IntermediateValuesKAT_224.txt
Algorithm Name: NaSHA
Principal Submitter: Smile Markovski
Message Digest Lenght = 224

##

One Block Message Sample
Input Message: STIP

==

Initial Hash Values:
H[0]=F3BCC9086A09E667
H[1]=C1059ED8CBBB9D5D
H[2]=84CAA73BBB67AE85
H[3]=367CD507629A292A
H[4]=FE94F82B3C6EF372
H[5]=3070DD179159015A
H[6]=5F1D36F1A54FF53A
H[7]=F70E5939152FECD8
==

Block contents:
M[0]=504954531
M[1]=00
M[2]=00
M[3]=00
M[4]=00
M[5]=00
M[6]=00
M[7]=200
==

in compile
S[0]=504954531
S[1]=F3BCC9086A09E667
S[2]=00
S[3]=C1059ED8CBBB9D5D
S[4]=00
S[5]=84CAA73BBB67AE85
S[6]=00
S[7]=367CD507629A292A
S[8]=00
S[9]=FE94F82B3C6EF372
S[10]=00
S[11]=3070DD179159015A
S[12]=00
S[13]=5F1D36F1A54FF53A
S[14]=200
S[15]=F70E5939152FECD8

after LinTr256^16
S[0]=504954531
S[1]=F3BCC9086A09E667
S[2]=00

S[3]=C1059ED8CBBB9D5D
S[4]=00
S[5]=84CAA73BBB67AE85
S[6]=00
S[7]=367CD507629A292A
S[8]=00
S[9]=FE94F82B3C6EF372
S[10]=00
S[11]=3070DD179159015A
S[12]=00
S[13]=5F1D36F1A54FF53A
S[14]=200
S[15]=F70E5939152FECD8

leaders
l1=B9830699345FC999 l2=EB2CE732B93A5EB9

extended Feistel networks parameters
a1=23 b1=12 c1=81
a2=7D b2=C9 c2=58
a3=61 b3=E0 c3=23
alpha1=F7E2 beta1=BF74 gama1=FB12
alpha2=FB0 beta2=834A gama2=7405
A1=9A32760A B1=F39BB3F9 C1=7997D7D4
A2=2C29F589 B2=9E62317D C2=4D69E6E5

AE transformation
S[0]=5885AE7177FB8741
S[1]=7B17B42711C95EE
S[2]=46DD8E5E4FC4325D
S[3]=820AF9411FD442C0
S[4]=5584A97A42ABED4D
S[5]=80FFF2587A12AC7
S[6]=8506B89565801736
S[7]=3C77BC451E1B739F
S[8]=A0A40EFA7CEB2D66
S[9]=95532026A0971D55
S[10]=E79A16D030E3DEC2
S[11]=87B426CA4D6C4272
S[12]=ABA3754CD9C5D088
S[13]=E9BAED06EBB3C6C9
S[14]=782167C5CB1AEBB5
S[15]=CF9809EBF0976CB8

Rotate left for 32 bits
S[0]=77FB87415885AE71
S[1]=711C95EE7B17B42
S[2]=4FC4325D46DD8E5E
S[3]=1FD442C0820AF941
S[4]=42ABED4D5584A97A
S[5]=7A12AC780FFF258
S[6]=658017368506B895
S[7]=1E1B739F3C77BC45
S[8]=7CEB2D66A0A40EFA
S[9]=A0971D5595532026
S[10]=30E3DEC2E79A16D0
S[11]=4D6C427287B426CA

S[12]=D9C5D088ABA3754C
S[13]=EBB3C6C9E9BAED06
S[14]=CB1AEBB5782167C5
S[15]=F0976CB8CF9809EB

RAE transformation
S[0]=77A18B57A0D34EB6
S[1]=841C9D12AE9369BC
S[2]=BAF7FCE4D8011FC6
S[3]=9D34D04F10384C60
S[4]=C99FC64C48A6F8E4
S[5]=E72232F8BA6616EA
S[6]=EFA580FCE5A8700F
S[7]=68878F6DDCFF7B7E
S[8]=D4DC4AF6DFC287B8
S[9]=90EB73C3E232EF83
S[10]=1930E40141F0E5E3
S[11]=27F32BA31E53ADFD
S[12]=23BEA7A28688C948
S[13]=4B368C3EABF53B42
S[14]=E59FB854D3818A18
S[15]=EAB49D9755339E5

H[0]=841C9D12AE9369BC
H[1]=9D34D04F10384C60
H[2]=E72232F8BA6616EA
H[3]=68878F6DDCFF7B7E
H[4]=90EB73C3E232EF83
H[5]=27F32BA31E53ADFD
H[6]=4B368C3EABF53B42
H[7]=EAB49D9755339E5

Message digest is:
10 38 4C 60 9D 34 D0 4F DC FF 7B 7E 68 87 8F 6D 1E 53 AD FD 27 F3 2B A3 75 53 39 E5
==========

##########

Two Block Message Sample
Input Message: STIPSTIPSTIPSTIPSTIPSTIPSTIPSTIPSTIPSTIPSTIPSTIPSTIPSTIP

==========

Initial Hash Values:
H[0]=F3BCC9086A09E667
H[1]=C1059ED8CBBB9D5D
H[2]=84CAA73BBB67AE85
H[3]=367CD507629A292A
H[4]=FE94F82B3C6EF372
H[5]=3070DD179159015A
H[6]=5F1D36F1A54FF53A
H[7]=F70E5939152FECD8
==========

==========

Block contents:
M[0]=5049545350495453
M[1]=5049545350495453
M[2]=5049545350495453
M[3]=5049545350495453
M[4]=5049545350495453
M[5]=5049545350495453
M[6]=5049545350495453
M[7]=10
==========

in compile
S[0]=5049545350495453
S[1]=F3BCC9086A09E667
S[2]=5049545350495453
S[3]=C1059ED8CBBB9D5D
S[4]=5049545350495453
S[5]=84CAA73BBB67AE85
S[6]=5049545350495453
S[7]=367CD507629A292A
S[8]=5049545350495453
S[9]=FE94F82B3C6EF372
S[10]=5049545350495453
S[11]=3070DD179159015A
S[12]=5049545350495453
S[13]=5F1D36F1A54FF53A
S[14]=10
S[15]=F70E5939152FECD8

after LinTr256^16
S[0]=5049545350495453
S[1]=F3BCC9086A09E667
S[2]=5049545350495453
S[3]=C1059ED8CBBB9D5D
S[4]=5049545350495453
S[5]=84CAA73BBB67AE85
S[6]=5049545350495453
S[7]=367CD507629A292A
S[8]=5049545350495453
S[9]=FE94F82B3C6EF372
S[10]=5049545350495453
S[11]=3070DD179159015A
S[12]=5049545350495453
S[13]=5F1D36F1A54FF53A
S[14]=10
S[15]=F70E5939152FECD8

leaders
l1=694C3B07345FC998 l2=1B7432DE59BAE73F

extended Feistel networks parameters
a1=D2 b1=DB c1=AD
a2=CB b2=C9 c2=58
a3=61 b3=C1 c3=D2

alpha1=A82B beta1=73A6 gama1=FB12
alpha2=F72 beta2=834A gama2=7402
A1=9A32760A B1=F39BB418 C1=99883733
A2=5BE14938 B2=6E1B852A C2=1DA112D3

AE transformation
S[0]=B8463A7E7033B2D
S[1]=E17F96611EB8216
S[2]=BEAE2BE41913E033
S[3]=E853FD6747FC6D9D
S[4]=9725B403B835BCC7
S[5]=B8D6756EC540277E
S[6]=99337F207D93C65E
S[7]=5178AE4DA4EB9CA
S[8]=919A9C6BE1FA87ED
S[9]=BB0A34953918627
S[10]=912DFCEBBF0D41A1
S[11]=5884505523805C15
S[12]=925D89E795D6F6F
S[13]=496CA7D7E8931C8
S[14]=BC537A282CFE0E02
S[15]=170F607CE57E2EF6

