MD5 Implementation Using Excel

Sang Bae Park*
*KISTI, Korea
E-mail : plucky@kisti.re.kr

1. Introduction

Hash Function is a very important cryptographic primitive for information security. [3] MD5 is the most famous hash function invented by L. Rivest in 1992. [1] There were many researches for security of hash functions. After Wang et al. found collisions for MD4, MD5, RIPEMD etc., the interest in hash function is increasing rapidly. [2] However hash function is hard to understand for its unfamiliar operations. In this paper, we present our implementation using familiar OA software Excel. With this, we can watch intermediate values of MD5 step by step. Moreover we can verify the Wang's collision just by a copy and paste.

2. Our Implementation

MD5 consists of 4 round functions and each round function has 16 steps. The following figure shows the structure of MD5. Nonlinear function in each step is composition of bitwise-or, and, xor operations.

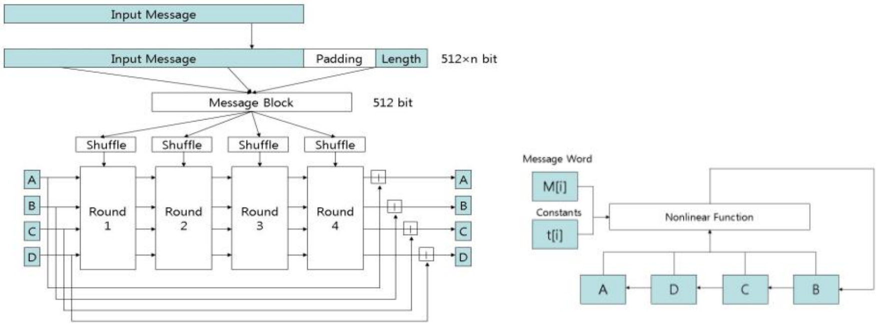


Figure 1. MD5 Structure

Although Excel provides many useful functions, there are some limitations in Excel. To implement MD5, we consider the followings.

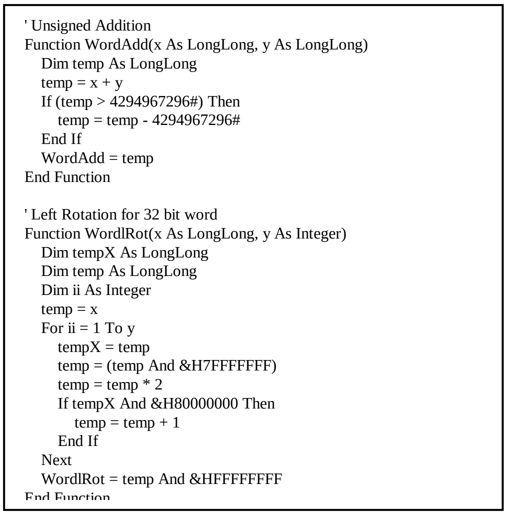
- There is no bitwise rotation operation.
- There is no unsigned integer operation.
- There is no hexadecimal operation.

For first and second, we implement these functions using VBA in Excel. Figure 2 shows our implementation of these functions. For hexadecimal presentation, we make two sheets. One is a hexadecimal representation sheet for user's view and message input. The other is a decimal representation sheet for real operations. Two sheets are connected by Excel functions @DEC2HEX() and @HEX2DEC().

The MD5 operations are implanted as followings.

- Input the hexadecimal message into sheet one.
- Using @HEX2DEC, translate the message to decimal number in sheet two.
- In sheet two, calculate each step.
- Using @DEC2HEX, translate the values to hexadecimal number into sheet one.

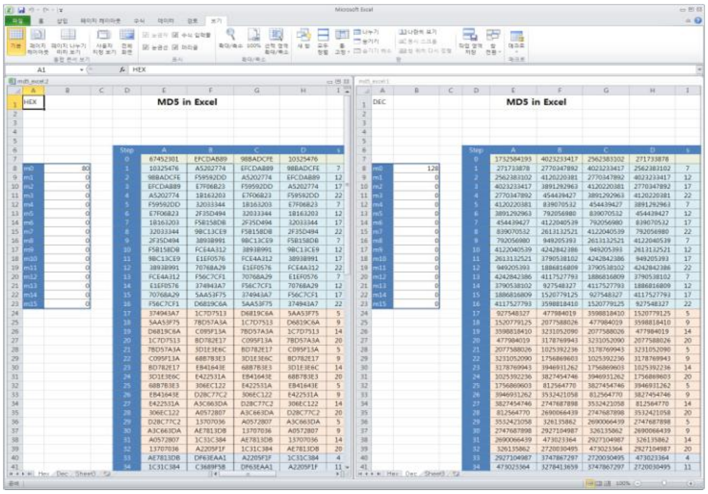
Figure 3 shows our implementation of MD5 in Excel. At this time, we consider one message block. But it can expand just by a copy-and-paste.



```
' Unsigned Addition
Function WordAdd(x As LongLong, y As LongLong)
    Dim temp As LongLong
    temp = x + y
    If (temp > 4294967296#) Then
        temp = temp - 4294967296#
    End If
    WordAdd = temp
End Function

' Left Rotation for 32 bit word
Function WordlRot(x As LongLong, y As Integer)
    Dim tempX As LongLong
    Dim temp As LongLong
    Dim ii As Integer
    temp = x
    For ii = 1 To y
        tempX = temp
        temp = (temp And &H7FFFFFFF)
        temp = temp * 2
        If tempX And &H80000000 Then
            temp = temp + 1
        End If
    Next
    WordlRot = temp And &HFFFFFFFF
End Function
```

