

Lab 3: Cryptographic Hashes

Team: Cyber Chargers

Chandrakanth Bogra(cbogra1s@semo.edu)

Baji Babu Kollipara(bkollipara1s@semo.edu)

Vamsi Javvaji(vjavvaji1s@semo.edu)

Cryptographic Hash:

A cryptographic hash function is an algorithm that takes an arbitrary amount of data input and produces a fixed-size output of enciphered text called a hash value, or just “hash.” That enciphered text can then be stored instead of the password itself, and later used to verify the user.

Cleartext passwords are converted to enciphered text for storage using cryptographic hashes. If an attacker tries to hack your database, they'll have to decode those hash values. Hashes, in other words, slow down attackers.

Hashing is a mathematical operation that is easy to perform, but extremely difficult to reverse. (The difference between hashing and encryption is that encryption can be reversed, or decrypted, using a specific key.) The most widely used hashing functions are MD5, SHA1 and SHA-256. Some hashing processes are significantly harder to crack than others.

MD5, MD4, SHA1, SHA256, SHA384, SHA512, RIPEMD160, CRC32 are some of the commonly and widely used Hash functions.

Properties of a Strong Hash Algorithm:

1). Determinism: A hash algorithm should be deterministic, which means it should always produce an output of the same size regardless of the size of the input.

2). Collision Resistance: The risk is that someone might build a malicious file with an artificial hash value that matches a genuine (safe) file and pass it off as the genuine article because the signatures match. As a result, a successful and reliable hashing algorithm is one that avoids collisions.

3). Hash Speed: Hash algorithms should operate at a reasonable speed. In many situations, hashing algorithms should compute hash values quickly; this is considered an ideal property of a cryptographic hash function.

Functions of Hash Function:

One purpose of a hash function in cryptography is to take a plaintext input and generate a hashed value output of a specific size in a way that can't be reversed.

- Ensures data integrity,
- Secures against unauthorized modifications,
- Protects stored passwords, and
- Operates at different speeds to suit different purposes.

The following are the few of the important Hash Algorithm:

MD5: The MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value.

MD4: The digest length is 128 bits. The algorithm has influenced later designs, such as the MD5, SHA-1 and RIPEMD algorithms. The initialism "MD" stands for "Message Digest."

SHA1: In cryptography, SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest.

SHA256: SHA-256 is one of the successor hash functions to SHA-1 and is one of the strongest hash functions available. It is a 256 bits hash function.

SHA384: SHA384 (Secure Hash Algorithm) is a cryptographic hash function designed by the National Security Agency (NSA). SHA384 produces a 384-bit (48-byte) hash value.

SHA512: SHA512 (Secure Hash Algorithm) is a cryptographic hash function designed by the National Security Agency (NSA). SHA512 produces a 512-bit (64-byte) hash value, typically rendered as a hexadecimal number, 128 digits long.

RIPEMD160: RIPEMD160 (RACE Integrity Primitives Evaluation Message Digest) is a family of cryptographic hash functions developed in Leuven, Belgium. RIPEMD160 produces a 160-bit (20-byte) hash value.

CRC32: A very commonly used hash function is CRC32 (that's a 32-bit cyclic redundancy code). There's a CRC32 "checksum" on every Internet packet; if the network flips a bit, the checksum will fail and the system will drop the packet.

Applications of Cryptographic Hash Functions:

A hash function in cryptography is used to map data integrity. Hashing protects data from leakage, compares the large chunks of data, and detects the data tampering.

Some of the uses of hashing include:

- Digital signatures,
- Biometrics,

- Password storage,
- SSL/TLS certificates,
- Code signing certificates,
- Document signing certificates, and
- Email signing certificates.