Rotate left for 32 bits
S[0]=7033B2DB8463A7E
S[1]=11EB8216E17F966
S[2]=1913E033BEAE2BE4
S[3]=47FC6D9DE853FD67
S[4]=B835BCC79725B403
S[5]=C540277EB8D6756E
S[6]=7D93C65E99337F20
S[7]=A4EB9CA5178AE4D
S[8]=E1FA87ED919A9C6B
S[9]=53918627BB0A349
S[10]=BF0D41A1912DFCEB
S[11]=23805C1558845055
S[12]=795D6F6F925D89E
S[13]=7E8931C8496CA7D
S[14]=2CFE0E02BC537A28
S[15]=E57E2EF6170F607C

RAE transformation
S[0]=879E67CE66602BBC
S[1]=F5F112A0E2FD9E6
S[2]=7FB5CC59C76C6341
S[3]=9C05F6D971D8F162
S[4]=4EA59A171313D50C
S[5]=2896297378E712C6
S[6]=F2B1FB4498DDE8D3
S[7]=62D59A6BC592885C
S[8]=1279B416377C6701
S[9]=BE8372E69B7FB69B
S[10]=1F824D7AD46C06DC
S[11]=1D74A935F368586
S[12]=38EF596A7D470AB
S[13]=B4323A7F8A2ED4C
S[14]=75F5EA5538B3B54

S[15]=261BD41EBB3A2426

H[0]=F5F112A0E2FD9E6
H[1]=9C05F6D971D8F162
H[2]=2896297378E712C6
H[3]=62D59A6BC592885C
H[4]=BE8372E69B7FB69B
H[5]=1D74A935F368586
H[6]=B4323A7F8A2ED4C
H[7]=261BD41EBB3A2426

Block contents:
M[0]=00
M[1]=00
M[2]=00
M[3]=00
M[4]=00
M[5]=00
M[6]=00
M[7]=1C00
==========

in compile
S[0]=00
S[1]=F5F112A0E2FD9E6
S[2]=00
S[3]=9C05F6D971D8F162
S[4]=00
S[5]=2896297378E712C6
S[6]=00
S[7]=62D59A6BC592885C
S[8]=00
S[9]=BE8372E69B7FB69B
S[10]=00
S[11]=1D74A935F368586
S[12]=00
S[13]=B4323A7F8A2ED4C
S[14]=1C00
S[15]=261BD41EBB3A2426

after LinTr256^16
S[0]=00
S[1]=F5F112A0E2FD9E6
S[2]=00
S[3]=9C05F6D971D8F162
S[4]=00
S[5]=2896297378E712C6
S[6]=00
S[7]=62D59A6BC592885C
S[8]=00
S[9]=BE8372E69B7FB69B
S[10]=00
S[11]=1D74A935F368586
S[12]=00

S[13]=B4323A7F8A2ED4C
S[14]=1C00
S[15]=261BD41EBB3A2426

leaders
l1=21353B61766CCCD8 l2=B3503D14DED0AF12

extended Feistel networks parameters
a1=B0 b1=8 c1=F0
a2=58 b2=AC c2=C2
a3=5E b3=62 c3=B0
alpha1=AEE beta1=2FB9 gama1=D36F
alpha2=2538 beta2=F9FE gama2=8DCD
A1=ED15BFC0 B1=B436DD4 C1=A4F8AE59
A2=386DA245 B2=CA8476A5 C2=2D3378D4

AE transformation
S[0]=D90BD7FB24D5F2F3
S[1]=1EFD5AF55D16A30D
S[2]=80762A45E1A72964
S[3]=293DE2869C8564EC
S[4]=CA21A6769939D6BE
S[5]=DDC3A1F7BBF12322
S[6]=8E2CE48F7066A1F
S[7]=B5294311213CF99B
S[8]=1A5A90251809618C
S[9]=A944B3315377D4E4
S[10]=194CE956C011A3B7
S[11]=ECECCEAAF1AC6589
S[12]=12F646E5883A7DF8
S[13]=E2EBB670ED305A0B
S[14]=6E02A02BB6E55A96
S[15]=521BF6FCCA8A7C72

Rotate left for 32 bits
S[0]=24D5F2F3D90BD7FB
S[1]=5D16A30D1EFD5AF5
S[2]=E1A7296480762A45
S[3]=9C8564EC293DE286
S[4]=9939D6BECA21A676
S[5]=BBF12322DDC3A1F7
S[6]=F7066A1F8E2CE48
S[7]=213CF99BB5294311
S[8]=1809618C1A5A9025
S[9]=5377D4E4A944B331
S[10]=C011A3B7194CE956
S[11]=F1AC6589ECECCEAA
S[12]=883A7DF812F646E5
S[13]=ED305A0BE2EBB670
S[14]=B6E55A966E02A02B
S[15]=CA8A7C72521BF6FC

RAE transformation
S[0]=54B46688ECAEBE27
S[1]=5E10253F99E51EA8
S[2]=13FCE5096E903D01
S[3]=4E2C7178181302B6

S[4]=BFB0C382B79009EA
S[5]=212E4BC5E28AB91C
S[6]=35DE068FB3156FD3
S[7]=5520521627754D73
S[8]=17DBB74352136362
S[9]=3D392786CDA9994
S[10]=7E7CDB4DCEFABD3
S[11]=7F2003C5B2552406
S[12]=F3D2B530B1FF2AC8
S[13]=D8D48C244DB1B883
S[14]=B36115A55591790C
S[15]=2DE570EED1D0AA30

H[0]=5E10253F99E51EA8
H[1]=4E2C7178181302B6
H[2]=212E4BC5E28AB91C
H[3]=5520521627754D73
H[4]=3D392786CDA9994
H[5]=7F2003C5B2552406
H[6]=D8D48C244DB1B883
H[7]=2DE570EED1D0AA30

Message digest is:
18 13 2 B6 4E 2C 71 78 27 75 4D 73 55 20 52 16 B2 55 24 6 7F 20 3 C5 D1 D0 AA 30
==========

IntermediateValuesKAT_256.txt
Algorithm Name: NaSHA
Principal Submitter: Smile Markovski
Message Digest Lenght = 256

##########

One Block Message Sample
Input Message: STIP

==========

Initial Hash Values:
H[0]=ADE682D1510E527F
H[1]=FFC00B3167332667
H[2]=2B3E6C1F9B05688C
H[3]=685815118EB44A87
H[4]=FB41BD6B1F83D9AB
H[5]=64F98FA7DB0C2E0D
H[6]=137E21795BE0CD19
H[7]=BEFA4FA447B5481D
==========

Block contents:
M[0]=504954531
M[1]=00
M[2]=00
M[3]=00

M[4]=00
M[5]=00
M[6]=00
M[7]=200
==========

in compile
S[0]=504954531
S[1]=ADE682D1510E527F
S[2]=00
S[3]=FFC00B3167332667
S[4]=00
S[5]=2B3E6C1F9B05688C
S[6]=00
S[7]=685815118EB44A87
S[8]=00
S[9]=FB41BD6B1F83D9AB
S[10]=00
S[11]=64F98FA7DB0C2E0D
S[12]=00
S[13]=137E21795BE0CD19
S[14]=200
S[15]=BEFA4FA447B5481D

after LinTr256^16
S[0]=504954531
S[1]=ADE682D1510E527F
S[2]=00
S[3]=FFC00B3167332667
S[4]=00
S[5]=2B3E6C1F9B05688C
S[6]=00
S[7]=685815118EB44A87
S[8]=00
S[9]=FB41BD6B1F83D9AB
S[10]=00
S[11]=64F98FA7DB0C2E0D
S[12]=00
S[13]=137E21795BE0CD19
S[14]=200
S[15]=BEFA4FA447B5481D

leaders
l1=F84A2C199775954C l2=E2B4BAB5E85A2BAA

extended Feistel networks parameters
a1=FC b1=18 c1=DB
a2=83 b2=88 c2=35
a3=6F b3=18 c3=FC
alpha1=8A05 beta1=7037 gama1=1B8D
alpha2=EDBD beta2=5520 gama2=BBE3
A1=49182C44 B1=7C950934 C1=EB8DFC48
A2=864A161B B2=DA0B205D C2=E5BA663D

