



VIT[®]

Vellore Institute of Technology

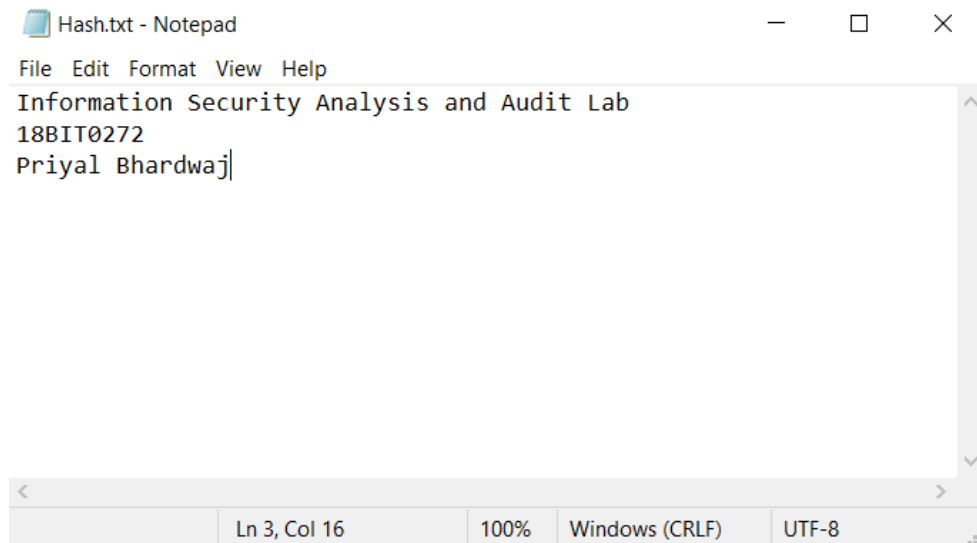
(Deemed to be University under section 3 of UGC Act, 1956)

School of Information Technology and Engineering
Lab Assessment-IV, AUGUST 2020
B.Tech., Fall-2020-2021

NAME	PRIYAL BHARDWAJ
REG. NO.	18BIT0272
COURSE CODE	CSE3501
COURSE NAME	INFORMATION SECURITY ANALYSIS & AUDIT
SLOT	L19+L20
FACULTY	Prof. THANDEESWARAN R.

Calculate Hash, Checksum, or HMAC to ensure the data Integrity of a file, before and after modification, using the HashCalc Tool.

