

Blog Entry © Thursday, August 20, 2026, by James Pate Williams, Jr. A Tale of Two Secure Hashing Algorithms (SHA-1 and SHA-3)

I translated my old C version of SHA-1 to C++. I translated my C# SHA-3 source code to C++.

```

== Menu ==
1 SHA-1 Tests
2 SHA-3 Tests
3 BBS and Maurer Tests
4 Exit
Option (1 - 4): 1

DA39A3EE 5E6B4B0D 3255BFEF 95601890 AFD80709
a
86F7E437 FAA5A7FC E15D1DDC B9EAEAEA 377667B8
abc
A9993E36 4706816A BA3E2571 7850C26C 9CD0D89D
abcdefghijklmnopqrstuvwxyz
32D10C7B 8CF96570 CA04CE37 F2A19D84 240D3A89
The quick brown fox jumps over the lazy dog
2FD4E1C6 7A2D28FC ED849EE1 BB76E739 1B93EB12
The quick brown fox jumps over the lazy cog
DE9F2C7F D25E1B3A FAD3E85A 0BD17D9B 100DB4B3
== Menu ==
1 SHA-1 Tests
2 SHA-3 Tests
3 BBS and Maurer Tests
4 Exit
Option (1 - 4): 4

```

```

C:\Users\James\OneDrive\GuideToECC\x64\Release\GuideToECC.exe
(process 37960) exited with code 0 (0x0).
Press any key to close this window . . .

```

```

== Menu ==
1 SHA-1 Tests
2 SHA-3 Tests
3 BBS and Maurer Tests
4 Exit
Option (1 - 4): 2
== SHA-3 Test Menu ==
1 224
2 256
3 384
4 512
5 Exit

```

Option (1 - 5): 1
== Data Length Menu ==
1 0
2 5
3 30
4 1600
5 1605
6 1630
7 Exit
Option (1 - 7): 1

6B 4E 03 42 36 67 DB B7 3B 6E 15 45 4F 0E B1 AB
D4 59 7F 9A 1B 07 8E 3F 5B 5A 6B C7

== SHA-3 Test Menu ==
1 224
2 256
3 384
4 512
5 Exit
Option (1 - 5): 1
== Data Length Menu ==
1 0
2 5
3 30
4 1600
5 1605
6 1630
7 Exit
Option (1 - 7): 2

FF BA D5 DA 96 BA D7 17 89 33 02 06 DC 67 68 EC
AE B1 B3 2D CA 6B 33 01 48 96 74 AB

== SHA-3 Test Menu ==
1 224
2 256
3 384
4 512
5 Exit
Option (1 - 5): 1
== Data Length Menu ==
1 0
2 5
3 30
4 1600
5 1605

6 1630
 7 Exit
 Option (1 - 7): 3

D6 66 A5 14 CC 9D BA 25 AC 1B A6 9E D3 93 04 60
 DE AA C9 85 1B 5F 0B AA B0 07 DF 3B

== SHA-3 Test Menu ==

1 224
 2 256
 3 384
 4 512
 5 Exit
 Option (1 - 5): 1
 == Data Length Menu ==
 1 0
 2 5
 3 30
 4 1600
 5 1605
 6 1630
 7 Exit
 Option (1 - 7): 4

93 76 81 6A BA 50 3F 72 F9 6C E7 EB 65 AC 09 5D
 EE E3 BE 4B F9 BB C2 A1 CB 7E 11 E0

== SHA-3 Test Menu ==

1 224
 2 256
 3 384
 4 512
 5 Exit
 Option (1 - 5): 1
 == Data Length Menu ==
 1 0
 2 5
 3 30
 4 1600
 5 1605
 6 1630
 7 Exit
 Option (1 - 7): 5

22 D2 F7 BB 0B 17 3F D8 C1 96 86 F9 17 31 66 E3
 EE 62 73 80 47 D7 EA DD 69 EF B2 28

== SHA-3 Test Menu ==

- 1 224
- 2 256
- 3 384
- 4 512
- 5 Exit

Option (1 - 5): 1

== Data Length Menu ==

- 1 0
- 2 5
- 3 30
- 4 1600
- 5 1605
- 6 1630
- 7 Exit

Option (1 - 7): 6

4E 90 7B B1 05 78 61 F2 00 A5 99 E9 D4 F8 5B 02
D8 84 53 BF 5B 8A CE 9A C5 89 13 4C

== SHA-3 Test Menu ==

- 1 224
- 2 256
- 3 384
- 4 512
- 5 Exit

Option (1 - 5): 5

== Menu ==

- 1 SHA-1 Tests
- 2 SHA-3 Tests
- 3 BBS and Maurer Tests
- 4 Exit

Option (1 - 4): *Warning*

Illegal option

== Menu ==

- 1 SHA-1 Tests
- 2 SHA-3 Tests
- 3 BBS and Maurer Tests
- 4 Exit

Option (1 - 4): 4

C:\Users\James\OneDrive\GuideToECC\x64\Release\GuideToECC.exe
(process 21884) exited with code 0 (0x0).
Press any key to close this window . . .