AE transformation
S[0]=B9144B09EBD0528E

S[1]=CC9E70615B1986B2
S[2]=BDC326A64B2EB0FC
S[3]=9A484F139D8A0F4F
S[4]=EB4357E75BEEEB32
S[5]=7A24FA3B6202977A
S[6]=FEB788317D6EC96C
S[7]=1B2641A370632533
S[8]=C126D5B035C4F350
S[9]=3845876274D578B8
S[10]=E055D995BAD58E09
S[11]=5017D07115B93489
S[12]=CE3FCDAF7E037A93
S[13]=68CDE0FCBE82CB74
S[14]=C26FDAB66D2F65CC
S[15]=ED9A9D2B08DB6DF

Rotate left for 32 bits
S[0]=EBD0528EB9144B09
S[1]=5B1986B2CC9E7061
S[2]=4B2EB0FCBDC326A6
S[3]=9D8A0F4F9A484F13
S[4]=5BEEEB32EB4357E7
S[5]=6202977A7A24FA3B
S[6]=7D6EC96CFEB78831
S[7]=706325331B2641A3
S[8]=35C4F350C126D5B0
S[9]=74D578B838458762
S[10]=BAD58E09E055D995
S[11]=15B934895017D071
S[12]=7E037A93CE3FCDAF
S[13]=BE82CB7468CDE0FC
S[14]=6D2F65CCC26FDAB6
S[15]=B08DB6DFED9A9D2

RAE transformation
S[0]=ED766D897A39EF42
S[1]=CBEEE363618A00A
S[2]=D42675A0F7D65C8F
S[3]=39F801241D121A2
S[4]=97C3D8169514907F
S[5]=7B73A357B48F8BF8
S[6]=E3E6FFE79B09A3BC
S[7]=31091C2FCFA3111F
S[8]=C1A41EA2AD10387
S[9]=9DBF036889B53AC4
S[10]=E1D37F2BF53D1C21
S[11]=5205899DE523B9FF
S[12]=8562DD379DB4BA3C
S[13]=13F78B2525C7055D
S[14]=1809315662B643FC
S[15]=5ED0226385F7D23

H[0]=CBEEE363618A00A
H[1]=39F801241D121A2
H[2]=7B73A357B48F8BF8
H[3]=31091C2FCFA3111F

H[4]=9DBF036889B53AC4
H[5]=5205899DE523B9FF
H[6]=13F78B2525C7055D
H[7]=5ED0226385F7D23

Message digest is:
1 D1 21 A2 39 F8 1 24 CF A3 11 1F 31 9 1C 2F E5 23 B9 FF 52 5 89 9D 38 5F 7D 23 5 ED 2 26
==========

##########

Two Block Message Sample
Input Message: STIPSTIPSTIPSTIPSTIPSTIPSTIPSTIPSTIPSTIPSTIPSTIPSTIPSTIP

==========

Initial Hash Values:
H[0]=ADE682D1510E527F
H[1]=FFC00B3167332667
H[2]=2B3E6C1F9B05688C
H[3]=685815118EB44A87
H[4]=FB41BD6B1F83D9AB
H[5]=64F98FA7DB0C2E0D
H[6]=137E21795BE0CD19
H[7]=BEFA4FA447B5481D
==========

==========

Block contents:
M[0]=5049545350495453
M[1]=5049545350495453
M[2]=5049545350495453
M[3]=5049545350495453
M[4]=5049545350495453
M[5]=5049545350495453
M[6]=5049545350495453
M[7]=10
==========

in compile
S[0]=5049545350495453
S[1]=ADE682D1510E527F
S[2]=5049545350495453
S[3]=FFC00B3167332667
S[4]=5049545350495453
S[5]=2B3E6C1F9B05688C
S[6]=5049545350495453
S[7]=685815118EB44A87
S[8]=5049545350495453
S[9]=FB41BD6B1F83D9AB
S[10]=5049545350495453
S[11]=64F98FA7DB0C2E0D
S[12]=5049545350495453

S[13]=137E21795BE0CD19
S[14]=10
S[15]=BEFA4FA447B5481D

after LinTr256^16
S[0]=5049545350495453
S[1]=ADE682D1510E527F
S[2]=5049545350495453
S[3]=FFC00B3167332667
S[4]=5049545350495453
S[5]=2B3E6C1F9B05688C
S[6]=5049545350495453
S[7]=685815118EB44A87
S[8]=5049545350495453
S[9]=FB41BD6B1F83D9AB
S[10]=5049545350495453
S[11]=64F98FA7DB0C2E0D
S[12]=5049545350495453
S[13]=137E21795BE0CD19
S[14]=10
S[15]=BEFA4FA447B5481D

leaders
l1=A803802B9775954B l2=127DEE83C859D30E

extended Feistel networks parameters
a1=2C b1=50 c1=2F
a2=51 b2=88 c2=35
a3=6E b3=F7 c3=2C
alpha1=59CC beta1=3C65 gama1=1B8D
alpha2=EDBD beta2=5520 gama2=BBE4
A1=49182C44 B1=7C950915 C1=B8DF3E7
A2=3613424C B2=A524C0F C2=157119CB

AE transformation
S[0]=7986D8C11B196E7A
S[1]=62360AA0BB7CF48D
S[2]=2AF177F8710F8E2F
S[3]=7B2461D2E0B2884E
S[4]=DEC2489C288B922F
S[5]=453A9CE8518387AF
S[6]=243980112DA322D
S[7]=20BD8A6774173561
S[8]=8887A18E32EC320B
S[9]=75516E1D3D7BA4FB
S[10]=2FC8712EF9E1A494
S[11]=B5D2C9C1E62C4C26
S[12]=25AA42D0B4B72831
S[13]=CBBE191DB7B66AA6
S[14]=DD1B97F8FDFADED
S[15]=C4E402E4B2827CE

Rotate left for 32 bits
S[0]=1B196E7A7986D8C1
S[1]=BB7CF48D62360AA0
S[2]=710F8E2F2AF177F8
S[3]=E0B2884E7B2461D2

S[4]=288B922FDEC2489C
S[5]=518387AF453A9CE8
S[6]=12DA322D2439801
S[7]=7417356120BD8A67
S[8]=32EC320B8887A18E
S[9]=3D7BA4FB75516E1D
S[10]=F9E1A4942FC8712E
S[11]=E62C4C26B5D2C9C1
S[12]=B4B7283125AA42D0
S[13]=B7B66AA6CBBE191D
S[14]=FDFADEDDD1B97F8
S[15]=B2827CEC4E402E4

RAE transformation
S[0]=A408B26B453E490C
S[1]=109FB76ACA06681D
S[2]=181A4ADC32C8D715
S[3]=44DBA905954DB44A
S[4]=DBE6822B8451125E
S[5]=D85761B7BB68E93E
S[6]=B7D8B06F906977DA
S[7]=9AB89B0516EF3288
S[8]=14E2F04ABB53D5A7
S[9]=D501BDDB2FB9A877
S[10]=22CF3963CF4A2281
S[11]=4A9CB27B14FE2227
S[12]=FF803D676B9ADBFE
S[13]=FC05BCD033D811B1
S[14]=563FA69EF3CD0F01
S[15]=558564FFD2495A54

H[0]=109FB76ACA06681D
H[1]=44DBA905954DB44A
H[2]=D85761B7BB68E93E
H[3]=9AB89B0516EF3288
H[4]=D501BDDB2FB9A877
H[5]=4A9CB27B14FE2227
H[6]=FC05BCD033D811B1
H[7]=558564FFD2495A54