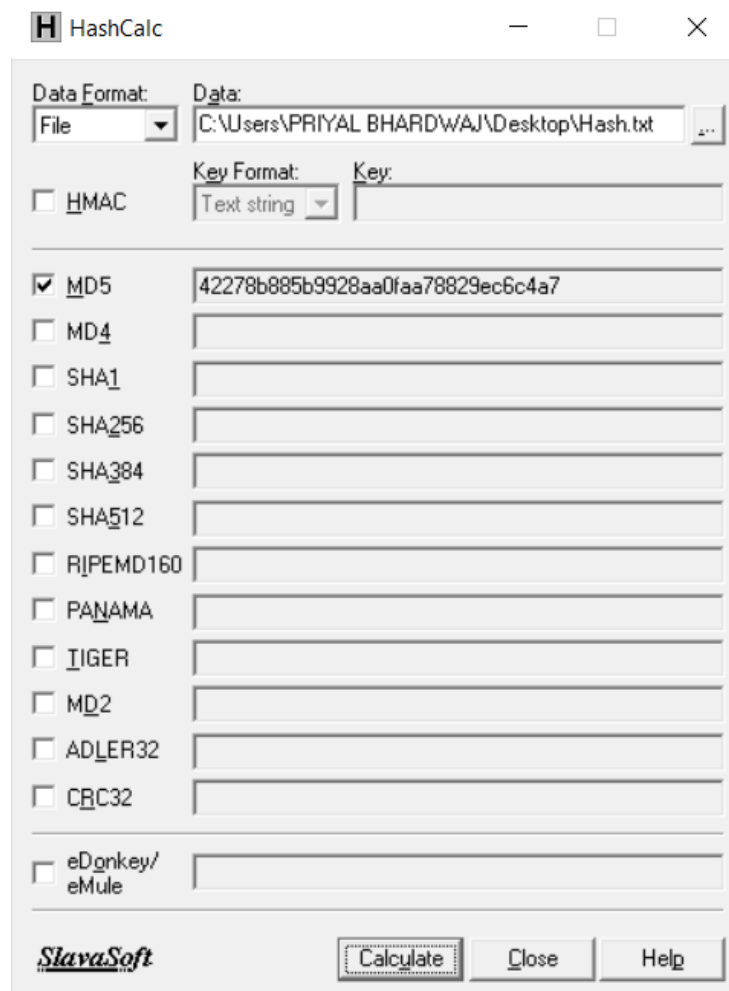
Step 1: Create a Text file



Step 2: Install HashCalc

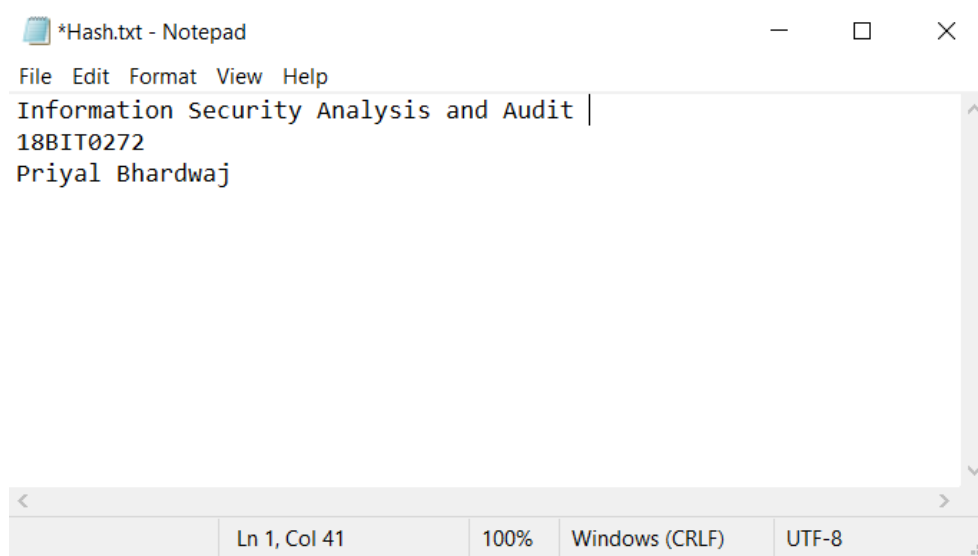
Step 3: Calculate a hash of the Hash.txt file

MD5 Value: 42278b885b9928aa0faa78829ec6c4a7



Step 4: Make a change to the Hash.txt file

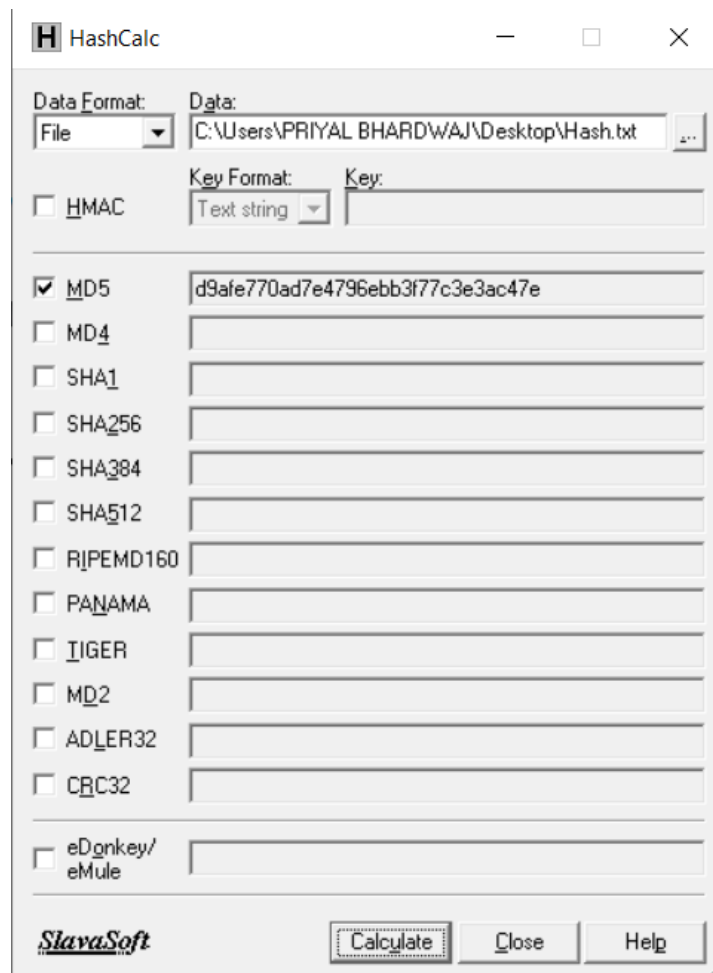
Deleted "Lab" from the text.



