**x) € Schneier 2015: Applied Cryptography: [2.3 One-Way Functions](https://learning.oreilly.com/library/view/applied-cryptography-protocols/9781119096726/10_chap02.html" \l "chap02-sec003)**

* It is easy to generate a one way function but almost impossible to reverse the computational function back to the original input.
* It would take all current worlds computational power millions of years to reverse a one-way fuction.
* Simply put – You can break a plate in a million tiny pieces but cant fix it back.
* Mathematically speakin, there is no proof that one-way functions exist, and no real evidence that they can be formed.
* We can compute one-way functions but currently, no solution to reverse.
* One-way functions are useless as we cant decrypt a message encrypted with it. Use something else for public key encryption!
* Trapdoor one-way, is a one-way function with a secrete formular to reverse it. That is if you know the secret.
* Like an unassembled watch, the tiny small pieces can be put back into a working watch with the assembly manual.

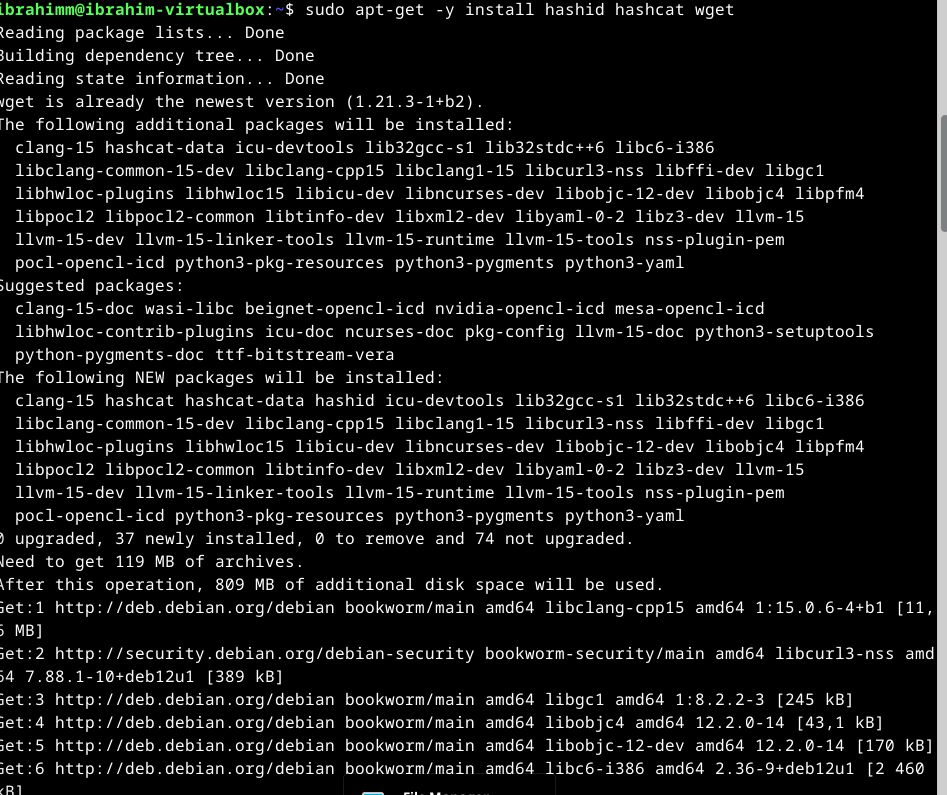
**2.4 One-Way Hash Functions.**

* one-way hash function, also called: compression function, contraction function, message digest, fingerprint, cryptographic checksum, message integrity check (MIC), and manipulation detection code (MDC). Is essential to modern cryptography and a building block for many protocols.
* It takes an input and generates a fixed-length output (hash value), acting like a fingerprint.
* It's easy to compute the hash value from the input but hard to reverse the input from the hash value.
* The hash function is designed to be public and provides a way to check if an input corresponds to a specific pre-image.
* It's computationally impractical to find a pre-image that hashes to a particular value.
* One-way hash functions are generally used to ensure data integrity, for example in financial transactions and file verification.

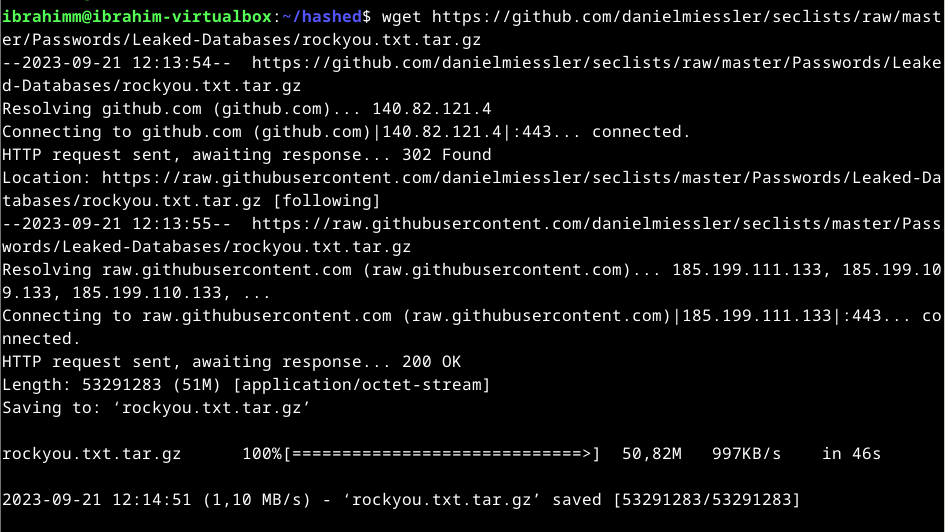
**Särökaari 2018: [Phishing trough email](https://www.youtube.com/watch?v=m9YFJGSHYtY) (video, 33 min)**