Block contents:
M[0]=00
M[1]=00
M[2]=00
M[3]=00
M[4]=00
M[5]=00
M[6]=00
M[7]=1C00
==========

in compile
S[0]=00
S[1]=109FB76ACA06681D

S[2]=00
S[3]=44DBA905954DB44A
S[4]=00
S[5]=D85761B7BB68E93E
S[6]=00
S[7]=9AB89B0516EF3288
S[8]=00
S[9]=D501BDDB2FB9A877
S[10]=00
S[11]=4A9CB27B14FE2227
S[12]=00
S[13]=FC05BCD033D811B1
S[14]=1C00
S[15]=558564FFD2495A54

after LinTr256^16
S[0]=00
S[1]=109FB76ACA06681D
S[2]=00
S[3]=44DBA905954DB44A
S[4]=00
S[5]=D85761B7BB68E93E
S[6]=00
S[7]=9AB89B0516EF3288
S[8]=00
S[9]=D501BDDB2FB9A877
S[10]=00
S[11]=4A9CB27B14FE2227
S[12]=00
S[13]=FC05BCD033D811B1
S[14]=1C00
S[15]=558564FFD2495A54

leaders
l1=3C1013A733F784E0 l2=1C9E6C18A8F69EB

extended Feistel networks parameters
a1=95 b1=10 c1=E2
a2=71 b2=CD c2=72
a3=57 b3=B0 c3=95
alpha1=3F0A beta1=8E2 gama1=C3CF
alpha2=3797 beta2=53B6 gama2=493D
A1=389A0E94 B1=1F5D7B0A C1=847EFF6E
A2=BAFE39C4 B2=24262FA8 C2=9CB6D098

AE transformation
S[0]=BA1B9D31758F8B39
S[1]=63C16294917E2A0D
S[2]=CBEECAD7FA0E805C
S[3]=E2E9EB17A7348379
S[4]=674E391B465F8792
S[5]=600CA37FB295086F
S[6]=3FBB4ED6D96810
S[7]=97E3039194347B58
S[8]=35F959975D89F926
S[9]=87D276C397560014
S[10]=F4A66320D1A7154A

S[11]=72B409DDE21E2704
S[12]=62234E0E5E83A139
S[13]=45EC449579CC0BC2
S[14]=4C493ED845E622D1
S[15]=3A0B49784D09625

Rotate left for 32 bits
S[0]=758F8B39BA1B9D31
S[1]=917E2A0D63C16294
S[2]=FA0E805CCBEECAD7
S[3]=A7348379E2E9EB17
S[4]=465F8792674E391B
S[5]=B295086F600CA37F
S[6]=6D968103FBB4ED
S[7]=94347B5897E30391
S[8]=5D89F92635F95997
S[9]=9756001487D276C3
S[10]=D1A7154AF4A66320
S[11]=E21E270472B409DD
S[12]=5E83A13962234E0E
S[13]=79CC0BC245EC4495
S[14]=45E622D14C493ED8
S[15]=84D096253A0B497

RAE transformation
S[0]=747FD64BAC45C791
S[1]=9E645A07B6ABF2FA
S[2]=A7565F9D423E0604
S[3]=2CF1ACA759DFC7C7
S[4]=B5CF46E4362CCC0F
S[5]=6B4DD52513D1F5D3
S[6]=96EED34EF22C7C45
S[7]=963B0817CF23A8C9
S[8]=D3DBDCE8F216AE83
S[9]=61BCD026742E4D96
S[10]=84BC7CC1BDC191CF
S[11]=90555B97C2BE6A7F
S[12]=D839758EAD55DE4F
S[13]=3CBEEFE970478982
S[14]=E444F70AA77874B2
S[15]=818EEC4C9563F5A

H[0]=9E645A07B6ABF2FA
H[1]=2CF1ACA759DFC7C7
H[2]=6B4DD52513D1F5D3
H[3]=963B0817CF23A8C9
H[4]=61BCD026742E4D96
H[5]=90555B97C2BE6A7F
H[6]=3CBEEFE970478982
H[7]=818EEC4C9563F5A

Message digest is:
59 DF C7 C7 2C F1 AC A7 CF 23 A8 C9 96 3B 8 17 C2 BE 6A 7F 90 55 5B 97 C9 56 3F 5A 8 18 EE C4
==========

IntermediateValuesKAT_384.txt
Algorithm Name: NaSHA
Principal Submitter: Smile Markovski
Message Digest Lenght = 384

##

One Block Message Sample
Input Message: STIP

==

Initial Hash Values:
H[0]=F3BCC9086A09E667
H[1]=C1059ED8CBBB9D5D
H[2]=84CAA73BBB67AE85
H[3]=367CD507629A292A
H[4]=FE94F82B3C6EF372
H[5]=3070DD179159015A
H[6]=5F1D36F1A54FF53A
H[7]=F70E5939152FECD8
H[8]=ADE682D1510E527F
H[9]=FFC00B3167332667
H[10]=2B3E6C1F9B05688C
H[11]=685815118EB44A87
H[12]=FB41BD6B1F83D9AB
H[13]=64F98FA7DB0C2E0D
H[14]=137E21795BE0CD19
H[15]=BEFA4FA447B5481D
==

Block contents:
M[0]=504954531
M[1]=00
M[2]=00
M[3]=00
M[4]=00
M[5]=00
M[6]=00
M[7]=00
M[8]=00
M[9]=00
M[10]=00
M[11]=00
M[12]=00
M[13]=00
M[14]=00
M[15]=200
==

in compile
S[0]=504954531
S[1]=F3BCC9086A09E667
S[2]=00
S[3]=C1059ED8CBBB9D5D

S[4]=00
S[5]=84CAA73BBB67AE85
S[6]=00
S[7]=367CD507629A292A
S[8]=00
S[9]=FE94F82B3C6EF372
S[10]=00
S[11]=3070DD179159015A
S[12]=00
S[13]=5F1D36F1A54FF53A
S[14]=00
S[15]=F70E5939152FECD8
S[16]=00
S[17]=ADE682D1510E527F
S[18]=00
S[19]=FFC00B3167332667
S[20]=00
S[21]=2B3E6C1F9B05688C
S[22]=00
S[23]=685815118EB44A87
S[24]=00
S[25]=FB41BD6B1F83D9AB
S[26]=00
S[27]=64F98FA7DB0C2E0D
S[28]=00
S[29]=137E21795BE0CD19
S[30]=200
S[31]=BEFA4FA447B5481D

after LinTr512^32
S[0]=D82564C9B327554
S[1]=96BD8F243A94FAB9
S[2]=FC7B876BD39F6FD1
S[3]=C148F53F1F987280
S[4]=B40A0A784959D4B3
S[5]=20BF1DF1A80F6C4A
S[6]=303832C4CC0793C1
S[7]=D2F8E99EF4AADE5B
S[8]=C505A5B43ACF7C
S[9]=404DC63C2DBC20EA
S[10]=B2C2B910F11725C1
S[11]=AA5C1A2244DE0CBF
S[12]=ED1B19BF360C959D
S[13]=7FB73EAFD15047DB
S[14]=D477B7B163987834
S[15]=243B02B9701B72A4
S[16]=9BB9266565F3E0D0
S[17]=D8CFCEF0252F6136
S[18]=68C4FD27E4D33E97
S[19]=D28312356671515
S[20]=FAE1278EB5F8466A
S[21]=F17543CF5AE29C07
S[22]=60BADF7BF5A88F44
S[23]=DBD791EA1E285BBF
S[24]=2560187274213348
S[25]=AB08E9381F83D9AA
S[26]=F2E83A1231543372

S[27]=64F98FA7DB0C2E0D
S[28]=DA4B2FD0C1E7F48B
S[29]=137E21795BE0CD19
S[30]=B38F84FB909C1138
S[31]=BEFA4FA447B5481D

leaders l1
l1=A43FE570D5C7700D l2=BDC47CAAF337E252

extended Feistel networks parameters
a1=F1 b1=69 c1=40
a2=FD b2=D4 c2=C9
a3=28 b3=69 c3=F1
alpha1=C0B2 beta1=721D gama1=331
alpha2=1C62 beta2=31F6 gama2=F066
A1=35F53281 B1=5D1ED332 C1=75CDD79
A2=6CD2586E B2=D3B3EAD8 C2=F8B2BA6A

