

CypherMatrix

Hash Function

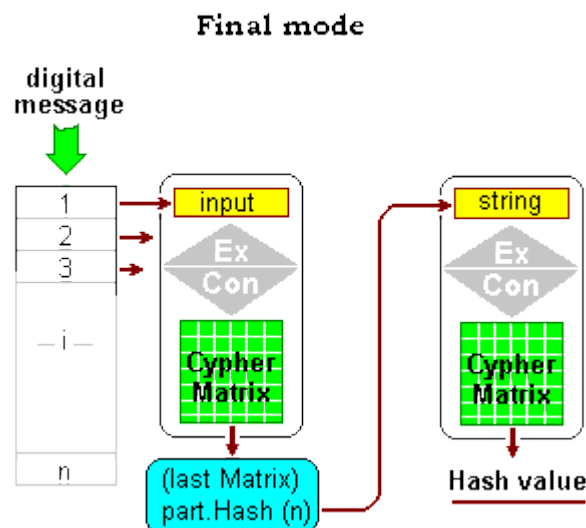
Task of a hash function is the clear marking of digital informations as constant characteristic:

Texts (messages), drawings, digital images, digital sound, programs, readings and other digitally stored informations

In the progress of researching digital facts many hash functions have been developed, which fulfill their task also more or less well. As problem remains however that the procedures must be also safe enough (clearly and indisputable). The so far used procedures of the SHA family are lately endangered by special attacks. NIST [#1] therefore accomplishes at present an international competition, in which at the end the best suitable procedure is to be elect.

Those candidates already became known [#2] are essentially arranged according to a pattern, which corresponds to the structure of previous hash functions to a large extent. In order to compare with the [CypherMatrix Hash Function](#) a confrontation of the two ranges is to be made in the following.

CypherMatrix final mode demonstrates as follows:



The fundamental difference shows up already in the basic elements: Both the current procedures and the candidates in the NIST competition use „**bits**“ as the smallest working unit while on the other hand CypherMatrix processes only „**bytes**“ (**8 bits**) as numbers (number systems of basis 2 up to basis 256). Accordingly CypherMatrix is strictly speaking a pure mathematical procedure

Hash Functions (general)	CypherMatrix Hash Function
Fundamental Elements	
bits	bytes
Additional Functions	
IVs, SALT, padding	none
Working Steps, Sequences (message digest)	
224, 256, 384, 512, 1024 bits (in part: variable)	continuous, unlimited (optimal: 16 up to 256 bytes)
Internal Consistence (internal states)	
Feistel network keys, S-boxes, constants, shifting, rotation, mixing, XOR swapping, permutations	position weighted hash constant C expansion, contraction (one way functions)
Compression Function	
„Merkle-Damgård“ block ciphers, AES-based Threefish based	none
Output Function	
output function truncated to output fixed length	CypherMatrix: $GF(16^2)$ threefold permutation number system to basis 62 (9 up to 11 digits)
Applications (Anwendungen)	
hashing, MAC, randomizing, PRNG, digital signatures, authentication, encryptions	hash funktion, randomizing digital signatures, RNG, authentication, encryptions

Working Steps

The data process in the CypherMatrix hash function is represented by example of the upper written text - „*Task of a hash function procedure is to be elect*“ - (EXAMPLE.TXT: 678 bytes) with differently long hash sequences:

A. Hash sequence = 47 bytes

Parameter: Length hash sequence [16 – 256]: **47**
 Number base output [36 – 82]: **62**
 Expansion factor [35 – 255]: **77**
 User code number [1 – 99]: **1**

Program **CMHash.exe** calculates the following results:

Serial matrix values in Example.txt

```
-----  
991845778630    HSdvo6Y    1  
1013660779962   HqSHKUK   2  
904088450981    Fuqt0I1   3  
956918429259    GqWCCzr   4  
940795426793    GYv3jWz   5  
1089822002787   JBaY3iV   6  
921326958436    GDfW1Yq   7  
896349770914    FmPAI5a   8  
876983715916    FRGYIVo   9  
938428920134    GWKu72k   10  
958788557142    GsYl4go   11  
910641135388    G20LOqC   12  
1125198483626   JoCgAR8   13  
1010755609339   HnHfWu3   14  
13410665877    EdZmoX    15  
-----
```

decimal: 13549014685184

base 16: C52A0351600

base 62: **3qXM4q2K**

Matrix value last cycle:

decimal: 9213511724747775

base 16: 20BBA3DD7CCBFF

base 62: **gCH2WOJMV**

Final **Hash value** for: EXAMPLE.TXT
decimal: 9227060739432959
base 16: 20C7F67DB1E1FF
base 62: **gG7ZsT9Op**