Lab Questions

1 List of contributions - which group member did what for the preparation of the assignment.

Name	Contribution
Vamsi Javvaji	1)Applied SHA1 algorithm to name, 2)Applied MD5, MD4, to given sample text. 3) hash function algorithm is used on the certificate of SEMO
Baji Babu Kollipara	1)Applied SHA512 algorithm to name, 2)Applied SHA1, SHA256, SHA384, to given sample text. 3) Compare algorithms in terms of security
Chandrakanth Bogra	1)Applied SHA512 algorithm to name, 2)Applied SHA512, RIPEMD160, CRC32 to given sample text. 3)Compare algorithms in terms of security

2 Create a hash with your full name (first last) as the input data and “security” as the key using MD5, SHA1, and SHA512. Capture a screenshot as proof of your work.

The team member name as input data and “Security” as the Key using different algorithms like MD5,SHA1, and SHA512 we have generated the hash.

1)Input: chandrakanth Bogra

Key: security

Algorithm: MD5

Hash: 6c77bab7b859d19f1c9324f1150b1ea9

2) Input: BajiBabu Kollipara

Key: security

Algorithm: SHA1

Hash: eb4f70b58be11e2c2e51b398e9da73dcaffb1402

3)Input: Vamsi Javvaji

Key: security

Algorithm:SHA512

Hash:

b5a2cbbbc979360e591a6f13c66c17c55fa9970246875bd7f3003b0c8ac9e7fcdcc88fb17e2f56a
ba3fb270948061c892f1a68352c571d4354e6ef6ce65ebfad1

Screenshots:

1)MD5:

Copy-paste the string here

chandrakanth Bogra

Secret Key

security

Select a message digest algorithm

MD5

COMPUTE HMAC



Computed HMAC:

6c77bab7b859d19f1c9324f1150b1ea9

2)SHA1:

Copy-paste the string here

BajiBabu Kollipara


Secret Key

security

Select a message digest algorithm


SHA1

COMPUTE HMAC

 **START NOW**

3 Easy Steps:

- 1) Click 'Start Now
- 2) Download on our website!
- 3) Get Wave Browser Now

 **Wave Browser**

Computed HMAC:

eb4f70b58be11e2c2e51b398e9da73dcaffb1402

3)SHA512:

Copy-paste the string here

vamsi Javvaji

Secret Key

security

Select a message digest algorithm

SHA512

COMPUTE HMAC


START NOW

3 Easy Steps:

1) Click 'Start Now'

2) Download on our website!

3) Get Wave Browser Now

 Wave Browser

Computed HMAC:

b5a2cbbbc979360e591a6f13c66c17c55fa9970246875bd7f3003b0c8ac9e7fcdcc88fb17e2f56aba3fb270948061c892f1a68352c571d4354e6ef6ce65ebfad1

3 Using the additional file (“sample_text.pdf”) provided this as the input, compute the following hashes: MD5, MD4, SHA1, SHA256, SHA384, SHA512, RIPEMD160, CRC32. Capture screenshot(s) as proof of your work.

1) **Key:** security
Algorithm: MD5
Hash: f1b33759d77543f151aa203a431ddbd3

2)**Key:** security
Algorithm: MD4
Hash: 9230e489ce3bb86d15d8332fd495222c

3)**Key:** security
Algorithm: SHA1

Hash: 8136a4fcac06c68b16ae1d8e6f986324ef40c9c7

4)Key: security

Algorithm: SHA256

Hash: d7395073c1af2ec1cb40a02d07c4ec3a2851a0a3a9729a95c28b5d9554c54ef6

5)Key: security

Algorithm: SHA384

Hash:0a21a7f1079acad8a2efab29a0549ac95f1f35dd9d4925e072565d6d67297e0ebcb
27368b16ab327f186866b51f936b9

6)Key: security

Algorithm: SHA512

Hash:caa674c4133df5e645be898a9188a0475ee8da0b567372d9d474b578136c702ebe
643122ef9763f60fe8e91e6f3ea3d0cecca2956a178558768ae5cb8f43c532

7)Key: security

Algorithm: RIPEMD160

Hash: aa48ff105208ea8c20d3641c821428a8fc53aa60

8)Key: security

Algorithm: CRC32

Hash: 6cb310f4

Screenshots:

1)MD5:

Copy-paste the string here

In this paper, we discuss an emerging field of study: adversarial machine learning—the study of effective machine learning techniques against an adversarial opponent. To see why this field is needed, is learning—the study of effective machine learning techniques against an adversarial opponent. To see why this field is needed, it is helpful to recall a common metaphor: security is sometimes thought of as a chess game between two players. For a player to win, it is not only necessary to have an effective strategy, one must also anticipate the opponent's response to that

Secret Key**Select a message digest algorithm****COMPUTE HMAC****Computed HMAC:**

f1b33759d77543f151aa203a431ddb3

2)MD4:

Copy-paste the string here

In this paper, we discuss an emerging field of study: adversarial machine learning—the study of effective machine learning techniques against an adversarial opponent. To see why this field is needed, is learning—the study of effective machine learning techniques against an adversarial opponent. To see why this field is needed, it is helpful to recall a common metaphor: security is sometimes thought of as a chess game between two players. For a player to win, it is not only necessary to have an effective strategy, one must also anticipate the opponent's response to that

Secret Key**Select a message digest algorithm****COMPUTE HMAC****Computed HMAC:**

9230e489ce3bb86d15d8332fd495222c

3)SHA1

Copy-paste the string here

In this paper, we discuss an emerging field of study: adversarial machine learning—the study of effective machine learning techniques against an adversarial opponent. To see why this field is needed, is learning—the study of effective machine learning techniques against an adversarial opponent. To see why this field is needed, it is helpful to recall a common metaphor: security is sometimes thought of as a chess game between two players. For a player to win, it is not only necessary to have an effective strategy, one must also anticipate the opponent's response to that

Secret Key

Select a message digest algorithm

SHA1

COMPUTE HMAC

Computed HMAC:

8136a4fcac06c68b16ae1d8e6f986324ef40c9c7

4)SHA256:

Copy-paste the string here

In this paper, we discuss an emerging field of study: adversarial machine learning—the study of effective machine learning techniques against an adversarial opponent. To see why this field is needed, is learning—the study of effective machine learning techniques against an adversarial opponent. To see why this field is needed, it is helpful to recall a common metaphor: security is sometimes thought of as a chess game between two players. For a player to win, it is not only necessary to have an effective strategy, one must also anticipate the opponent's response to that

Secret Key

Select a message digest algorithm

SHA256

COMPUTE HMAC

Computed HMAC:

d7395073c1af2ec1cb40a02d07c4ec3a2851a0a3a9729a95c28b5d9554c54ef6

5)SHA384

Copy-paste the string here

In this paper, we discuss an emerging field of study: adversarial machine learning—the study of effective machine learning techniques against an adversarial opponent. To see why this field is needed, is learning—the study of effective machine learning techniques against an adversarial opponent. To see why this field is needed, it is helpful to recall a common metaphor: security is sometimes thought of as a chess game between two players. For a player to win, it is not only necessary to have an effective strategy, one must also anticipate the opponent's response to that

Secret Key

Select a message digest algorithm

COMPUTE HMAC

Computed HMAC:

0a21a7f1079acad8a2efab29a0549ac95f1f35dd9d4925e072565d6d67297e0ebcb27368b16ab327f186866b51f936b9

6)SHA512:

Copy-paste the string here

In this paper, we discuss an emerging field of study: adversarial machine learning—the study of effective machine learning techniques against an adversarial opponent. To see why this field is needed, is learning—the study of effective machine learning techniques against an adversarial opponent. To see why this field is needed, it is helpful to recall a common metaphor: security is sometimes thought of as a chess game between two players. For a player to win, it is not only necessary to have an effective strategy, one must also anticipate the opponent's response to that

Secret Key

Select a message digest algorithm

COMPUTE HMAC

Computed HMAC:

caa674c4133df5e645be898a9188a0475ee8da0b567372d9d474b578136c702ebe643122ef9763f60fe8e91e6f3ea3d0cecca2956a178558768ae5cb8f43c532