AE transformation
S[0]=DCB57AD26803C36F
S[1]=C8B6FCABEAAF4EEA
S[2]=D202C848DF235E2D
S[3]=2806449F786E08B9
S[4]=392EE99114B6A35D
S[5]=6ED0798EE4AB44B8
S[6]=92CEBADA56C23FD6
S[7]=600C94BA7660A13C
S[8]=876A86AF51C348B3
S[9]=D88C80B09FBC98BC
S[10]=13037423FD6F9790
S[11]=787D46F76628AA59
S[12]=7EFEEF328B7ADE15
S[13]=A1B7099E65A46614
S[14]=48F8A98FF4343C4B
S[15]=DE4B483FCE6EED4
S[16]=8484CE57B1BB9A90
S[17]=3868D06995410000
S[18]=8661870418CF3CA1
S[19]=FDA85357FD33AE90
S[20]=E18C4EAB82652980
S[21]=E7B08BAE4D637F33
S[22]=2299A2BBE88C0997
S[23]=26D1FD68E7BCC71
S[24]=9EA023C928860C61
S[25]=586E18C6C8D70F12
S[26]=1188C707BD1F6939
S[27]=BE02496AFC82C585
S[28]=B3F9DB29B61490E0
S[29]=C4651D7CBA1C2243
S[30]=FF2DC6661120535
S[31]=72F313EB2571932

Rotate left for 32 bits
S[0]=6803C36FDCB57AD2
S[1]=EAAF4EEAC8B6FCAB
S[2]=DF235E2DD202C848
S[3]=786E08B92806449F

S[4]=14B6A35D392EE991
S[5]=E4AB44B86ED0798E
S[6]=56C23FD692CEBADA
S[7]=7660A13C600C94BA
S[8]=51C348B3876A86AF
S[9]=9FBC98BCD88C80B0
S[10]=FD6F979013037423
S[11]=6628AA59787D46F7
S[12]=8B7ADE157EFEEF32
S[13]=65A46614A1B7099E
S[14]=F4343C4B48F8A98F
S[15]=CE6EED4DE4B483F
S[16]=B1BB9A908484CE57
S[17]=954100003868D069
S[18]=18CF3CA186618704
S[19]=FD33AE90FDA85357
S[20]=82652980E18C4EAB
S[21]=4D637F33E7B08BAE
S[22]=E88C09972299A2BB
S[23]=E7BCC7126D1FD68
S[24]=28860C619EA023C9
S[25]=C8D70F12586E18C6
S[26]=BD1F69391188C707
S[27]=FC82C585BE02496A
S[28]=B61490E0B3F9DB29
S[29]=BA1C2243C4651D7C
S[30]=61120535FF2DC66
S[31]=257193272F313EB

RAE transformation
S[0]=861EF70C404807DD
S[1]=F82EE57747F5B967
S[2]=B9117B57999168F6
S[3]=3B670CB85EE73C07
S[4]=745B1B7F7E8C0449
S[5]=3659FA1E14C97870
S[6]=9F94B082A9BF180D
S[7]=377194C28ACDF053
S[8]=54872498BC985CA
S[9]=124AC13F4B6C1636
S[10]=26C50707A5F6C877
S[11]=5F374C1655EA700B
S[12]=CAFBFD5FF5B6DE8C
S[13]=B0EA2FA0AF7C660F
S[14]=B80A3EE419EDF2EE
S[15]=6942FBBE93840532
S[16]=6BBCF102ACC8241F
S[17]=97B4D722B44CC8FB
S[18]=23497B8A24136C4
S[19]=5E2DE72428CC214
S[20]=E97417CDAFF718E
S[21]=BEDE5DE8937F385C
S[22]=F53361F58A8727A
S[23]=26A81DD961286237
S[24]=10A3EDC1F5CC4EB2
S[25]=827439E07CC23933
S[26]=DAE169622310FD74

S[27]=3540BBFDEF35220E
S[28]=9D397E9428D7B291
S[29]=C3F4A8AAD41E686B
S[30]=F9533076ED5A2382
S[31]=EF4618080A93C06

H[0]=F82EE57747F5B967
H[1]=3B670CB85EE73C07
H[2]=3659FA1E14C97870
H[3]=377194C28ACDF053
H[4]=124AC13F4B6C1636
H[5]=5F374C1655EA700B
H[6]=B0EA2FA0AF7C660F
H[7]=6942FBBE93840532
H[8]=97B4D722B44CC8FB
H[9]=5E2DE72428CC214
H[10]=BEDE5DE8937F385C
H[11]=26A81DD961286237
H[12]=827439E07CC23933
H[13]=3540BBFDEF35220E
H[14]=C3F4A8AAD41E686B
H[15]=EF4618080A93C06

Message digest is:
5E E7 3C 7 3B 67 C B8 8A CD F0 53 37 71 94 C2 55 EA 70 B 5F 37 4C 16 93 84 5 32 69
42 FB BE 42 8C C2 14 5 E2 DE 72 61 28 62 37 26 A8 1D D9
==========

##########

Two Block Message Sample
Input Message: STIPSTIPSTIPSTIPSTIPSTIPSTIPSTIPSTIPSTIPSTIPSTIPSTIP

==========

Initial Hash Values:
H[0]=F3BCC9086A09E667
H[1]=C1059ED8CBBB9D5D
H[2]=84CAA73BBB67AE85
H[3]=367CD507629A292A
H[4]=FE94F82B3C6EF372
H[5]=3070DD179159015A
H[6]=5F1D36F1A54FF53A
H[7]=F70E5939152FECD8
H[8]=ADE682D1510E527F
H[9]=FFC00B3167332667
H[10]=2B3E6C1F9B05688C
H[11]=685815118EB44A87
H[12]=FB41BD6B1F83D9AB
H[13]=64F98FA7DB0C2E0D
H[14]=137E21795BE0CD19
H[15]=BEFA4FA447B5481D
==========

Block contents:
M[0]=5049545350495453
M[1]=5049545350495453
M[2]=5049545350495453
M[3]=5049545350495453
M[4]=5049545350495453
M[5]=5049545350495453
M[6]=5049545350495453
M[7]=10
M[8]=00
M[9]=00
M[10]=00
M[11]=00
M[12]=00
M[13]=00
M[14]=00
M[15]=1C00
==========

in compile
S[0]=5049545350495453
S[1]=F3BCC9086A09E667
S[2]=5049545350495453
S[3]=C1059ED8CBBB9D5D
S[4]=5049545350495453
S[5]=84CAA73BBB67AE85
S[6]=5049545350495453
S[7]=367CD507629A292A
S[8]=5049545350495453
S[9]=FE94F82B3C6EF372
S[10]=5049545350495453
S[11]=3070DD179159015A
S[12]=5049545350495453
S[13]=5F1D36F1A54FF53A
S[14]=10
S[15]=F70E5939152FECD8
S[16]=00
S[17]=ADE682D1510E527F
S[18]=00
S[19]=FFC00B3167332667
S[20]=00
S[21]=2B3E6C1F9B05688C
S[22]=00
S[23]=685815118EB44A87
S[24]=00
S[25]=FB41BD6B1F83D9AB
S[26]=00
S[27]=64F98FA7DB0C2E0D
S[28]=00
S[29]=137E21795BE0CD19
S[30]=1C00
S[31]=BEFA4FA447B5481D

after LinTr512^32
S[0]=5DCB03FF9B327555
S[1]=C6F4DA966ADDAEEA

S[2]=AC32D2D9D39F6FD0
S[3]=9101A16D1F987281
S[4]=E4435E2B4959D4B2
S[5]=70F64842F8463819
S[6]=303832C4CC0793C1
S[7]=82B1BDCDF4AADE5A
S[8]=5C190E0854739B2F
S[9]=404DC7DC2DBC20EA
S[10]=B2C2B911F11725C1
S[11]=AA5C1A22149758ED
S[12]=BD524DEC6645C1CE
S[13]=2FFE6AFC81191388
S[14]=843EE3E233D12C67
S[15]=7472570A205226F7
S[16]=9BB9278465F3E0D0
S[17]=D8CFCEF175663564
S[18]=388DA974E4D33E96
S[19]=D28312356671515
S[20]=FAE1278EB5F8466A
S[21]=A13C179DAABC854
S[22]=60BADF7BF5A88F44
S[23]=8B9EC4594E610FEC
S[24]=75294C202468671B
S[25]=FB41BD6B1F83D9AB
S[26]=F2E83A1231543372
S[27]=64F98FA7DB0C2E0D
S[28]=DA4B2FD0C1E7F48B
S[29]=137E21795BE0CD19
S[30]=B38F851B909C1138
S[31]=EEB31BF617FC1C4E

leaders l1
l1=24BFDE956102440 l2=3D347446F337E252

extended Feistel networks parameters
a1=41 b1=A0 c1=C
a2=CC b2=55 c2=39
a3=A6 b3=6D c3=41
alpha1=C0B2 beta1=721B gama1=B2E9
alpha2=F091 beta2=822F gama2=BC19
A1=5AE7EAF B1=5D1ED333 C1=E75ED556
A2=ED50B8E8 B2=5423535E C2=F8B13AEC

