|  |  |  |
| --- | --- | --- |
| Name | Length | Hash |
| Md2 | 16 | 0DF1C64F7E9BB8846F8A1F5418A8EFC3 |
| Md4 | 16 | AE0D7ED27F9EF9F815680D2B72A7FA4A |
| Md5 | 16 | B6D1253010EDC806940C8F6EF3D030BC |
| Sha1 | 20 | E5DA57735E7B24A3F9C1DDD6CEAF25EE4C77B823 |
| Ripemd160 | 20 | D6CD75A476AFE72390D95D8B7E07417749AF678D |
| Sha256 | 32 | 6DCCE7B58ABA7DD27FE65899E6CE09209DA7FC5BC6C21F52E0CF04503EC2BC11 |
| Whirlpool | 64 | 410431D5F7553D280A3017095B1FE9AD1D78A7F2C0398EB0DAADE61D5A891A330DD2173B477670EE1B1484F7ADFB8985B76B6B6A4293D5693AED6F19CB0719C1 |

Discussion:  
Is it possible to generate the original text from Hash Value? Why?

It isn’t possible because hashing is a one-way function.

What is the significance of the length recorded in the table?

A longer hash length provides a higher level of encryption due to increasing possible combinations.

Is there any direct impact of digest length on the level of security of a Hash algorithm?

As stated in the previous answer a longer hash means more possible combinations for the hash meaning a higher level of security.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Plaintext  Alphabet | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| Cipher  Alphabet | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |

**4 Shift Caesar Cipher ^**

Hello encryption 3 shift = Khoor

FUBSWR decryption 3 shift = Crypto

Transposition Cipher:  
1. Encrypt the following sentence with Keywords: RMIT

We are going to cinema after the meeting tonight.

Ai evi ksmrk xs gmriqe ejxiv xli qiixmrk xsrmklx.

2. Decrypt the following cipher text using keyword: STOCK.

MNBONTXTEGESEITHEISPONENTEHETDLMHTANPUNO

3. Decrypt Encrypted Message: " YRCIFNTN CEERYUAO BSUTODIS" Keyword: "KEY"

4 5 3 1 2 = STOCK

THE MEETING HAS BEEN POSTPONED UNTIL NEXT MONTH

KEY = 2 1 3

CYBER SECURITY FOUNDATIONS