A STUDY IN ENCRYPTION

HASH FUNCTIONS

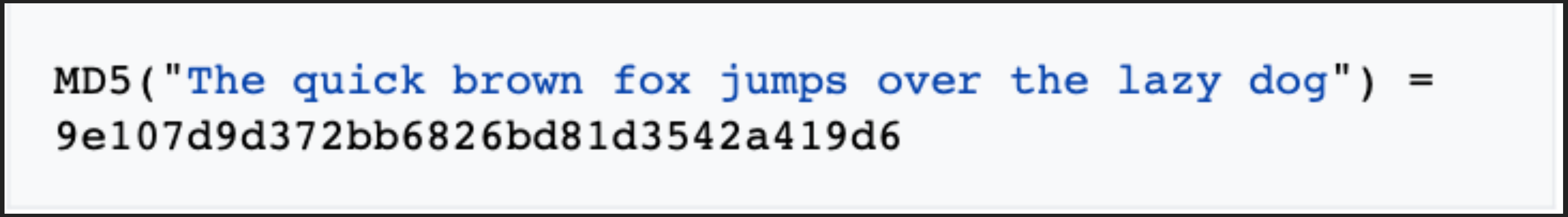
INDEX

TYPES COVERED IN THIS PRESENTATION:

- Message Digest Algorithm 5 (MDA5)
- Secure Hash Algorithm 1 (SHA1)
- Secure Hash Algorithm 256 (SHA256)
- Secure Hash Algorithm 512 (SHA512)
- LAN Manager Hash (LM)

MESSAGE DIGEST ALGORITHM 5

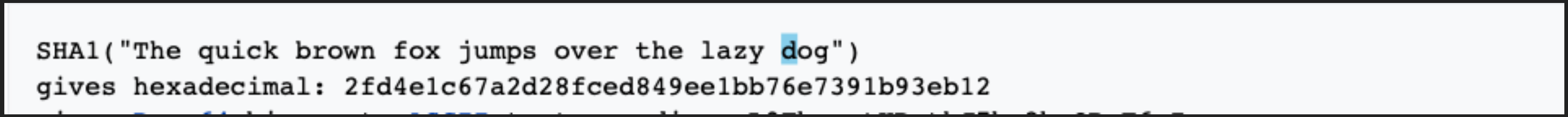
- 128-bits (16 bytes) represented as 32 hexadecimal digits.
- Originally designed as a Cryptographic Hash function by Ronald Rivest in 1991.
- Suffers from extensive vulnerabilities
- As of 2019, MD5 continues to be widely used despite its well documented weaknesses by security experts
- Eg:



```
MD5("The quick brown fox jumps over the lazy dog") =
9e107d9d372bb6826bd81d3542a419d6
```

SECURE HASH ALGORITHM 1

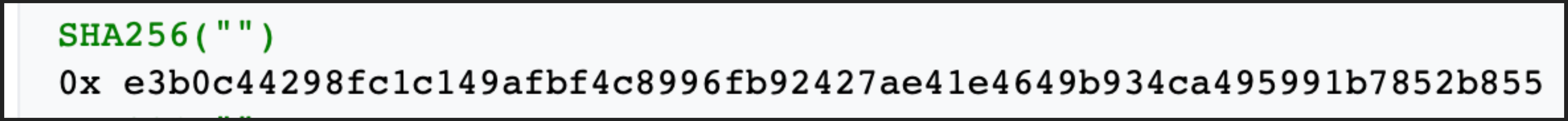
- 160 bits (20 bytes) represented as 40 hexadecimal digits.
- Developed by National Security Agency, USA.
- Has not been secure since 2005 against well funded opponents.
- Major vendors ceased use in 2017 when CWI Amsterdam and Google recorded same hash code for different PDFs.
- Eg:



```
SHA1("The quick brown fox jumps over the lazy dog")
gives hexadecimal: 2fd4e1c67a2d28fced849ee1bb76e7391b93eb12
```

SECURE HASH ALGORITHM 256

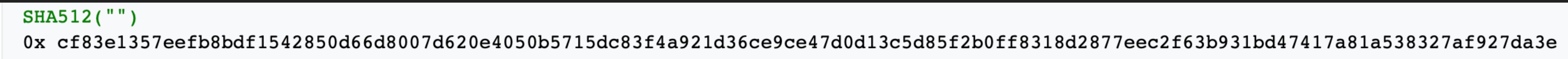
- 256 bits (32 bytes) represented as 64 hexadecimal digits.
- Developed by National Institute of Standards & Technology, USA.
- Part of SHA-2 family
- Used in protocols like TLS, SSL, PGP, SSH, IPsec, etc.
- Eg:



```
SHA256("")
0x e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
```

SECURE HASH ALGORITHM 512

- 512 bits (64 bytes) represented as 128 hexadecimal digits.
- Developed by National Institute of Standards & Technology, USA
- Part of the SHA-2 family
- Used in protocols like TLS, SSL, PGP, SSH, IPsec, etc.
- Eg:



```
SHA512("")
0x cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36ce9ce47d0d13c5d85f2b0ff8318d2877eec2f63b931bd47417a81a538327af927da3e
```

COMPARISON

SHA 256

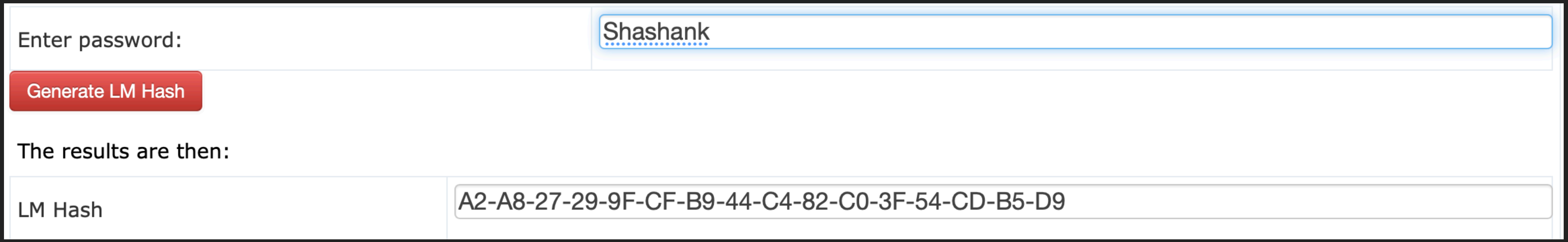
- 64 hexadecimal digits
- Requires less bandwidth to store and transmit
- Less processing power to compute
- No collision resistance in Quantum Computing
- Slightly less secure

SHA 512

- 128 hexadecimal digits
- Significant resources and bandwidth
- Comparatively more processing power
- Collision resistance offered for Quantum Computing
- Slightly more secure

LAN MANAGER HASH

- Max. Length is 14 bytes divided into half of 7 bytes each.
- Developed by Microsoft
- Hash value sent to Networks without salting, making it susceptible to Man in the Middle Attacks and allowing construction of Rainbow Tables.
- Still used as considerable time taken to add support for stronger protocols, poor patching and dependancy of WinVista.
- Eg:



Enter password:	Shashank

The results are then:

LM Hash	A2-A8-27-29-9F-CF-B9-44-C4-82-C0-3F-54-CD-B5-D9

BY ANSH CHANDNANI