AE transformation
S[0]=7BD3183259A87040
S[1]=80B6868EB40F81B
S[2]=602FD99DCE3DF8E7
S[3]=F1D2132C7A06D649
S[4]=9FC786C7EA18561
S[5]=3E41D5C4F7ECCE5A
S[6]=4D7D1AB197EBD722
S[7]=D7C4726EA39BC546
S[8]=36E11C863E196BFE
S[9]=6D602F441F717DFB
S[10]=4AE360EE66590A2A
S[11]=EDF3032B4E5A4770
S[12]=3BB6E0A275FCA39A

S[13]=306A60EAC0FC4C45
S[14]=ACF6FD556E8F5E6
S[15]=38B44F4E70E75B0D
S[16]=313DA9702F89CF29
S[17]=F7331626A20AFD5B
S[18]=494A6E4F63056D7
S[19]=B60607514F5D829E
S[20]=BE73305FA503194
S[21]=BAA9D87531AEBC4
S[22]=4DA06CD78BD89960
S[23]=A255E0CB196E842A
S[24]=44A6E5B34390797F
S[25]=D159688BDE84B971
S[26]=1C11D69A253D552
S[27]=C38983CE3B50B944
S[28]=3220641583D6166A
S[29]=7B2565478AE1741
S[30]=9DDA0AFD80900EE
S[31]=ACB5D25A706C5FE4

Rotate left for 32 bits
S[0]=59A870407BD31832
S[1]=EB40F81B80B6868
S[2]=CE3DF8E7602FD99D
S[3]=7A06D649F1D2132C
S[4]=7EA185619FC786C
S[5]=F7ECCE5A3E41D5C4
S[6]=97EBD7224D7D1AB1
S[7]=A39BC546D7C4726E
S[8]=3E196BFE36E11C86
S[9]=1F717DFB6D602F44
S[10]=66590A2A4AE360EE
S[11]=4E5A4770EDF3032B
S[12]=75FCA39A3BB6E0A2
S[13]=C0FC4C45306A60EA
S[14]=6E8F5E6ACF6FD55
S[15]=70E75B0D38B44F4E
S[16]=2F89CF29313DA970
S[17]=A20AFD5BF7331626
S[18]=F63056D7494A6E4
S[19]=4F5D829EB6060751
S[20]=FA503194BE73305
S[21]=31AEBC4BAA9D875
S[22]=8BD899604DA06CD7
S[23]=196E842AA255E0CB
S[24]=4390797F44A6E5B3
S[25]=DE84B971D159688B
S[26]=253D5521C11D69A
S[27]=3B50B944C38983CE
S[28]=83D6166A32206415
S[29]=8AE17417B256547
S[30]=80900EE9DDA0AFD
S[31]=706C5FE4ACB5D25A

RAE transformation
S[0]=9F45FE0BCAA489BD
S[1]=5719049452CA1D8F

S[2]=2F5975724634C888
S[3]=743653AFC6FDEA73
S[4]=3291C60FB61055E
S[5]=304333612C7807A9
S[6]=CF1E9A68B38D4414
S[7]=52C82B07D6050F46
S[8]=1C8819465E5C1C4
S[9]=64700827DD444A71
S[10]=285E47D5FB4A1B6E
S[11]=C0487C60BFECE37
S[12]=780F14F180AA6AA3
S[13]=7A8C2E129EC3708
S[14]=913B9554260CC151
S[15]=7B26A5DBA2C41A49
S[16]=B5095EA5E1CEF0CF
S[17]=7562272B56BEC7EA
S[18]=65ABFB55271F64C2
S[19]=DE9A3EF2E420784F
S[20]=8339AFD3DEB468F7
S[21]=E0D7BD0C6ABDC25
S[22]=6D3DB4126656F97
S[23]=C3AF7340C1C4D5E7
S[24]=CF9FCA4A3A9EC686
S[25]=A1917EC72CD919A4
S[26]=E4A8F792268E84C
S[27]=7E91BEEA317C3B30
S[28]=5EF2C43AB9B5C414
S[29]=93C31D6B8E89F52D
S[30]=4F44F34DC15EEAC3
S[31]=749F673BBAD52FEF

H[0]=5719049452CA1D8F
H[1]=743653AFC6FDEA73
H[2]=304333612C7807A9
H[3]=52C82B07D6050F46
H[4]=64700827DD444A71
H[5]=C0487C60BFECE37
H[6]=7A8C2E129EC3708
H[7]=7B26A5DBA2C41A49
H[8]=7562272B56BEC7EA
H[9]=DE9A3EF2E420784F
H[10]=E0D7BD0C6ABDC25
H[11]=C3AF7340C1C4D5E7
H[12]=A1917EC72CD919A4
H[13]=7E91BEEA317C3B30
H[14]=93C31D6B8E89F52D
H[15]=749F673BBAD52FEF

Message digest is:
C6 FD EA 73 74 36 53 AF D6 5 F 46 52 C8 2B 7 B FE CE 37 C0 48 7C 60 A2 C4 1A 49 7B
26 A5 DB E4 20 78 4F DE 9A 3E F2 C1 C4 D5 E7 C3 AF 73 40
==========

IntermediateValuesKAT_512.txt
Algorithm Name: NaSHA

Principal Submitter: Smile Markovski
Message Digest Lenght = 512

##

One Block Message Sample
Input Message: STIP

==

Initial Hash Values:
H[0]=3C4E3EFB2DD8A09A
H[1]=6F166B73E07688DC
H[2]=60948DCD61A77A0
H[3]=315E01D5C34AA2A
H[4]=80559CE68A47EA18
H[5]=4A0B98F4C785F436
H[6]=264607A89F22535B
H[7]=56E1288C53A8C8CA
H[8]=9CCDE59D2547D84E
H[9]=317C57A13C1563A9
H[10]=C7D8037F9486EB50
H[11]=D21E9A4077341EDA
H[12]=41C9CB74C0F905D7
H[13]=45121DBBD648813E
H[14]=A985E51EAD0D1E41
H[15]=7DF11B004CF768FC
==

Block contents:
M[0]=504954531
M[1]=00
M[2]=00
M[3]=00
M[4]=00
M[5]=00
M[6]=00
M[7]=00
M[8]=00
M[9]=00
M[10]=00
M[11]=00
M[12]=00
M[13]=00
M[14]=00
M[15]=200
==

in compile
S[0]=504954531
S[1]=3C4E3EFB2DD8A09A
S[2]=00
S[3]=6F166B73E07688DC
S[4]=00
S[5]=60948DCD61A77A0
S[6]=00