7)RIPEMD 160:

Copy-paste the string here

In this paper, we discuss an emerging field of study: adversarial machine learning—the study of effective machine learning techniques against an adversarial opponent. To see why this field is needed, is learning—the study of effective machine learning techniques against an adversarial opponent. To see why this field is needed, it is helpful to recall a common metaphor: security is sometimes thought of as a chess game between two players. For a player to win, it is not only necessary to have an effective strategy, one must also anticipate the opponent's response to that

Secret Key

security

Select a message digest algorithm

RIPMD160

COMPUTE HMAC

Computed HMAC:

aa48ff105208ea8c20d3641c821428a8fc53aa60

8)CRC 32:

In this paper, we discuss an emerging field of study: adversarial machine learning—the study of effective machine learning techniques against an adversarial opponent. To see why this field is needed, is learning—the study of effective machine learning techniques against an adversarial opponent. To see why this field is needed, it is helpful to recall a common metaphor: security is sometimes thought of as a chess game between two players. For a player to win, it is not only necessary to have an effective strategy, one must also anticipate the opponent's response to that strategy.

Statistical machine learning has already become an important tool in a security engineer's repertoire. However, machine learning in an adversarial environment requires us to anticipate that our opponent will try to cause machine learning to fail in many ways. In this paper, we discuss both a theoretical framework for understanding adversarial machine learning, and then discuss a number of specific examples illustrating how these techniques succeed or fail.

secret

crc32

Calculate HMAC

Clear

6cb310f4

4 Compare the properties of the above algorithms in terms of security and performance with 1-2 simple experiments. Read the textbook or additional sources, if necessary. Explain your answer in your own words. Cite any additional reference that you found helpful.

Protecting passwords is now a big challenge because users want to do all types of work online. Hashing is the current best solutions for protecting the user passwords. Now we consider applying various hash algorithms on the password and compare them.

While comparing hash algorithms we should consider three things

- 1) Performance or speed
- 2) Collision resistance
- 3) Deterministic.

MD5 is vulnerable to a lot of collision attacks, so if you don't trust the users, it is possible for them to make files which hash to the same value as other files, but which are not in fact the same. Although SHA-256, SHA-384, and SHA-512 have longer hash codes, MD5 and SHA-1 are tried and tested and are known to be reliable. **Remember that a longer hash code does not provide greater security if the underlying algorithm is flawed. MD5 is the fastest hashing algorithm** included in the .NET Framework, but the relatively small hash code size makes it more susceptible to brute force and birthday attacks.

The NSA stated that the change addressed a flaw in the original algorithm that reduced its cryptographic security. The NSA has never described this flaw, leading the paranoid world of cryptographers to spend many thousands of hours analyzing the algorithm, looking for any weaknesses deliberately introduced into SHA-1 to facilitate government skullduggery. To date, no weaknesses have been found, and **SHA-2 is considered a secure algorithm.**

SHA-256 or other SHA-2 family algorithms are the most effective algorithms that can be used for the website's security because they do not have the collisions that MD5 and older hash techniques have.

Comparing various Hash Algorithms:

	SHA1	SHA-256	SHA-384		SHA-512	MD5	MD4

Message digest size	160	256	384		512	128	128
Message size	$<2^{64}$	$<2^{64}$	$<2^{64}$		$<2^{128}$	$<2^{64}$	$<2^{64}$
Word size	512	512	1024		1024	32	32
Block size	32	32	60		60	512	512
No of steps	80	64	80		80	64	3
security	80	128	190		256	64	64

Reference: https://en.wikipedia.org/wiki/Comparison_of_cryptographic_hash_functions

5) Which hash function algorithm is used on the certificate for the following site?

<https://semo.instructure.com/>

- What kind of certificate header values differentiate two different browsers on your lab-mate's and your computers?
- Capture the screenshot of the certificate details showing up on the browsers.
- Explain your answer in your own words.

The hash function algorithm used for <https://semo.instructure.com/> is **SHA256**, the certificate is issued by the Amazon.