== Menu ==

- 1 SHA-1 Tests

```

2 SHA-3 Tests
3 BBS and Maurer Tests
4 Exit

```

```
Option (1 - 4): 2
```

```
== SHA-3 Test Menu ==
```

```

1 224
2 256
3 384
4 512
5 Exit

```

```
Option (1 - 5): 2
```

```
== Data Length Menu ==
```

```

1 0
2 5
3 30
4 1600
5 1605
6 1630
7 Exit

```

```
Option (1 - 7): 1
```

```

A7 FF C6 F8 BF 1E D7 66 51 C1 47 56 A0 61 D6 62
F5 80 FF 4D E4 3B 49 FA 82 D8 0A 4B 80 F8 43 4A

```

```
== SHA-3 Test Menu ==
```

```

1 224
2 256
3 384
4 512
5 Exit

```

```
Option (1 - 5): 2
```

```
== Data Length Menu ==
```

```

1 0
2 5
3 30
4 1600
5 1605
6 1630
7 Exit

```

```
Option (1 - 7): 2
```

```

7B 00 47 CF 5A 45 68 82 36 3C BF 0F B0 53 22 CF
65 F4 B7 05 9A 46 36 5E 83 01 32 E3 B5 D9 57 AF

```

```
== SHA-3 Test Menu ==
```

```

1 224
2 256

```

```

3 384
4 512
5 Exit
Option (1 - 5): 2
== Data Length Menu ==
1 0
2 5
3 30
4 1600
5 1605
6 1630
7 Exit
Option (1 - 7): 3

```

```

C8 24 2F EF 40 9E 5A E9 D1 F1 C8 57 AE 4D C6 24
B9 2B 19 80 9F 62 AA 8C 07 41 1C 54 A0 78 B1 D0

```

```

== SHA-3 Test Menu ==
1 224
2 256
3 384
4 512
5 Exit
Option (1 - 5): 2
== Data Length Menu ==
1 0
2 5
3 30
4 1600
5 1605
6 1630
7 Exit
Option (1 - 7): 4

```

```

79 F3 8A DE C5 C2 03 07 A9 8E F7 6E 83 24 AF BF
D4 6C FD 81 B2 2E 39 73 C6 5F A1 BD 9D E3 17 87

```

```

== SHA-3 Test Menu ==
1 224
2 256
3 384
4 512
5 Exit
Option (1 - 5): 2
== Data Length Menu ==
1 0
2 5

```

3 30
4 1600
5 1605
6 1630
7 Exit

Option (1 - 7): 5

81 EE 76 9B ED 09 50 86 2B 1D DD ED 2E 84 AA A6
AB 7B FD D3 CE AA 47 1B E3 11 63 D4 03 36 36 3C

== SHA-3 Test Menu ==

1 224
2 256
3 384
4 512
5 Exit

Option (1 - 5): 2

== Data Length Menu ==

1 0
2 5
3 30
4 1600
5 1605
6 1630
7 Exit

Option (1 - 7): 6

52 86 0A A3 01 21 4C 61 0D 92 2A 6B 6C AB 98 1C
CD 06 01 2E 54 EF 68 9D 74 40 21 E7 38 B9 ED 20

== SHA-3 Test Menu ==

1 224
2 256
3 384
4 512
5 Exit

Option (1 - 5): 5

== Menu ==

1 SHA-1 Tests
2 SHA-3 Tests
3 BBS and Maurer Tests
4 Exit

Option (1 - 4): *Warning*

Illegal option

== Menu ==

1 SHA-1 Tests
2 SHA-3 Tests

3 BBS and Maurer Tests

4 Exit

Option (1 - 4): 4

C:\Users\James\OneDrive\GuideToECC\x64\Release\GuideToECC.exe

(process 20020) exited with code 0 (0x0).

Press any key to close this window . . .

