Secure Hash Algorithm
Message Digest Length = 224

One Block Message Sample
Input Message: "abc"

Initial hash value:
H[0] = C1059ED8
H[1] = 367CD507
H[2] = 30700D17
H[4] = FFC00831
H[5] = 68581511
H[6] = 64F98FA7
H[7] = BEFA4FA4

Block Contents:
W[0] = 61626380
W[1] = 00000000
W[2] = 00000000
W[3] = 00000000
W[4] = 00000000
W[5] = 00000000
W[6] = 00000000
W[7] = 00000000
W[8] = 00000000
W[9] = 00000000
W[10] = 00000000
W[12] = 00000000
W[13] = 00000000
W[14] = 00000000
W[15] = 00000000

A B C D E F G H
0: 0E96B2DA C1059ED8 367CD507 30700D17 0434222E FFC00831 68581511 64F98FA7
1: C20DA680 0E96B2DA C1059ED8 367CD507 9CA8416F 0434222E FFC00831 68581511
2: AB113B7A C20DA680 0E96B2DA C1059ED8 82177FE8 9CA8416F 0434222E FFC00831
3: 8253CC1A AB113B7A C20DA680 0E96B2DA 8346B27D 82177FE8 9CA8416F 0434222E
4: 08A0DC0C 8253CC1A AB113B7A C20DA680 058557DB 8346B27D 82177FE8 9CA8416F
5: B2CA3A91 08A0DC0C 8253CC1A AB113B7A 890DC7BB 058557DB 8346B27D 82177FE8
6: 08B69023 B2CA3A91 08A0DC0C 8253CC1A A2E49147 890DC7BB 058557DB 8346B27D
7: F09D1160 08B69023 B2CA3A91 08A0DC0C 7A84120D A2E49147 890DC7BB 058557DB
8: ED6FA633 F09D1160 08B69023 B2CA3A91 0C37FAAD 7A84120D A2E49147 890DC7BB
9: 5566A637 ED6FA633 F09D1160 08B69023 AAE50091 0C37FAAD 7A84120D A2E49147
10: 0817E82B S56EA637 ED6FA633 F09D1160 82C53A2C AAE50091 C037FAAD 7A84120D
11: 17142334 0817E82B S56EA637 ED6FA633 D4C7BE9 C8C53A2C AAE50091 C037FAAD
12: FC4F023E 17142334 0817E82B S56EA637 D4C7BE9 878EBEA51A D4C7BE9 C8C53A2C AAE50091
13: BE316902 FC4F023E 17142334 0817E82B 65141125 878EBEA51A D4C7BE9 C8C53A2C
14: 1D800178 BE316902 FC4F023E 17142334 4545F53A 65141125 878EBEA51A D4C7BE9
15: 9F341A45 1D800178 BE316902 FC4F023E 6A61C411 4545F53A 65141125 878EBEA51A
16: 0F324089 9F341A45 1D800178 BE316902 06C8006A 6A61C411 4545F53A 65141125
17: FFE70128 0F324089 9F341A45 1D800178 B78601F4 06C8006A 6A61C411 4545F53A
18: 62932AB8 FFE70128 0F324089 9F341A45 7638B27A B78601F4 06C8006A 6A61C411
t=19: 5207D867 62932AB8 FFE70128 7FBA936 763B627A 878601F4 06C80D6A

H[0] = C1059ED8 + 6203DE4A = 23097D22
H[1] = 367CD507 + FD89031B = 3405D822
H[2] = 3070DD17 + 55D1C700 = 8642A477
H[3] = F70E5937 + C693FC7A = BDA255B3
H[4] = FFC00B31 + 2AD0B183 = 2AAD8CE4
H[5] = 68581511 + 55489EE6 = BDA0B3F7
H[6] = 64F98FA7 + 77E30E00 = E36CD9A7
H[7] = BEF4A4FA + 13DF8889 = D2DA882D

Message Digest is

23097D22
3405D822 8642A477 BDA255B3 2AAD8CE4 BDA0B3F7 E36CD9A7
Two Block Message Sample

Input Message:
"abcdecdefgefgghighijijikklmnlmnopnopq"

Initial hash value:
$H[0] = C1059ED8$
$H[1] = 367CD507$
$H[2] = 3070DD17$
$H[3] = F70E5939$
$H[4] = FF00831$
$H[5] = 68581511$
$H[6] = 64F98FA7$
$H[7] = BEFA4FA4$

Block Contents:
$W[0] = 61626364$
$W[1] = 62636465$
$W[2] = 63646566$
$W[3] = 64656667$
$W[4] = 65666768$
$W[5] = 66676869$
$W[6] = 6768696A$
$W[7] = 68696A6B$
$W[8] = 696A6B6C$
$W[9] = 6A6B6C6D$
$W[10] = 6B6C6D6E$
$W[12] = 6D6E6F70$
$W[13] = 6E6F7071$
$W[14] = 80000000$
$W[15] = 00000000$