Step 5: Calculate a new hash of the Hash.txt file

a. New MD5 Value: d9afe770ad7e4796ebb3f77c3e3ac47e

Yes, MD5 value in Step 3 and Step 5 is different because file content has changed because content of Hash.txt has changed now.



Calculating all hash types

d. Many of the hash types create a hash of a different length because they have different algorithms for calculating the hash function. For example, MD5 generates 128 bit and SHA256 generates 256 bits.

It depends on key size as well but here we have unchecked HMAC so we do not need to provide key.

Before tampering data in Hash.txt:

HashCalc application window showing the following configuration and results:

- Data Format: File
- Data: C:\Users\PRIYAL BHARDWAJ\Desktop\Hash.txt
- HMAC: ☐ (unchecked)
- Key Format: Text string
- Key: (empty)

Algorithm	Hash Value
<input checked="" type="checkbox"/> MD5	42278b885b9928aa0faa78829ec6c4a7
<input checked="" type="checkbox"/> MD4	58f94d600d289bca336641cb92d1127b
<input checked="" type="checkbox"/> SHA1	ac619ab69b78d11fa57de2fe697c9c9a7b6f9c65
<input checked="" type="checkbox"/> SHA256	1ba8c7ff90996ee24ff43d3900fa3173d558bf317def14c3266876da39e5a4c9
<input checked="" type="checkbox"/> SHA384	b380d2a869d34c533ec2ebfcd53aef648d045f3991b882e09df5eb5328c65d615aeeba4dd1e4beb4f0c987e8c440ac2d
<input checked="" type="checkbox"/> SHA512	277080344ad2356a55c5529e9704530d0cc03cabee6bbe10fc0b15e8a43fa41fc00df0f05eeb456ca6a4f04fb8d4c9e219dd02874087935fc170c98eb6185d9
<input checked="" type="checkbox"/> RIPEMD160	d97af8db799a3ebf4019e9ccb9cf30bd1560d4ca
<input checked="" type="checkbox"/> PANAMA	9018880f5aa3559dbbc38ab778370fdbcee1aa61baf507fb180c8e10424edf9b
<input checked="" type="checkbox"/> TIGER	b841d0b78d4a80748205cfe44367c33dde585f966fe9128
<input checked="" type="checkbox"/> MD2	59246e40ae66a0fdee1832ca7100583d
<input checked="" type="checkbox"/> ADLER32	88ef17f1
<input checked="" type="checkbox"/> CRC32	6df6e0ac
<input checked="" type="checkbox"/> eDonkey/ eMule	58f94d600d289bca336641cb92d1127b

Buttons: Calculate, Close, Help

After tampering with the data in Hash.txt file:

HashCalc application window showing the following configuration and results:

- Data Format: File
- Data: C:\Users\PRIYAL BHARDWAJ\Desktop\Hash.txt
- HMAC: ☐ (unchecked)
- Key Format: Text string
- Key: (empty)