SHA-256 or other SHA-2 family algorithms are the most effective algorithms that can be used for the website's security because they do not have the collisions that MD5 and older hash techniques have.

Essentially, a website security certificate is a digital stamp of approval from an industry-trusted third party known as a certificate authority (CA). More specifically, it's a digital file containing information that's issued by a CA that indicates that the website is secured using an encrypted connection.

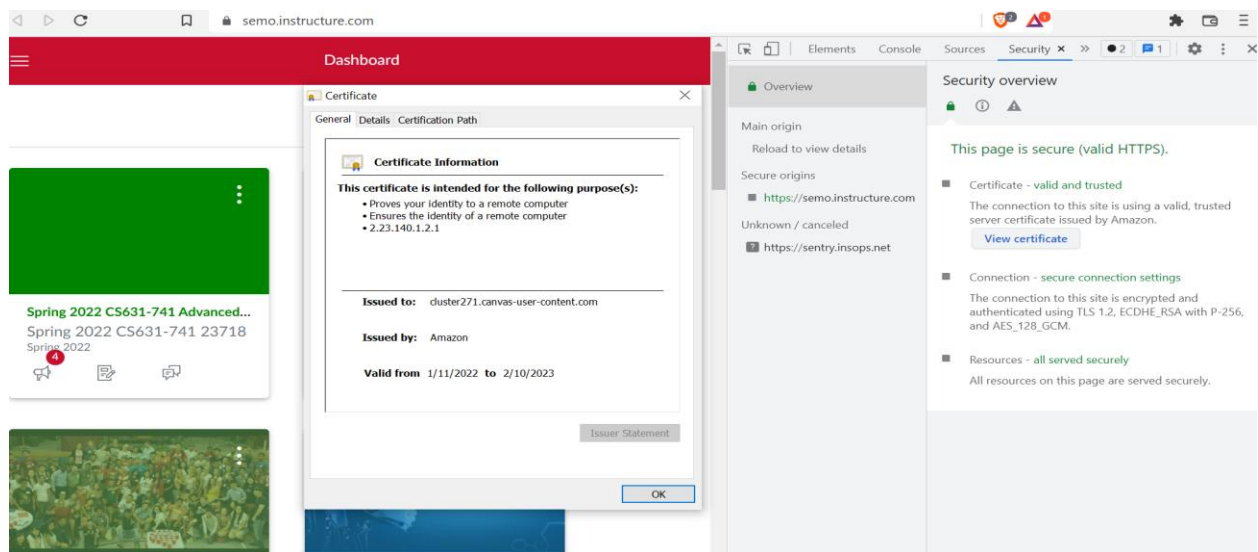
With a website security certificate, users can be confident that:

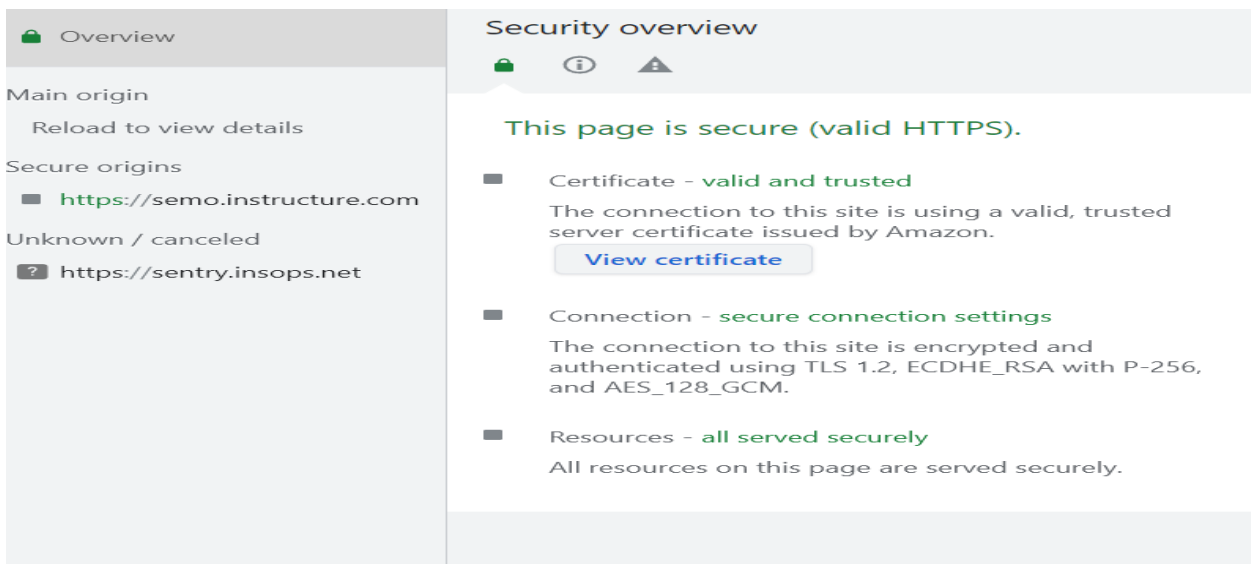
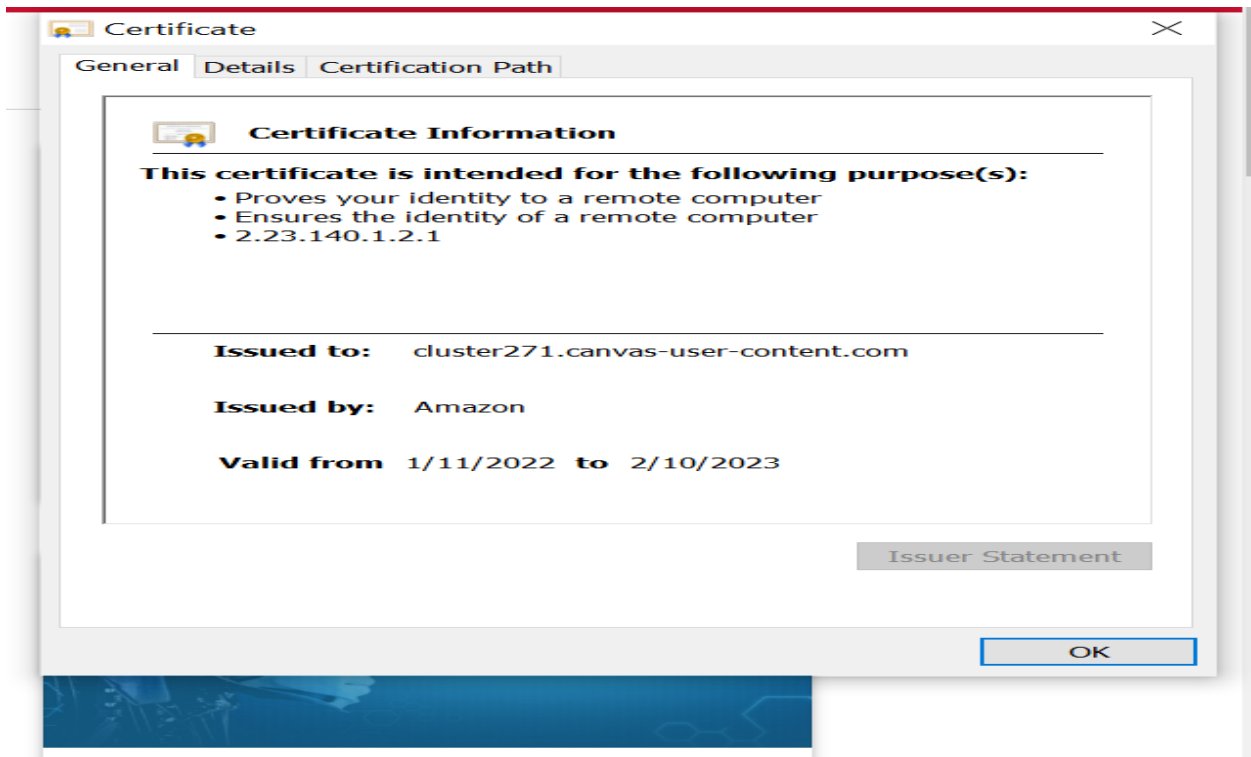
- They're connected to the correct, official server for the website they're trying to visit.
- Nobody can intercept data they send to the website and use it for wrong purposes.