S[7]=315E01D5C34AA2A
S[8]=00
S[9]=80559CE68A47EA18
S[10]=00
S[11]=4A0B98F4C785F436
S[12]=00
S[13]=264607A89F22535B
S[14]=00
S[15]=56E1288C53A8C8CA
S[16]=00
S[17]=9CCDE59D2547D84E
S[18]=00
S[19]=317C57A13C1563A9
S[20]=00
S[21]=C7D8037F9486EB50
S[22]=00
S[23]=D21E9A4077341EDA
S[24]=00
S[25]=41C9CB74C0F905D7
S[26]=00
S[27]=45121DBBD648813E
S[28]=00
S[29]=A985E51EAD0D1E41
S[30]=200
S[31]=7DF11B004CF768FC

after LinTr512^32
S[0]=5F35B137F7A39596
S[1]=2D1E0A8C1821F80F
S[2]=B2B53D3026C01576
S[3]=8866187119EB01C1
S[4]=B53713637C39D8A4
S[5]=6187DEC336C7AB24
S[6]=902D6EB7EE4F8A4E
S[7]=432102957241C381
S[8]=2741CC68F1FBD7A1
S[9]=EB416E0DB04B569F
S[10]=6270BAD2604C4FDD
S[11]=A0A9546076AB8C67
S[12]=999D326B77CDBC1C
S[13]=C8C18630854B9E58
S[14]=BDC6174C86CAC881
S[15]=5DDD78D6451B53C0
S[16]=BB760DA35F88A61F
S[17]=1CE64E8640C3C2D7
S[18]=67C539282AA4517A
S[19]=BC1BA21DA79F4A82
S[20]=C427160A91C5AB9
S[21]=251DF38727F37CEA
S[22]=9FF0405FF8BFA12B
S[23]=46D28A45993824FB
S[24]=D062FF4865841A98
S[25]=11809F27C0F905D6
S[26]=8D67F5BC9B8A292B
S[27]=45121DBBD648813E
S[28]=E2C5F0F8B37597BA
S[29]=A985E51EAD0D1E41

S[30]=94CC1005EE0C3A21
S[31]=7DF11B004CF768FC

leaders l1
l1=8C53BBC3FC58DA5 l2=3B1B55A140AB1738

extended Feistel networks parameters
a1=B3 b1=1 c1=83
a2=C9 b2=16 c2=BE
a3=F2 b3=26 c3=B3
alpha1=6091 beta1=4DCF gama1=D34E
alpha2=714C beta2=A247 gama2=2E41
A1=D6F7DC45 B1=31A0F32 C1=FD195A75
A2=625EB89B B2=CBE61C42 C2=1BA39022

AE transformation
S[0]=1EC9BCE3E430FE3C
S[1]=3D70364CA82FE9A9
S[2]=2D28FBC4B2A7877F
S[3]=68A519A4F2F5D1C0
S[4]=A1BBF5262253A85
S[5]=5B78BC7F82F47A4B
S[6]=73599B0B4333138A
S[7]=22DFE2EC51ED80F1
S[8]=CF912AC14A6C68D8
S[9]=6E805282372F7C19
S[10]=1B3FFC5043A241E
S[11]=91C99354BB1C54F2
S[12]=1290564013C1978D
S[13]=B7396858402C185D
S[14]=ACEC9F0299047C2C
S[15]=9029C4F6C4FBE08B
S[16]=26BEDF5F7996A560
S[17]=BCE2A9F9C9777DF1
S[18]=5A8D4F18BF315736
S[19]=17829E22DBDBC5EF
S[20]=66BAE362506CF81E
S[21]=661E14865FC185C1
S[22]=128AF187B7B669D4
S[23]=47733EFF50400937
S[24]=F8D3927D74C707D2
S[25]=73C4D299DDA7710
S[26]=BB9E8255C136C887
S[27]=8070028B451DE0D0
S[28]=93A61896E4724884
S[29]=B4A351E7EF54DAAE
S[30]=EFB60C09E558978D
S[31]=6A16B3A8A5688B0

Rotate left for 32 bits
S[0]=E430FE3C1EC9BCE3
S[1]=A82FE9A93D70364C
S[2]=B2A7877F2D28FBC4
S[3]=F2F5D1C068A519A4
S[4]=2253A85A1BBF526
S[5]=82F47A4B5B78BC7F
S[6]=4333138A73599B0B

S[7]=51ED80F122DFE2EC
S[8]=4A6C68D8CF912AC1
S[9]=372F7C196E805282
S[10]=43A241E1B3FFC50
S[11]=BB1C54F291C99354
S[12]=13C1978D12905640
S[13]=402C185DB7396858
S[14]=99047C2CACEC9F02
S[15]=C4FBE08B9029C4F6
S[16]=7996A56026BEDF5F
S[17]=C9777DF1BCE2A9F9
S[18]=BF3157365A8D4F18
S[19]=DBDBC5EF17829E22
S[20]=506CF81E66BAE362
S[21]=5FC185C1661E1486
S[22]=B7B669D4128AF187
S[23]=5040093747733EFF
S[24]=74C707D2F8D3927D
S[25]=DDA771073C4D299
S[26]=C136C887BB9E8255
S[27]=451DE0D08070028B
S[28]=E472488493A61896
S[29]=EF54DAAEB4A351E7
S[30]=E558978DEFB60C09
S[31]=8A5688B06A16B3A

RAE transformation
S[0]=8762D2FBF54FC6C
S[1]=8A0CC5E9C83DC20A
S[2]=DAAA8C684326AEDC
S[3]=7BFD422B90525CCD
S[4]=1A1B1729A544C3DA
S[5]=B91F340DDCBF3A30
S[6]=4E63146691C9B9D2
S[7]=3B5DA1125ADB0B54
S[8]=D47A59A22C3006C0
S[9]=B8CDF4E137A76078
S[10]=8B4565F13221F46E
S[11]=D5D1A68B730EA5F2
S[12]=17743B3CE7134661
S[13]=53F396E0DEA8F0DA
S[14]=FDCE12689E71280
S[15]=AD96790F73A8409
S[16]=43F675981943C543
S[17]=346942CB88B55134
S[18]=34757E7D218DBE37
S[19]=72F1986E74336F25
S[20]=EF7481B3EF63B7D0
S[21]=81058DEBA5688DFA
S[22]=EC864AE46E924B7E
S[23]=2D779C564BC9AA94
S[24]=664B273587E8EC55
S[25]=27E91AE114EDDF32
S[26]=3C1FFBCCBECE8FCC
S[27]=2707AFA139FA05A3
S[28]=B01C92C66B132BF3
S[29]=3095640564925ECE

S[30]=B7E8C2DA9A024F8B
S[31]=E02660D2E8C48CB8

H[0]=8A0CC5E9C83DC20A
H[1]=7BFD422B90525CCD
H[2]=B91F340DDCBF3A30
H[3]=3B5DA1125ADB0B54
H[4]=B8CDF4E137A76078
H[5]=D5D1A68B730EA5F2
H[6]=53F396E0DEA8F0DA
H[7]=AD96790F73A8409
H[8]=346942CB88B55134
H[9]=72F1986E74336F25
H[10]=81058DEBA5688DFA
H[11]=2D779C564BC9AA94
H[12]=27E91AE114EDDF32
H[13]=2707AFA139FA05A3
H[14]=3095640564925ECE
H[15]=E02660D2E8C48CB8

Message digest is:
90 52 5C CD 7B FD 42 2B 5A DB B 54 3B 5D A1 12 73 E A5 F2 D5 D1 A6 8B 7 3A 84 9 AD
96 79 F 74 33 6F 25 72 F1 98 6E 4B C9 AA 94 2D 77 9C 56 39 FA 5 A3 27 7 AF A1 E8 C4
8C B8 E0 26 60 D2
==========

##########

Two Block Message Sample
Input Message: STIPSTIPSTIPSTIPSTIPSTIPSTIPSTIPSTIPSTIPSTIPSTIPSTIP

==========

Initial Hash Values:
H[0]=3C4E3EFB2DD8A09A
H[1]=6F166B73E07688DC
H[2]=60948DCD61A77A0
H[3]=315E01D5C34AA2A
H[4]=80559CE68A47EA18
H[5]=4A0B98F4C785F436
H[6]=264607A89F22535B
H[7]=56E1288C53A8C8CA
H[8]=9CCDE59D2547D84E
H[9]=317C57A13C1563A9
H[10]=C7D8037F9486EB50
H[11]=D21E9A4077341EDA
H[12]=41C9CB74C0F905D7
H[13]=45121DBBD648813E
H[14]=A985E51EAD0D1E41
H[15]=7DF11B004CF768FC
==========

