Assignment on Cryptography for CS50L

Total points 9/10

Starting in 2021, all assignments in CS50L are out of 10 points. A score of 7 points or better (70%) is required to be considered to have "passed" an assignment in this course. Please do not resubmit an assignment if you have already obtained a passing score. You don't receive a final grade at the end of the course, so it will have no bearing on your certificate, and it will only slow down our graders!

Unlike CS50x, assignments in this course are graded on a set schedule, and depending on when you submitted, it may take up to three weeks for your work to be graded. Do be patient! Project scores and assignment status on cs50.me/cs50l (e.g. "Your submission has been received...") will likely change over time and are not final until the scores have been released.

Email *

maz786@outlook.com

Name *

Mazafer Ul-Raqib

edX Username *

Mazafer

What is your GitHub username?

You only need to tell us if you are concerned about checking your progress in the course and/or you want a free CS50 Certificate after you satisfy all of the requirements of the course. If you do not already have a GitHub account, you can sign up for one at https://github.com/join. You can then use this account to log in to cs50.me/cs50l to track your progress in the course (your progress will only show up after you have received at least one score release email from CS50 Bot, so do be patient!). Don't worry about seeing a 'No Submissions' message on submit.cs50.io, if you find that. The course collects submissions using Google Forms, and only the gradebook on cs50.me/cs50l is important! If you do decide to provide us with a GitHub username, BE CERTAIN IT IS CORRECT. If you provide the wrong username, you will not be able to see your scores.

https://github.com/maz786

This course is graded by human graders, and has a ZERO TOLERANCE plagiarism and collaboration policy. If *any* of your answers are copied and pasted from, or obviously based on (a) an online source or (b) another student's work in the course, in *any* of the course's ten assignments, you will be reported to edX and removed from the course immediately. There is no opportunity for appeal. There are no warnings or second chances. *

It is far better, we assure you, to leave an answer blank rather than risk it. This may be an online course, but it is offered by Harvard, and we're going to hold you to that standard.

- (◉) I understand this policy and agree to its terms; I hereby affirm that I will not plagiarize any answers or collaborate with any other students in this course .

Questions

✓ What is a primary difference between a cipher and a hash? 1/1

A hash is an algorithm that creates a fixed-size output (referred to as a hash value or hash code) from a variable-size input, whereas a cypher is an algorithm that is used to encrypt and decrypt data (called the message).

Ciphers and hashes differ primarily in the following ways:

A cypher is a two-way function, which means that both encrypting and decrypting data may be done with it. The opposite is true for a hash, which is a one-way function that can only be used to obtain a hash value from a message and cannot be used to reconstruct the original message from the hash value.

A cipher's primary function is to safeguard data by rendering it unintelligible to those without access to the decryption key. A hash's primary function is to give a mechanism to compare the hash values of an original message and a copy in order to validate the consistency of the message.

Ciphers frequently generate output that is either slightly larger than the input or the same size as it. As opposed to this, hashes often result in a fixed-size output that is significantly less than the input.

Resistance to collisions: When two distinct inputs result in the same hash value, a collision occurs. A hash function must have a low collision rate since a collision could allow a message to be forged by an adversary. Contrarily, since cyphers aren't used to check a message's integrity, they aren't worried about collisions.

Overall, in computer science and cryptography, cyphers and hashes are two different kinds of algorithms that are utilised for various objectives.

✓ In no more than a few sentences, why are most one-for-one substitution ciphers inherently insecure? 1/1

The majority of one-for-one substitution cyphers are intrinsically unsafe due to the ease with which letter frequency analysis may decrypt them. Each letter of the plaintext is swapped out for a different letter of the alphabet in a one-for-one substitution cypher in accordance with a predetermined rule. This implies that a letter in the ciphertext will always be used in place of a letter in the plaintext. This makes it simple to identify the correspondence between the letters in the plaintext and the ciphertext by analysing the frequency of the letters in each.

One-for-one substitution cyphers can be made more secure by employing a key that alters the correspondence between plaintext and ciphertext for each message or by implementing a more complicated substitution algorithm that does not maintain the plaintext's letter frequency. However, these techniques add more complexity and might not be applicable in all circumstances.

✓ Why do companies give you a link to create a new password when you click "Forgot Password" on a login screen? 1/1

Companies typically offer a link to establish a new password when a user hits "Forgot Password" on a login screen because it enables them to securely reset the user's password without sending the new password over the internet.

This is due, in part, to the security risk posed by transmitting a new password over the internet, even if it is encrypted. An attacker who intercepts the password may be able to decode it and access the user's account.

Companies can prevent the new password from being transmitted over the internet by offering a link to set a new password. Instead, users are taken to a screen where they can create a new password, which is subsequently encrypted and saved on the company's servers. This helps to safeguard the user's account by lowering the likelihood that the new password will be compromised.