== Menu ==

1 SHA-1 Tests

2 SHA-3 Tests

3 BBS and Maurer Tests

4 Exit

Option (1 - 4): 2

== SHA-3 Test Menu ==

1 224

2 256

3 384

4 512

5 Exit

Option (1 - 5): 3

== Data Length Menu ==

1 0

2 5

3 30

4 1600

5 1605

6 1630

7 Exit

Option (1 - 7): 1

0C 63 A7 5B 84 5E 4F 7D 01 10 7D 85 2E 4C 24 85

C5 1A 50 AA AA 94 FC 61 99 5E 71 BB EE 98 3A 2A

C3 71 38 31 26 4A DB 47 FB 6B D1 E0 58 D5 F0 04

== SHA-3 Test Menu ==

1 224

2 256

3 384

4 512

5 Exit

Option (1 - 5): 3

== Data Length Menu ==

1 0

2 5

3 30

4 1600

```

5 1605
6 1630
7 Exit
Option (1 - 7): 2

```

```

73 7C 9B 49 18 85 E9 BF 74 28 E7 92 74 1A 7B F8
DC A9 65 34 71 C3 E1 48 47 3F 2C 23 6B 6A 0A 64
55 EB 1D CE 9F 77 9B 4B 6B 23 7F EF 17 1B 1C 64

```

```

== SHA-3 Test Menu ==
1 224
2 256
3 384
4 512
5 Exit
Option (1 - 5): 3
== Data Length Menu ==
1 0
2 5
3 30
4 1600
5 1605
6 1630
7 Exit
Option (1 - 7): 3

```

```

95 5B 4D D1 BE 03 26 1B D7 6F 80 7A 7E FD 43 24
35 C4 17 36 28 11 B8 A5 0C 56 4E 7E E9 58 5E 1A
C7 62 6D DE 2F DC 03 0F 87 61 96 EA 26 7F 08 C3

```

```

== SHA-3 Test Menu ==
1 224
2 256
3 384
4 512
5 Exit
Option (1 - 5): 3
== Data Length Menu ==
1 0
2 5
3 30
4 1600
5 1605
6 1630
7 Exit
Option (1 - 7): 4

```

```

18 81 DE 2C A7 E4 1E F9 5D C4 73 2B 8F 5F 00 2B
18 9C C1 E4 2B 74 16 8E D1 73 26 49 CE 1D BC DD
76 19 7A 31 FD 55 EE 98 9F 2D 70 50 DD 47 3E 8F

```

```
== SHA-3 Test Menu ==
```

```

1 224
2 256
3 384
4 512
5 Exit

```

```
Option (1 - 5): 3
```

```
== Data Length Menu ==
```

```

1 0
2 5
3 30
4 1600
5 1605
6 1630
7 Exit

```

```
Option (1 - 7): 5
```

```

A3 1F DB D8 D5 76 55 1C 21 FB 11 91 B5 4B DA 65
B6 C5 FE 97 F0 F4 A6 91 03 42 4B 43 F7 FD B8 35
97 9F DB EA E8 B3 FE 16 CB 82 E5 87 38 1E B6 24

```

```
== SHA-3 Test Menu ==
```

```

1 224
2 256
3 384
4 512
5 Exit

```

```
Option (1 - 5): 3
```

```
== Data Length Menu ==
```

```

1 0
2 5
3 30
4 1600
5 1605
6 1630
7 Exit

```

```
Option (1 - 7): 6
```

```

34 85 D3 B2 80 BD 38 4C F4 A7 77 84 4E 94 67 81
73 05 5D 1C BC 40 C7 C2 C3 83 3D 9E F1 23 45 17
2D 6F CD 31 92 3B B8 79 5A C8 18 47 D3 D8 85 5C

```

```
== SHA-3 Test Menu ==
```

```
1 224
2 256
3 384
4 512
5 Exit
Option (1 - 5): 5
== Menu ==
1 SHA-1 Tests
2 SHA-3 Tests
3 BBS and Maurer Tests
4 Exit
Option (1 - 4): *Warning*
Illegal option
== Menu ==
1 SHA-1 Tests
2 SHA-3 Tests
3 BBS and Maurer Tests
4 Exit
Option (1 - 4): 4
```

```
C:\Users\James\OneDrive\GuideToECC\x64\Release\GuideToECC.exe
(process 30200) exited with code 0 (0x0).
Press any key to close this window . . .
```

```
== Menu ==
1 SHA-1 Tests
2 SHA-3 Tests
3 BBS and Maurer Tests
4 Exit
Option (1 - 4): 2
== SHA-3 Test Menu ==
1 224
2 256
3 384
4 512
5 Exit
Option (1 - 5): 4
== Data Length Menu ==
1 0
2 5
3 30
4 1600
5 1605
6 1630
7 Exit
```