Algorithm	Hash Value
<input checked="" type="checkbox"/> MD5	d9afe770ad7e4796ebb3f77c3e3ac47e
<input checked="" type="checkbox"/> MD4	495cf550d809bc4762d26505f04a2774
<input checked="" type="checkbox"/> SHA1	4a310e8dc84f82e3aa45a76cde0303f4e62d2ef9
<input checked="" type="checkbox"/> SHA256	84edb8e0631ebc6eb14639844d5eea97f4c4658fe9dcc45cc1420adb46637102
<input checked="" type="checkbox"/> SHA384	23847b18a2366e63bf4f02217a0b22ad221c343908dbda07ba14952f980af968e08cba9fbafdf5f3487c0c16cbf9ca236
<input checked="" type="checkbox"/> SHA512	8950a7438e92da3c609b34fe53c9ea3bb7682cef3990ac8430776c25cddfaf2662bcf5e4c9c4a399322fd4e66aef81e8626c0b7f49871326661878b83226ae84
<input checked="" type="checkbox"/> RIPEMD160	694e801eb858bedc67f17e9b4e0facdc6e9348de
<input checked="" type="checkbox"/> PANAMA	5863829f7454a38f4e161175cf6ca09ad5ec1e3df406dcba0b019f1c43d43c
<input checked="" type="checkbox"/> TIGER	0d79cb615bbf9bec9c1d6fcc3b28fb87f98c566b25063fac
<input checked="" type="checkbox"/> MD2	104f6a675ea29f26de52b5f93fe12c4a
<input checked="" type="checkbox"/> ADLER32	3c7c16e2
<input checked="" type="checkbox"/> CRC32	4be6a96a
<input type="checkbox"/> eDonkey/ eMule	

Buttons: Calculate, Close, Help

Now we have enabled **HMAC** and provided random text “isaa” as key and calculated hash values again. We can see the hash values are different from the ones obtained in above step without key.

Before tampering data in Hash.txt:

HashCalc application window showing calculated hashes for various algorithms. The Data Format is set to File, and the Data is C:\Users\PRIYAL BHARDWAJ\Desktop\Hash.txt. The Key Format is Text string, and the Key is isaa. The calculated hashes are as follows:

Algorithm	Hash Value
MD5	e90a4d1c2d2cf02f1f6f1a0aac96a8f6
MD4	3fb8fd3739d8e2f6261444f316d8cf62
SHA1	9b58e8a59621e9940929b379652fdd68e4616c40
SHA256	e3a36e5348aefe0247b462a8694d1a91f864f87bea0075c52781d7a04a8d392d
SHA384	36cb186a1237de994e5a510b292aacb620c4183e336a48e65aee73faca07cbe5f703a2dc2f69b3e8bfe3f594bec50627
SHA512	436663a598312df7509042835e3c51afebdca1a7d66cd0f6eaa0b9663b89eedeff0d5d2a4b9380f0c7a0705f1692e31c676b1d921975701d0c3ccaf15f70b5b
RIPMD160	2e6d5aa9d29357569a01723da6953d5594eba906
PANAMA	bf0e41dda131d35eeb736c6c7dde6936d00adc5cce1196aa6a61e6c6014fed7c
TIGER	ce1dca44410d4fda859290699e47ac2dada62c16a5b113e0

After tampering with data in Hash.txt:

HashCalc application window showing calculated hashes for various algorithms after tampering the data. The Data Format is set to File, and the Data is C:\Users\PRIYAL BHARDWAJ\Desktop\Hash.txt. The Key Format is Text string, and the Key is isaa. The calculated hashes are as follows:

Algorithm	Hash Value
MD5	783ac340fc382cafb60ac9279e697a27
MD4	3b373bde7ddd4d41ca29b9612dcf9d9a
SHA1	7476b5d857671de92e12b48185a4ffb1b0f5d86d
SHA256	392724be126c45ff308595320ff6e8601157e37019d7267c48c770f32bd93eb5
SHA384	c308a929572c2e2fce5bb8c2600a0a3d7168e4f697a486b17ceb7d49ba3def7e293d5199aefff02fb1e347ac814b7041
SHA512	88190c6b20f06444abe8018a1d02489e3610ccee7bfa74089bd749d25e28601b5a373e662a01cb50ad7dc178a5e9e2c3ec6981e1245dcc3dd8999eb88e857fff
RIPMD160	7a9b613b2788facc72158367873b9d1b1bcfccd7
PANAMA	2b11b74ead452009b57ccf09370de3e8e03c4f9d2c42d74398b39434dde9eba6
TIGER	ed88cfaa1ef7090b65456fad7d50af8b3e8decf393c97c41