Block contents:
M[0]=5049545350495453

M[1]=5049545350495453
M[2]=5049545350495453
M[3]=5049545350495453
M[4]=5049545350495453
M[5]=5049545350495453
M[6]=5049545350495453
M[7]=10
M[8]=00
M[9]=00
M[10]=00
M[11]=00
M[12]=00
M[13]=00
M[14]=00
M[15]=1C00
==========

in compile
S[0]=5049545350495453
S[1]=3C4E3EFB2DD8A09A
S[2]=5049545350495453
S[3]=6F166B73E07688DC
S[4]=5049545350495453
S[5]=60948DCD61A77A0
S[6]=5049545350495453
S[7]=315E01D5C34AA2A
S[8]=5049545350495453
S[9]=80559CE68A47EA18
S[10]=5049545350495453
S[11]=4A0B98F4C785F436
S[12]=5049545350495453
S[13]=264607A89F22535B
S[14]=10
S[15]=56E1288C53A8C8CA
S[16]=00
S[17]=9CCDE59D2547D84E
S[18]=00
S[19]=317C57A13C1563A9
S[20]=00
S[21]=C7D8037F9486EB50
S[22]=00
S[23]=D21E9A4077341EDA
S[24]=00
S[25]=41C9CB74C0F905D7
S[26]=00
S[27]=45121DBBD648813E
S[28]=00
S[29]=A985E51EAD0D1E41
S[30]=1C00
S[31]=7DF11B004CF768FC

after LinTr512^32
S[0]=F7CE484F7A39597
S[1]=7D575F3E4868AC5C
S[2]=E2FC688226C01577
S[3]=D82F4C2319EB01C0

S[4]=E57E47307C39D8A5
S[5]=31CE8B70668EFF77
S[6]=902D6EB7EE4F8A4E
S[7]=136856C67241C380
S[8]=7708983BA1B283F2
S[9]=EB416FEDB04B569F
S[10]=6270BAD3604C4FDD
S[11]=A0A9546026E2D835
S[12]=C9D466382784E84F
S[13]=9888D263D502CA0B
S[14]=ED8F431FD6839CD2
S[15]=D942D6515520793
S[16]=BB760C425F88A61F
S[17]=1CE64E87108A9685
S[18]=378C6D7B2AA4517B
S[19]=BC1BA21DA79F4A82
S[20]=C427160A91C5AB9
S[21]=7554A7D577BA28B9
S[22]=9FF0405FF8BFA12B
S[23]=169BDFF6C97170A8
S[24]=802BAB1A35CD4ECB
S[25]=41C9CB74C0F905D7
S[26]=8D67F5BC9B8A292B
S[27]=45121DBBD648813E
S[28]=E2C5F0F8B37597BA
S[29]=A985E51EAD0D1E41
S[30]=94CC11E5EE0C3A21
S[31]=2DB84F521CBE3CAF

leaders l1
l1=8CD443C2400C41F3 l2=BB2BB4A540AB1738

extended Feistel networks parameters
a1=E2 b1=C8 c1=D8
a2=1D b2=17 c2=4C
a3=D2 b3=A0 c3=E2
alpha1=6091 beta1=4DCE gama1=A395
alpha2=C57D beta2=51FD gama2=DA92
A1=872F2813 B1=31A0F33 C1=FC87B25B
A2=625D389B B2=EBD5A465 C2=FB237084

AE transformation
S[0]=6CEC01D1B558C029
S[1]=271FC9F25853BA7E
S[2]=30093755490F6792
S[3]=BDB5F49E4ED3E688
S[4]=FF64D897BD5C8C48
S[5]=4A0C8D98E15C3813
S[6]=F2E12699237430A5
S[7]=ED56573E04FC00A
S[8]=E0FDDAE5D448CE74
S[9]=2B71A54E101A5BB3
S[10]=797851DC8F1BD3C
S[11]=8A1372BC1B45027A
S[12]=C385DA953A987E90
S[13]=ED5A963F96AB9C83
S[14]=1DB273EF66CA2E80

S[15]=393B45CDB4AFA3B1
S[16]=7F5B6E4F9760D041
S[17]=880692B917024CC7
S[18]=E011DB6425941427
S[19]=D8FBD3BD86BD0D
S[20]=E95032DFC74F46D7
S[21]=915669D5DB657DCB
S[22]=88D1B975D1266353
S[23]=D230B587C7A81E26
S[24]=52F8D48C6095AD63
S[25]=1A1A116492DD46B0
S[26]=1BC693AA3640F3A4
S[27]=E2DD520F74AD05F3
S[28]=1BBD5193133C0C56
S[29]=C6BE84B946E4E5FD
S[30]=189A65A9A6659549
S[31]=D85C9E85F07BEF15

Rotate left for 32 bits
S[0]=B558C0296CEC01D1
S[1]=5853BA7E271FC9F2
S[2]=490F679230093755
S[3]=4ED3E688BDB5F49E
S[4]=BD5C8C48FF64D897
S[5]=E15C38134A0C8D98
S[6]=237430A5F2E12699
S[7]=E04FC00AED56573
S[8]=D448CE74E0FDDAE5
S[9]=101A5BB32B71A54E
S[10]=8F1BD3C797851DC
S[11]=1B45027A8A1372BC
S[12]=3A987E90C385DA95
S[13]=96AB9C83ED5A963F
S[14]=66CA2E801DB273EF
S[15]=B4AFA3B1393B45CD
S[16]=9760D0417F5B6E4F
S[17]=17024CC7880692B9
S[18]=25941427E011DB64
S[19]=86BD0DD8FBD3BD
S[20]=C74F46D7E95032DF
S[21]=DB657DCB915669D5
S[22]=D126635388D1B975
S[23]=C7A81E26D230B587
S[24]=6095AD6352F8D48C
S[25]=92DD46B01A1A1164
S[26]=3640F3A41BC693AA
S[27]=74AD05F3E2DD520F
S[28]=133C0C561BBD5193
S[29]=46E4E5FDC6BE84B9
S[30]=A6659549189A65A9
S[31]=F07BEF15D85C9E85

RAE transformation
S[0]=3C2BCC6D457C6E1C
S[1]=D6609C92ACD4C843
S[2]=C423C979638DFF5E
S[3]=68451DB9C981EDC7

S[4]=DA96A1D3EAFC6F0
S[5]=FFE499F06D8A7B83
S[6]=74F0549BC13B8BF
S[7]=BF1235782CDBB003
S[8]=D253C11ED956446
S[9]=49C34B02C48EB0F9
S[10]=BC6763181B75CE7
S[11]=478EBD7942235219
S[12]=33FDA876EA664F4C
S[13]=727AE3D75C2A908B
S[14]=DAD958D0EBFE2B80
S[15]=58D32A2E3341F146
S[16]=78CFD6158F90CDDC
S[17]=199231362F96803
S[18]=F05400BA99AFDD4
S[19]=3C923725AC63BEC0
S[20]=908C0CE386AF1EE9
S[21]=977BFBC39425EF5F
S[22]=6F1F8B0CD6423902
S[23]=630E5C35C83C23CC
S[24]=53517ED7A4FFE404
S[25]=2F3FA76ED6E950A1
S[26]=13AC520985713F6
S[27]=8BCD879AF27E104D
S[28]=5971D04E47B3A955
S[29]=17A41A0E756A69
S[30]=8BFC680A2F6F744F
S[31]=3E8A1E0BF71E0520

H[0]=D6609C92ACD4C843
H[1]=68451DB9C981EDC7
H[2]=FFE499F06D8A7B83
H[3]=BF1235782CDBB003
H[4]=49C34B02C48EB0F9
H[5]=478EBD7942235219
H[6]=727AE3D75C2A908B
H[7]=58D32A2E3341F146
H[8]=199231362F96803
H[9]=3C923725AC63BEC0
H[10]=977BFBC39425EF5F
H[11]=630E5C35C83C23CC
H[12]=2F3FA76ED6E950A1
H[13]=8BCD879AF27E104D
H[14]=17A41A0E756A69
H[15]=3E8A1E0BF71E0520

Message digest is:
C9 81 ED C7 68 45 1D B9 2C DB B0 3 BF 12 35 78 42 23 52 19 47 8E BD 79 33 41 F1 46
58 D3 2A 2E AC 63 BE C0 3C 92 37 25 C8 3C 23 CC 63 E 5C 35 F2 7E 10 4D 8B CD 87 9A
F7 1E 5 20 3E 8A 1E B
==========