Option (1 - 7): 1

A6 9F 73 CC A2 3A 9A C5 C8 B5 67 DC 18 5A 75 6E
97 C9 82 16 4F E2 58 59 E0 D1 DC C1 47 5C 80 A6
15 B2 12 3A F1 F5 F9 4C 11 E3 E9 40 2C 3A C5 58
F5 00 19 9D 95 B6 D3 E3 01 75 85 86 28 1D CD 26

== SHA-3 Test Menu ==

1 224

2 256

3 384

4 512

5 Exit

Option (1 - 5): 4

== Data Length Menu ==

1 0

2 5

3 30

4 1600

5 1605

6 1630

7 Exit

Option (1 - 7): 2

A1 3E 01 49 41 14 C0 98 00 62 2A 70 28 8C 43 21
21 CE 70 03 9D 75 3C AD D2 E0 06 E4 D9 61 CB 27
54 4C 14 81 E5 81 4B DC EB 53 BE 67 33 D5 E0 99
79 5E 5E 81 91 8A DD B0 58 E2 2A 9F 24 88 3F 37

== SHA-3 Test Menu ==

1 224

2 256

3 384

4 512

5 Exit

Option (1 - 5): 4

== Data Length Menu ==

1 0

2 5

3 30

4 1600

5 1605

6 1630

7 Exit

Option (1 - 7): 3

98 34 C0 5A 11 E1 C5 D3 DA 9C 74 0E 1C 10 6D 9E
59 0A 0E 53 0B 6F 6A AA 78 30 52 5D 07 5C A5 DB
1B D8 A6 AA 98 1A 28 61 3A C3 34 93 4A 01 82 3C
D4 5F 45 E4 9B 6D 7E 69 17 F2 F1 67 78 06 7B AB

== SHA-3 Test Menu ==

1 224

2 256

3 384

4 512

5 Exit

Option (1 - 5): 4

== Data Length Menu ==

1 0

2 5

3 30

4 1600

5 1605

6 1630

7 Exit

Option (1 - 7): 4

E7 6D FA D2 20 84 A8 B1 46 7F CF 2F FA 58 36 1B
EC 76 28 ED F5 F3 FD C0 E4 80 5D C4 8C AE EC A8
1B 7C 13 C3 0A DF 52 A3 65 95 84 73 9A 2D F4 6B
E5 89 C5 1C A1 A4 A8 41 6D F6 54 5A 1C E8 BA 00

== SHA-3 Test Menu ==

1 224

2 256

3 384

4 512

5 Exit

Option (1 - 5): 4

== Data Length Menu ==

1 0

2 5

3 30

4 1600

5 1605

6 1630

7 Exit

Option (1 - 7): 5

FC 4A 16 7C CB 31 A9 37 D6 98 FD E8 2B 04 34 8C
95 39 B2 8F 0C 9D 3B 45 05 70 9C 03 81 23 50 E4
99 0E 96 22 97 4F 6E 57 5C 47 86 1C 0D 2E 63 8C
CF C2 02 3C 36 5B B6 0A 93 F5 28 55 06 98 78 6B

== SHA-3 Test Menu ==

1 224

2 256

3 384

4 512

5 Exit

Option (1 - 5): 4

== Data Length Menu ==

1 0

2 5

3 30

4 1600

5 1605

6 1630

7 Exit

Option (1 - 7): 6

CF 9A 30 AC 1F 1F 6A C0 91 6F 9F EF 19 19 C5 95
DE BE 2E E8 0C 85 42 12 10 FD F0 5F 1C 6A F7 3A
A9 CA C8 81 D0 F9 1D B6 D0 34 A2 BB AD C1 CF 7F
BC B2 EC FA 9D 19 1D 3A 50 16 FB 3F AD 87 09 C9

== SHA-3 Test Menu ==

1 224

2 256

3 384

4 512

5 Exit

Option (1 - 5): 5

== Menu ==

1 SHA-1 Tests

2 SHA-3 Tests

3 BBS and Maurer Tests

4 Exit

Option (1 - 4): *Warning*

Illegal option

== Menu ==

1 SHA-1 Tests
2 SHA-3 Tests
3 BBS and Maurer Tests
4 Exit
Option (1 - 4): 4

C:\Users\James\OneDrive\GuideToECC\x64\Release\GuideToECC.exe (process 39040)
exited with code 0 (0x0).
Press any key to close this window . . .