RSAES-OAEP-ENCRYPT
Intermediate Values
This file provides intermediate values for debugging purposes
The hash function is SHA3-256 and the MGF is SHAKE128

==========
OAEP_Enrypt() input parameters:
n

A674F0F2 A01FA0A9 87D0EF35 5F36CBD7
EDA5A931 D5ECA30B 18FC237A 481FCEA4 35FE5141 66DB877C
A1E64520 4B0E1E2A 8E5F7FCF 28A98306 C70424F0 F4025C7D
8C6D8906 3AC7847B F52EB1F2 852BDD5C C03C1CBF 63875B50
62F4D22B 290526A5 FECFE343 D39C3B46 626B63E9 1670802B
4D7A0669 73474A75 7D3E5957 DDC020AF DDBEEF96 3643B237
651F7BD5 8D9AF4EA 67DA7DE5 620539FB 904C5A02 43388498
013470DE 777C8F11 924ADD97 FA1FB11B 51CAB46E A38ADF99
5AD5EFD0 958A98CB F022DFB0 D4B12891 7E4B513F 12062905
1307B4D9 D1014A28 C55C93AA FF59F47A 7C0472A8 B7A1AD5D
BF07252C 4B260227 8FE18A77 EC8ACB87 98F9F8B7 20DAFE03

e

00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00F3E7AF

M

48656C 6C6F2057 6F726C64

L

00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F

seed

39EAA939 3979393C
3945479D 3C393989 A959F9D9 09C9D949 F9A90939 D9F9F999

==========

Step 2.a - lHash

050A4873 3BD5C275
6BA95C58 28CC83EE 16FABCD3 C086885B 7744F84A 0F9E0D94

Step 2.b - PS

000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

Step 2.c - DB

050A48 733BD5C2
756BA95C 5828CC83 EE16FABC D3C08688 5B7744F8 4A0F9E0D
94000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 0148656C 6C6F2057 6F726C64

Step 2.d - seed

39EAA939 3979393C
3945479D 3C393989 A959F9D9 09C9D949 F9A90939 D9F9F999

Step 2.e - dbMask

6098FF A618E5C2
23177308 8FAB3CFB DD855465 6280093C 9E5FA50B CF37A571
4B8E3D06 A139C686 73CD6257 CE10F5F3 396936BD 600A510B
589AFE3F 3B7BCA2C DB89BA81 6553451C 5C0EDD96 CD33BC5D
6C6D65B7 51A2DE31 9904AD0F 096FBCCF 4372721A 62D923F0
0D39384A C27F24F9 F8AB48CC 7960AD1F 070DD9C6 B781C173
70BA9C5F 95AEDEDA 3AD300F1 48A53666 E19AD2AD 259988BB
C6C04752 457E30E8 0D2CCBB8 0AF12CE9 44F67DB4 35F1B650
790718E9 F4127D59 B1365D39 F37ECBE9 78A8ACAF 244B6D73
8A91DCAA 68C72205 8F4F387D B419C407 A443134B 09CD3769

Step 2.f - maskedDB

6592B7 D5233000
567CDA54 D783F078 3393AED9 B1408FB4 C528E1F3 85383B7C

DF8E3D06 A139C686 73CD6257 CE10F5F3 396936BD 600A510B
589AFE3F 3B7BCA2C DB89BA81 6553451C 5C0EDD96 CD33BC5D
6C6D65B7 51A2DE31 9904AD0F 096FBCCF 4372721A 62D923F0
0D39384A C27F24F9 F8AB48CC 7960AD1F 070DD9C6 B781C173
70BA9C5F 95AEDEDA 3AD300F1 48A53666 E19AD2AD 259988BB
C6C04752 457E30E8 0D2CCBB8 0AF12CE9 44F67DB4 35F1B650
790718E9 F4127D59 B1365D39 F37ECBE9 78A8ACAF 244B6D73
8A91DCAA 68C72205 8F4F387D B551A16B C82C331C 66BF5B0D