A B C D E F G H
$t= 0: 0E96B2BE C1059ED8 367CD507 3070DD17 04342242 FFC00831 68581511 64F98FA7$
$t= 1: 51D17D7B 0E96B2BE C1059ED8 367CD507 2F8EA3D4 04342242 FFC00831 68581511$
$t= 2: FF1CBD7F 51D17D7B 0E96B2BE C1059ED8 79A896FA 2F8EA3D4 04342242 FFC00831$
$t= 3: 24BCC047 FF1CBD7F 51D17D7B 0E96B2BE 1F60795A 79A896FA 2F8EA3D4 04342242$
$t= 4: 7D56A6AC 24BCC047 FF1CBD7F 51D17D7B DE395286 1F60795A 79A896FA 2F8EA3D4$
$t= 5: 7458EB11 7D56A6AC 24BCC047 FF1CBD7F D863D132 DE395286 1F60795A 79A896FA$
$t= 6: 0DD41573 7458EB11 7D56A6AC 24BCC047 2E6D0323 D863D132 DE395286 1F60795A$
$t= 7: 9A2541FD 0DD41573 7458EB11 7D56A6AC 08D2B348 2E6D0323 D863D132 DE395286$
$t= 8: 314E5E99 9A2541FD 0DD41573 7458EB11 95DF0D70 08D2B348 2E6D0323 8D63D132$
$t= 9: B2954925 314E5E99 9A2541FD 0DD41573 05EF5E3D 95DF0D70 08D2B348 2E6D0323$
$t=10: B2A874FB 82954925 314E5E99 9A2541FD 8D30E98D 95DF0D70 08D2B348$
$t=11: 116CE44D B2A874FB 82954925 314E5E99 8D30E98D 95DF0D70 08D2B348$
$t=12: 5FF9349A 116CE44D B2A874FB 82954925 8EB33025 8D30E98D 95DF0D70 08D2B348$
$t=13: 7FA09E6D 5FF9349A 116CE44D B2A874FB 4657CF17 8EB33025 8D30E98D 95DF0D70 08D2B348$
$t=14: 06F831B6 7FA09E6D 5FF9349A 116CE44D D809E68D 4657CF17 8EB33025 8D30E98D 06D566A$
$t=15: B301C98A 06F831B6 7FA09E6D 5FF9349A 0EB1E816 4657CF17 8EB33025 8D30E98D 06D566A$
$t=16: E623ECC0 B301C98A 06F831B6 7FA09E6D 6F9349A 0EB1E816 4657CF17 8EB33025 8D30E98D$
$t=17: D9244A78 E623ECC0 B301C98A 06F831B6 6F9349A 0EB1E816 4657CF17 8EB33025 8D30E98D$
$t=18: 99C72726 D9244A78 E623ECC0 B301C98A 06F831B6 6F9349A 0EB1E816 4657CF17 8EB33025 8D30E98D$
$t=19: A80CBE02 99C72726 D9244A78 E623ECC0 010D7C65 B26A409C 8D608D0C 2B3F859C 0EB1E816 4657CF17 8EB33025 8D30E98D$
$t=20: 78662878 A80CBE02 99C72726 D9244A78 6E23ECC0 010D7C65 B26A409C 8D608D0C 2B3F859C 0EB1E816 4657CF17 8EB33025 8D30E98D$
$t=21: D7CC5C05 78662878 A80CBE02 99C72726 6B280360C 5678A949 010D7C65 B26A409C 8D608D0C 2B3F859C 0EB1E816 4657CF17 8EB33025 8D30E98D$
$t=22: 6D2AEE72 D7CC5C05 78662878 A80CBE02 0D4CD0C4 B280360C 5678A949 010D7C65 B26A409C 8D608D0C 2B3F859C 0EB1E816 4657CF17 8EB33025 8D30E98D$
$t=23: BCF47346 BAD2EE72 D7CC5C05 78662878 D6A19DC8 0D4CD0C4 B280360C 5678A949 010D7C65 B26A409C 8D608D0C 2B3F859C 0EB1E816 4657CF17 8EB33025 8D30E98D$
$t=24: SECC417B BCF47346 BAD2EE72 D7CC5C05 3337A11C D6A19DC8 0D4CD0C4 B280360C 5678A949 010D7C65 B26A409C 8D608D0C 2B3F859C 0EB1E816 4657CF17 8EB33025 8D30E98D
Block Contents:

<table>
<thead>
<tr>
<th>Block Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>W[0] = 00000000</td>
</tr>
<tr>
<td>W[1] = 00000000</td>
</tr>
<tr>
<td>W[2] = 00000000</td>
</tr>
<tr>
<td>W[3] = 00000000</td>
</tr>
<tr>
<td>W[4] = 00000000</td>
</tr>
<tr>
<td>W[5] = 00000000</td>
</tr>
<tr>
<td>W[6] = 00000000</td>
</tr>
<tr>
<td>W[7] = 00000000</td>
</tr>
<tr>
<td>W[8] = 00000000</td>
</tr>
<tr>
<td>W[9] = 00000000</td>
</tr>
<tr>
<td>W[10] = 00000000</td>
</tr>
</tbody>
</table>
t=58: 4EC725F6 882ED69E E8C8FEC7 D4EA8C7E CE1D1CE4 30267D8E 35F6800E 2958CE2A

H[0] = 8250E65D + F2E7A4B9 = 75388B16

H[1] = BCF62F84 + 94314748 = 512776CC 

Message Digest is

75388B16

512776CC 5DBA5DA1 FD890150 B0C6455C B4F58B19 52522525