,
0x4f3ffea2,0xe887ad8c,0xb58ce006,0x7af4d6b6,0xaace1e7c,0xd3375fec,
0xce78a399,0x406b2a42,0x20fe9e35,0xd9f385b9,0xee39d7ab,0x3b124e8b,
0x1dc9faf7,0x4b6d1856,0x26a36631,0xeae397b2,0x3a6efa74,0xdd5b4332,
0x6841e7f7,0xca7820fb,0xfb0af54e,0xd8feb397,0x454056ac,0xba489527,
0x55533a3a,0x20838d87,0xfe6ba9b7,0xd096954b,0x55a867bc,0xa1159a58,
0xcca92963,0x99e1db33,0xa62a4a56,0x3f3125f9,0x5ef47e1c,0x9029317c,
0xfdf8e802,0x04272f70,0x80bb155c,0x05282ce3,0x95c11548,0xe4c66d22,
0x48c1133f,0xc70f86dc,0x07f9c9ee,0x41041f0f,0x404779a4,0x5d886e17,
0x325f51eb,0xd59bc0d1,0xf2bcc18f,0x41113564,0x257b7834,0x602a9c60,
0xdff8e8a3,0x1f636c1b,0x0e12b4c2,0x02e1329e,0xaf664fd1,0xcad18115,
0x6b2395e0,0x333e92e1,0x3b240b62,0xeebeb922,0x85b2a20e,0xe6ba0d99,
0xde720c8c,0x2da2f728,0xd0127845,0x95b794fd,0x647d0862,0xe7ccf5f0,
0x5449a36f,0x877d48fa,0xc39dfd27,0xf33e8d1e,0x0a476341,0x992eff74,
0x3a6f6eab,0xf4f8fd37,0xa812dc60,0xa1ebddf8,0x991be14c,0xdb6e6b0d,
0xc67b5510,0x6d672c37,0x2765d43b,0xdcd0e804,0xf1290dc7,0xcc00ffa3,
0xb5390f92,0x690fed0b,0x667b9ffb,0xcedb7d9c,0xa091cf0b,0xd9155ea3,
0xbb132f88,0x515bad24,0x7b9479bf,0x763bd6eb,0x37392eb3,0xcc115979,
0x8026e297,0xf42e312d,0x6842ada7,0xc66a2b3b,0x12754ccc,0x782ef11c,
0x6a124237,0xb79251e7,0x06a1bbe6,0x4bfb6350,0x1a6b1018,0x11caedfa,
0x3d25bdd8,0xe2e1c3c9,0x44421659,0x0a121386,0xd90cec6e,0xd5abea2a,
0x64af674e,0xda86a85f,0xbebfe988,0x64e4c3fe,0x9dbc8057,0xf0f7c086,
0x60787bf8,0x6003604d,0xd1fd8346,0xf6381fb0,0x7745ae04,0xd736fccc,
0x83426b33,0xf01eab71,0xb0804187,0x3c005e5f,0x77a057be,0xbde8ae24,
0x55464299,0xbf582e61,0x4e58f48f,0xf2ddfda2,0xf474ef38,0x8789bdc2,
0x5366f9c3,0xc8b38e74,0xb475f255,0x46fcd9b9,0x7aeb2661,0x8b1ddf84,
0x846a0e79,0x915f95e2,0x466e598e,0x20b45770,0x8cd55591,0xc902de4c,
0xb90bace1,0xbb8205d0,0x11a86248,0x7574a99e,0xb77f19b6,0xe0a9dc09,
0x662d09a1,0xc4324633,0xe85a1f02,0x09f0be8c,0x4a99a025,0x1d6efe10,

0x1ab93d1d,0x0ba5a4df,0xa186f20f,0x2868f169,0xdcb7da83,0x573906fe,
0xa1e2ce9b,0x4fcd7f52,0x50115e01,0xa70683fa,0xa002b5c4,0x0de6d027,
0x9af88c27,0x773f8641,0xc3604c06,0x61a806b5,0xf0177a28,0xc0f586e0,
0x006058aa,0x30dc7d62,0x11e69ed7,0x2338ea63,0x53c2dd94,0xc2c21634,
0xbbcbee56,0x90bcb6de,0xebfc7da1,0xce591d76,0x6f05e409,0x4b7c0188,
0x39720a3d,0x7c927c24,0x86e3725f,0x724d9db9,0x1ac15bb4,0xd39eb8fc,
0xed545578,0x08fca5b5,0xd83d7cd3,0x4dad0fc4,0x1e50ef5e,0xb161e6f8,
0xa28514d9,0x6c51133c,0x6fd5c7e7,0x56e14ec4,0x362abfce,0xddc6c837,
0xd79a3234,0x92638212,0x670efa8e,0x406000e0

3 Indications pour la phase 2

3.1 Descriptif des phases

L'analyse du module SBox du logiciel nous a permis de déterminer que celui-ci est composé de d'une seule communication (phase 2).

Lors de cette communication le logiciel génèrera un nombre aléatoire de mots binaires de 8 bits et attendra en retour leurs images par la SBox.

Bien évidemment, la communication devra commencer par l'envoi du mot de passe de celle-ci et se terminera par l'envoi par le logiciel de l'instruction "END".

3.2 Indications pour les mots de passes des communications

Le mot de passe de la communication est simplement la valeur décimale de Sbox(5).