- a) I have compared the two certificates one on my system other one on my friend's system, both looked same. There is no change in the value. I think the Certificate will be same and it does not depend on the browser. Its job is making the browser trust the website.

But the server identifies the client by using the IP address. In this case we have CSRF token. That is used identify each browser uniquely.

b) Screenshots of the certificate:



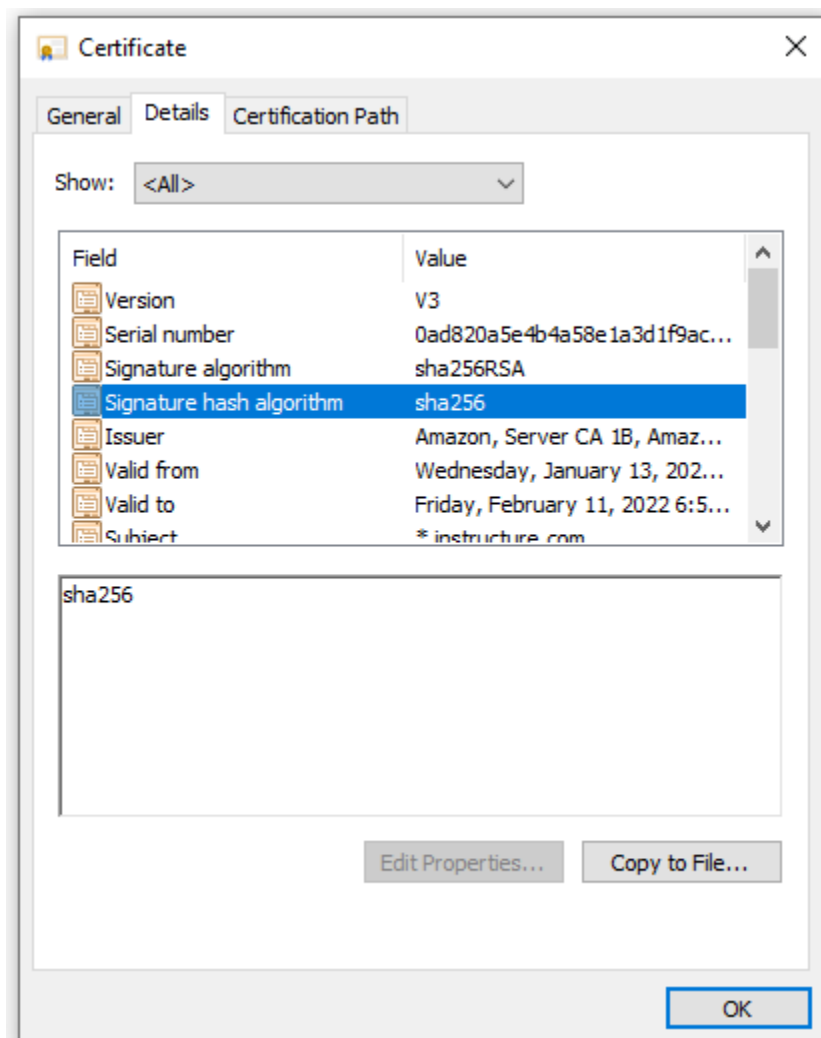


c) In the given website, <https://semo.instructure.com/> the certificate was issued by the third-party industry-trusted certificate authority (CA) which is Amazon.

In this certificate, in the general section tab, we can see that it has been ensured the following security details.