* Phishing through email is a type of cyber attack where false emails messages, trick receivers into revealing sensitive information like passwords, credit card numbers, or other personal information.
* Attackers exploit curiosity to make receiver click on the link.
* An experiment done on 1200 students showed that most individuals fall for the attack because they think sender is legitimate, message fit expectation, thought they know the sender.
* **Protection against email phishing,** implement an email verification system(SPF) to verify the sender IP address is legit.
* Implement DomainKeys Identified Mail and use SPF and DMARK which add cryptographic signatures to email headers.
* Malware/ Spam filtering protects against malicious attachments.
* URL whitelisting, only known domains are allowed to send messages.

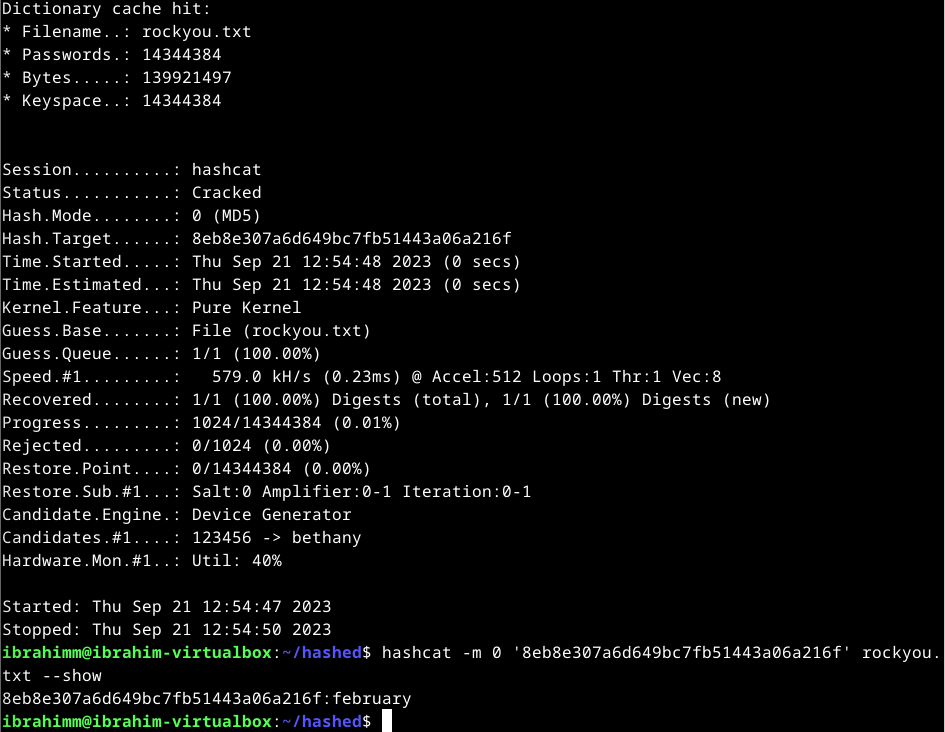
**a) Install Hashcat. Test it with a sample hash. See Karvinen 2022: [Cracking Passwords with Hashcat](https://terokarvinen.com/2022/cracking-passwords-with-hashcat/)**



* Download the Rockyou leaked passwords dictionary



**b) Crack this hash: 8eb8e307a6d649bc7fb51443a06a216f**



**c) Gone phising. Create a phising email. In addition to the email, you must explain your tactics and the scennario where the phising email is used.**

**Scenario:**

The attacker's focus is on a thriving small business, driven by a personal dislike for the business owner. Their intent is to disrupt the business's social media presence. This business has quite a large Instagram following, using this platform for product marketing, customer engagement through quizzes, and hosting various giveaways.

The attacker decides to create a phishing email account with a domain name very similar to that of Instagram. But it ends with Gmail instead.

For this attack the attacker is using a tool called Blackeye which can be found in GitHub. The tool is used for replicating various sites including Amazon, Facebook, and many more popular sites. So, it is the perfect tool to carry out the attack.

**Attack: A fake user privacy policy update.**

**Email hearder:** Updated User Generated Content Policies

**Body:**

We have updated our User Generated Content Policies with immediate effect. Read more (Link) how this affects your business.

The business owner now has a sense of urgency to find out what this means for their business on the platform. After clicking the link in the email it directs them to a replica of ig’s login page.

A screenshot of a login page

Description automatically generated

If the link is successfully clicked and the login credentials are provided on the form, the attacker receives the password and username combination.

From here it only depends on whether the account has MFA enabled.