The ability for consumers to select a password that is more secure than their current password is another reason why businesses may offer a link to create a new password. This can aid in defending the user's account from assaults like brute-force cracking, in which an attacker attempts every conceivable combination in an attempt to guess the user's password. Companies can implement password rules that encourage users to select robust, distinctive passwords that are more difficult to crack by asking the user to create a new password.

✓ How are cryptographic hash functions different from other hash functions? 1/1

A particular kind of hash function created especially for use in cryptography is known as a cryptographic hash function. They are suited for use in cryptography applications due to a number of factors, including:

A cryptographic hash function is a one-way function, making it simple to calculate a message's hash value but impossible to reconstruct the original message from the hash value. This attribute is crucial for maintaining a message's integrity since it prevents an attacker from forging a message by producing a duplicate with the same hash value as the original.

A cryptographic hash function is collision-resistant if it makes it challenging to locate two messages that give the same hash result. This attribute is crucial for guaranteeing a message's uniqueness since it prevents an attacker from producing a duplicate message that is identical to the original.

Pseudorandomness: A cryptographic hash function should have the appearance of being random, which makes it challenging to anticipate the function's result from its input. This attribute ensures that an attacker cannot simply guess the hash value of a new message, which is crucial for message security.

Fixed-size output: Regardless of the size of the input message, a cryptographic hash function should have a fixed-size output. Practically speaking, this attribute is significant since it guarantees that, regardless of the size of the message, the hash value will always be the same size.

For a variety of cryptographic applications, cryptographic hash functions are created to be safe, effective, and simple to use. They are a crucial tool in computer science and are applied to several systems and methods.

✗ Have a look at http://shattered.io. In a few sentences of your own words, what techniques did the researchers employ to "break" SHA-1? 0/1

The SHA-1 hashing algorithm was cracked by researchers that used methods including collision attacks and hash collision resolution to identify two distinct messages that result in the same hash value when hashed with the SHA-1 algorithm. By combining two PDF files with distinct contents into one, they were able to produce the same SHA-1 hash value. Even though the contents of the two PDF files were different, they were still able to utilise the first file's digital signature as a legitimate signature on the second one. This showed that the SHA-1 method is no longer secure for usage in specific applications like digital signatures and file integrity verification. It also showed that it is now practically easy to counterfeit a SHA-1 signature.

✓ Why is it not a problem for me to reveal my public key? 1/1

Since it is intended to be shared publicly, it is not a concern to divulge your public key. In a system of public-key cryptography, each user has a set of two keys: a public key and a private key. Messages that were encrypted with the matching public key are decrypted using the private key, which is kept a secret. On the other hand, the public key is used to encrypt messages that can only be decoded with the accompanying private key and is meant to be widely distributed.

Because the public key is incapable of decrypting messages or carrying out any other sensitive operations, disclosing it does not jeopardise the security of your private key or your messages. It can only be used to encrypt messages, and the associated private key is required to decrypt those messages.

Overall, sharing your public key broadly is not an issue, but it is crucial to keep your private key secure and guard it against unauthorised access. In fact, to effectively use public-key cryptography, this is a need.

✓ In your own words, how does my digital signature provide an almost certain guarantee that a message came from me? 1/1

A digital signature employs the private key of a particular person or organisation to generate an exclusive, unforgeable signature for the message, providing an almost definite assurance that the message originated from that person or organisation.

The sender applies a cryptographic change to the message using their private key to establish a digital signature. The message and the sender's private key are linked to the distinctive signature that results from this change. The receiver is then sent the message and the signature.

The recipient uses the sender's public key to validate the signature after receiving the message and signature. The message must have originated from the sender if the signature is legitimate since it proves that it was signed using the sender's private key. If the signature is invalid, the message may have been changed while in transit or may not even have been sent by the intended recipient.

Since it is very difficult to fabricate a digital signature without the private key, it offers an almost definite assurance that a communication was sent by a particular person or organisation.

✓ Provide an example of an everyday activity you perform on the internet that relies on encryption. 1/1

Email, online shopping/ banking, VPNs etc

✓ What does it mean for a blockchain ledger to be decentralized? 1/1

A decentralised blockchain ledger is one that is managed by a network of participating nodes rather than being under the jurisdiction of a single central authority or organisation.

There is no centralised point of failure or control in a decentralised blockchain. Instead, a distributed network of nodes that each have a copy of the ledger and collaborate to validate and add new transactions to it maintains and updates the ledger. This means that the ledger may continue to function even if some nodes go offline or are compromised because it is not dependent on any one node or set of nodes.

A crucial aspect of blockchain technology is decentralisation, which enables the ledger to be open, safe, and impervious to interference and censorship. Additionally, it makes the network autonomous and decentralised, removing the need for a single authority to oversee it.

In general, decentralisation is a key characteristic of blockchain technology that promotes the reliability and security of the network and ledger.

✓ Jevgr "V penpxrq gur pbqr!" 1/1

No, the above isn't random typing! :)

"I cracked the code!" ✓

Debrief

About how many MINUTES would you say you spent on this assignment? *

Just to set expectations for future students.

666

This form was created inside CS50.

Google Forms