B. Hash sequence = 64 bytes

Parameter: Length hash sequence [16 – 256]: **64**
 Number base output [36 – 82]: **62**
 Expansion factor [35 – 255]: **77**
 User code number [1 – 99]: **1**

Program **CMHash.exe** calculates the following results:

Serial matrix values in Example.txt

4854912696362 1NTLyuPi 1
4269889502604 1DAm5Cvs 2
4257170390550 1CwtJ6rG 3
4712021369355 1KxNhSI1 4
4417819555429 1FmFMdLp 5
4615625971041 1JGA4CA5 6
4772896576632 1M1pTd2u 7
4203270673536 1C03bOEq 8
4506067870418 1HKZdZP0 9
4624587735796 1JPwYqYu 10
319809166868 5d5Kfgq 11

decimal: 45554071508591
base 16: 296E6240166F
base 62: **Cw0J7dQF**

Matrix value last cycle:
decimal: 9112341992901352
base 16: 205FA0738F0AE8
base 62: **fjXtEJgjo**

Final **Hash value** for: EXAMPLE.TXT
decimal: 9157896064409943
base 16: 20890ED5CF2157
base 62: **fwTtXRKA3**

C. Hash sequence = 128 bytes

Parameter: Length hash sequence [16 – 256]: **128**
Number base output [36 – 82]: **62**
Expansion factor [35 – 255]: **77**
User code number [1 – 99]: **1**

Program **CMHash.exe** calculates the following results:

Serial matrix values in example.txt

143987454817133 esykgec9 1
143797357593960 epdFi4vQ 2
148576355801679 gBlk7Wwx 3
140857142452926 dzrsMz42 4
147930893374184 g0PBwxoW 5
319808965130 5d5JpD0 6

decimal: 725469013005012
base 16: 293CF6AD0D2D4
base 62: **3K0HuA2a4**

Matrix value last cycle:
decimal: 9032737411244895
base 16: 20173A10BF235F
base 62: **fMwPGVYh5**

Final **Hash value** for: EXAMPLE.TXT
decimal: 9758206424249907
base 16: 22AB097B8FF633
base 62: **igwhAfbH9**
=====

D. Hash sequence = 256 bytes

Parameter: Length hash sequence [16 – 256]: **256**
Number base output [36 – 82]: **62**
Expansion factor [35 – 255]: **77**
User code number [1 – 99]: **1**

Program **CMHash.exe** calculates the following results:

Serial matrix values in example.txt

4.70881494977202E+15 LZ7KK62TQ 1
4.6329853015266E+15 LDalrpnZI 2
538261232573656 2SqOEPgs4 3

decimal: 9880061483872280
base 16: 2319DD131AF018
base 62: **jFY1QLWum**

Matrix value last cycle:
decimal: 9379080750402621
base 16: 21523968728C3D
base 62: **gxHyWcp9p**

Final **Hash value** for: EXAMPLE.TXT
decimal: 19259142234274901
base 16: 446C167B8D7C55
base 62: **1QCpzwym4b**
=====

Explanations

The output function of the CypherMatrix procedure represents the calculated hash function values in figures of the number system to **basis 62**.

The number system to basis 62 comprises the following digits:

0123456789ABCDEFGHIJKLMNPOQRSTUVWXYZ

abcdefghijklmnopqrstuvwxy

(determined by the Author, not standardized)

In addition, the calculated hash values can be implemented in all number systems by to basis 2 up to basis 256. With the values all mathematical operations can be executed (addition, subtraction, multiplication, division, MODULO calculation and others).

You may test the upper examples by yourself with the program

CMHash.exe

The program is available as download under

Telecypher.net/DELIVERY.HTM

Notes:

[#1] NIST: National Institute of Standards and Technology, USA

[#2] Grøstl, LANE, SHAvite-3, Skein, TIB3, ...

see: [//e-hash.iak.tugraz.at/wiki/The_SHA-3_Zoo](http://e-hash.iak.tugraz.at/wiki/The_SHA-3_Zoo)

Munich, 12th of January 2009

© Ernst Erich Schnoor