Step 2.g - seedMask

6C284287 A313ADD0
3528DC49 6C5CC862 B0B8B3C0 C668225D 477255FF ADAC38B6

Step 2.h - maskedSeed

55C2EBBE 9A6A94EC
0C6D9BD4 5065F1EB 19E14A19 CFA1FB14 BEDB5CC6 7455C12F

Step 2.i - EM

0055C2EB BE9A6A94 EC0C6D9B D45065F1
EB19E14A 19CFA1FB 14BEDB5C C67455C1 2F6592B7 D5233000
567CDA54 D783F078 3393AED9 B1408FB4 C528E1F3 85383B7C
DF8E3D06 A139C686 73CD6257 CE10F5F3 396936BD 600A510B
589AFE3F 3B7BCA2C DB89BA81 6553451C 5C0EDD96 CD33BC5D
6C6D65B7 51A2DE31 9904AD0F 096FBCCF 4372721A 62D923F0
0D39384A C27F24F9 F8AB48CC 7960AD1F 070DD9C6 B781C173
70BA9C5F 95AEDEDA 3AD300F1 48A53666 E19AD2AD 259988BB
C6C04752 457E30E8 0D2CCBB8 0AF12CE9 44F67DB4 35F1B650
790718E9 F4127D59 B1365D39 F37ECBE9 78A8ACAF 244B6D73
8A91DCAA 68C72205 8F4F387D B551A16B C82C331C 66BF5B0D

Step 3.a - m

42290527300904055368377788531939406029260535134364837691247675946075863075431346857211827109844750001656703216880319952969748232870794091457101918929316956516080434692408650744377446480761942694330330914670934334747121643519513830302822501824211330191953458632391075412288146304355945870231048564686890881612592213320811556411005127801691685493144056229732609455640035200918331402483103719911460257401368337590279975727077599992910788900443081541755789452676731243113198050263105575603898849752549743900534714752514425737201097550405191949951019309973912954314197899041920692592756505243309079402661963913450445581

Step 3.b - c

12275179295985888831563883494418727842742290981983341367292579608870679622411519173882106068071946763163977427323035656631190439151070192009932766786757226264822685225874442896091267284348729017476598902599316189419774358390523698275667897223442226204924714490499738960388400711389740158225004207642616846060595129026696560874955795004059707056680804867840344922481334864494565832

3756670983628127613040380730575545936985207822532444472842363057932289063229239179115364101569133775778082977585881753767768435616044299482762226196367721459748189691753558758708008895056938083086808066389902355534717360885781035466401 8

Step 3.c - C

09B94BF1 6C206C7B 69DF72F4 03E5A9D0 AC08744F 8EC7B002 322EFD8B 18F9F3A1 8854396F 5D1B2DA7 4CDD8483 A07941AB EFD7F959 924E247A 91F203EF D64340C7 D6DB4407 8090F1E8 43309A78 307235B8 B4B9AF4D 024612C3 CD1FDCD0 CA688AF8 346398C3 BA616041 9203A407 2BF6DA2B CA7C4A52 C02BBE5F 1C77D725 0F7A7433 88DE0843 3F522DD0 D804E7DE 8B889BB8 DD1858A1 7C30F757 DDE759EA 8E741C7F 2E51FDFE FA1F464B 4E8162E8 108155EA 02D312DD A438F1D2 3A135640 0F93ECEC BE35E315 2A3522BD 513EC141 D5F2F35F 53BB3701 078C49C2 CB2A4CF3 689E1AC2 34BB628C 768C8612 4AAF891B EEC5322D 6E89D637 45DCA5C1 579BE3BA 655D7252

Step 4 - Ciphertext, C, is

09B94BF1 6C206C7B 69DF72F4 03E5A9D0 AC08744F 8EC7B002 322EFD8B 18F9F3A1 8854396F 5D1B2DA7 4CDD8483 A07941AB EFD7F959 924E247A 91F203EF D64340C7 D6DB4407 8090F1E8 43309A78 307235B8 B4B9AF4D 024612C3 CD1FDCD0 CA688AF8 346398C3 BA616041 9203A407 2BF6DA2B CA7C4A52 C02BBE5F 1C77D725 0F7A7433 88DE0843 3F522DD0 D804E7DE 8B889BB8 DD1858A1 7C30F757 DDE759EA 8E741C7F 2E51FDFE FA1F464B 4E8162E8 108155EA 02D312DD A438F1D2 3A135640 0F93ECEC BE35E315 2A3522BD 513EC141 D5F2F35F 53BB3701 078C49C2 CB2A4CF3 689E1AC2 34BB628C 768C8612 4AAF891B EEC5322D 6E89D637 45DCA5C1 579BE3BA 655D7252