- ‘Proves your identity to a remote computer’
- ‘Ensures the identity of a remote computer’
- ‘Proves your identity to a remote computer’
- ‘Ensures software came from software publisher’
- ‘Protects software from alteration after publication’
- ‘Allows data on disk to be encrypted’
- ‘Protects e-mail messages’
- ‘Allows secure communication on the Internet’
- ‘Allows data to be signed with the current time’
- ‘All issuance policies’

The ‘2.23.140.1.2.1’ in the certificate denotes SSL certificate’s Domain Validation (DV)

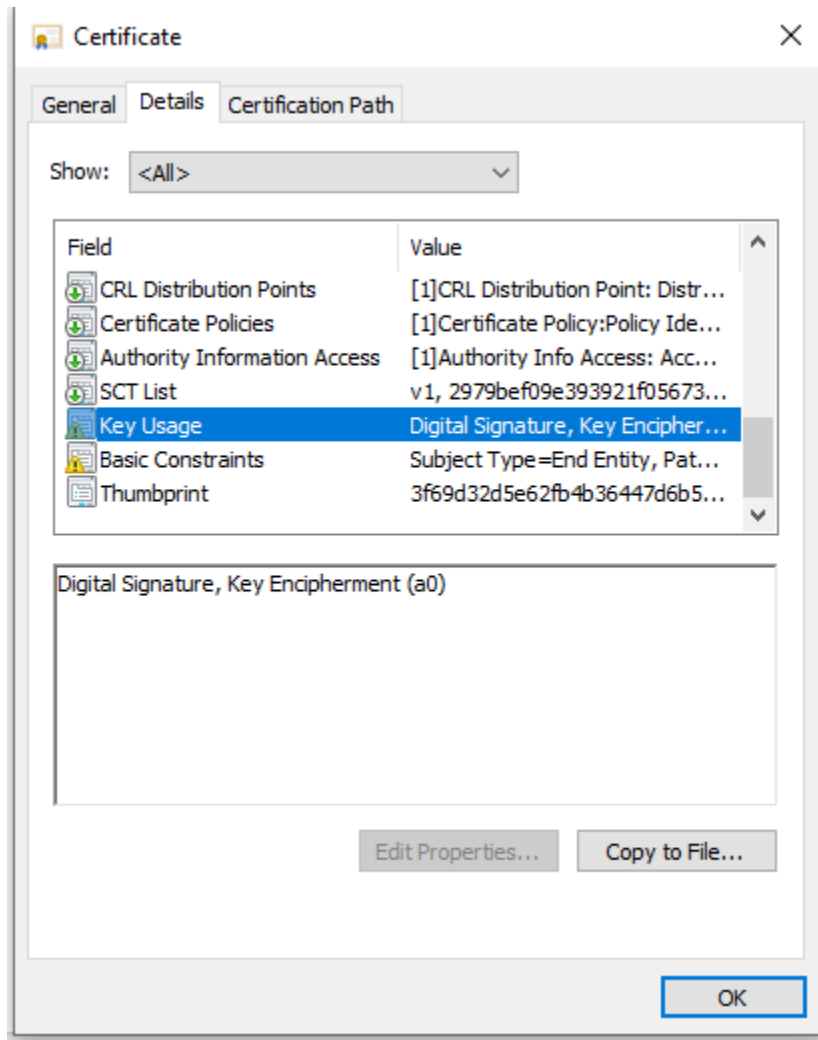


In the certificate’s details tab, we can see that **sha256** signature hash algorithm has been used for the security of the website.

The SSL industry has picked SHA as its hashing algorithm for digital signatures.

The SHA-2 group consists of six hash functions with digests (hash values) that are 224, 256, 384 or 512 bits: SHA-224, SHA-256, SHA-384, SHA-512.

SHA-256 is a novel hash functions computed with eight 32-bit.



In the above screenshot we can also see that this Hash function Algorithm is mainly for the purpose of :

‘Digital Signature, Key Encipherment’

The below screenshot gives the details regarding the CA(Certificate Authority) who is third party trusted authority to issue this certificate.