Figure 2. Bit operation function using VBA



HEX

MD5 in Excel

m0	80
m1	0
m2	0
m3	0
m4	0
m5	0
m6	0
m7	0
m8	0
m9	0
m10	0
m11	0
m12	0
m13	0
m14	0
m15	0

Step	A	B	C	D	s
0	67452301	EFCDAB89	98BADCFE	10325476	
1	10325476	A5202774	EFCDAB89	98BADCFE	7
2	98BADCFE	F59592DD	A5202774	EFCDAB89	12
3	EFCDAB89	E7F06B23	F59592DD	A5202774	17
4	A5202774	1B163203	E7F06B23	F59592DD	22
5	F59592DD	32033344	1B163203	E7F06B23	7
6	E7F06B23	2F35D494	32033344	1B163203	12
7	1B163203	F5B158DB	2F35D494	32033344	17
8	32033344	9BC13CE9	F5B158DB	2F35D494	22
9	2F35D494	3893B991	9BC13CE9	F5B158DB	7
10	F5B158DB	FCE4A312	3893B991	9BC13CE9	12
11	9BC13CE9	E1EF0576	FCE4A312	3893B991	17
12	3893B991	70768A29	E1EF0576	FCE4A312	22
13	FCE4A312	F56C7CF1	70768A29	E1EF0576	7
14	E1EF0576	374943A7	F56C7CF1	70768A29	12
15	70768A29	5AA53F75	374943A7	F56C7CF1	17
16	F56C7CF1	D6819C6A	5AA53F75	374943A7	22
17	374943A7	1C7D7513	D6819C6A	5AA53F75	5
18	5AA53F75	7BD57A3A	1C7D7513	D6819C6A	9
19	D6819C6A	C095F13A	7BD57A3A	1C7D7513	14
20	1C7D7513	BD782E17	C095F13A	7BD57A3A	20
21	7BD57A3A	3D1E3E6C	BD782E17	C095F13A	5
22	C095F13A	68B7B3E3	3D1E3E6C	BD782E17	9
23	BD782E17	EB41643E	68B7B3E3	3D1E3E6C	14
24	3D1E3E6C	E422531A	EB41643E	68B7B3E3	20
25	68B7B3E3	306EC122	E422531A	EB41643E	5
26	EB41643E	D28C77C2	306EC122	E422531A	9
27	E422531A	A3C663DA	D28C77C2	306EC122	14
28	306EC122	A0572807	A3C663DA	D28C77C2	20
29	D28C77C2	13707036	A0572807	A3C663DA	5
30	A3C663DA	AE7813DB	13707036	A0572807	9
31	A0572807	1C31C384	AE7813DB	13707036	14
32	13707036	A2205F1F	1C31C384	AE7813DB	20
33	AE7813DB	DF63EAA1	A2205F1F	1C31C384	4
34	1C31C384	C3689F58	DF63EAA1	A2205F1F	11

DEC

MD5 in Excel

m0	128
m1	0
m2	0
m3	0
m4	0
m5	0
m6	0
m7	0
m8	0
m9	0
m10	0
m11	0
m12	0
m13	0
m14	0
m15	0

Step	A	B	C	D	s
0	1732584193	4023233417	2562383102	271733878	
1	271733878	2770347892	4023233417	2562383102	7
2	2562383102	4120220381	2770347892	4023233417	12
3	4023233417	3891292963	4120220381	2770347892	17
4	2770347892	454439427	3891292963	4120220381	22
5	4120220381	839070532	454439427	3891292963	7
6	3891292963	792056980	839070532	454439427	12
7	454439427	4122040539	792056980	839070532	17
8	839070532	2613132521	4122040539	792056980	22
9	792056980	949205393	2613132521	4122040539	7
10	4122040539	4242842386	949205393	2613132521	12
11	2613132521	3790538102	4242842386	949205393	17
12	949205393	1886816809	3790538102	4242842386	22
13	4242842386	4117527793	1886816809	3790538102	7
14	3790538102	927548327	4117527793	1886816809	12
15	1886816809	1520779125	927548327	4117527793	17
16	4117527793	3598818410	1520779125	927548327	22
17	927548327	477984019	3598818410	1520779125	5
18	1520779125	2077588026	477984019	3598818410	9
19	3598818410	3231052090	2077588026	477984019	14
20	477984019	3178769943	3231052090	2077588026	20
21	2077588026	1025392236	3178769943	3231052090	5
22	3231052090	1756869603	1025392236	3178769943	9
23	3178769943	3946931262	1756869603	1025392236	14
24	1025392236	3827454746	3946931262	1756869603	20
25	1756869603	812564770	3827454746	3946931262	5
26	3946931262	3532421058	812564770	3827454746	9
27	3827454746	2747687898	3532421058	812564770	14
28	812564770	2690066439	2747687898	3532421058	20
29	3532421058	326135862	2690066439	2747687898	5
30	2747687898	2927104987	326135862	2690066439	9
31	2690066439	473023364	2927104987	326135862	14
32	326135862	2720030495	473023364	2927104987	20
33	2927104987	3747867297	2720030495	473023364	4
34	473023364	3278413659	3747867297	2720030495	11

Figure 3. MD5 in Excel

3. Conclusions

In this paper, we present our MD5 implementation in the spreadsheet Excel. With this, we can investigate internal state of MD5. This may be helpful for understanding MD5. We expect that this can be applied in cryptography class.

4. References

[1] R. Rivest, “The MD5 message-digest algorithm”, Request for Comments (RFC) 1321, Internet Activities Board, Internet Privacy Task Force, 1992.
[2] X. Wang and H. Yu, “How to Break MD5 and Other Hash Functions”, In Advances in Cryptology EUROCRYPT 2005, Springer-Verlag, 2005.
[3] A. Menezes, P. van Oorschot and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.