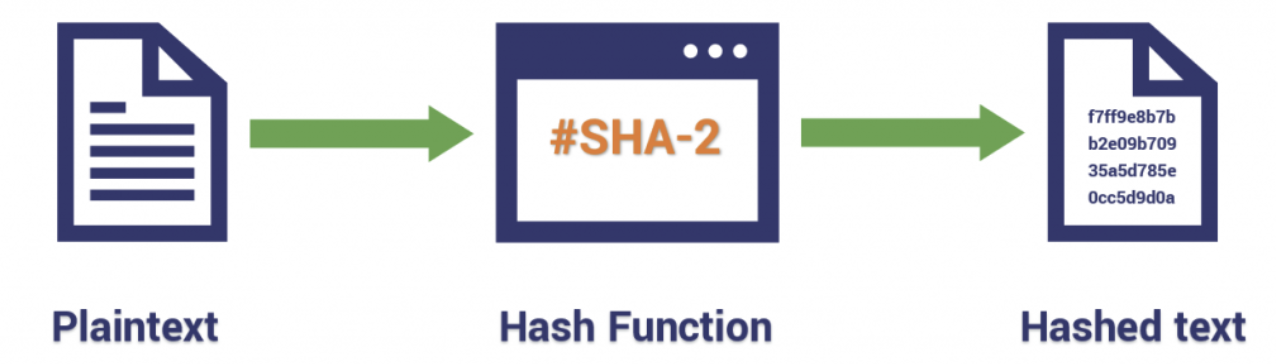
**Password Cracking Lab**

**Think Like an Adversary & Confidentiality**

**Intro:** Passwords are used in nearly every aspect of computers to help protect accounts and data. These passwords are almost always stored as a hash on the computer instead of the plaintext version of the password. A hash is just the output of a of a one way mathematical equation. When a user tries to log in with their password, the computer takes the entered password, hashes it, and then compares the hash to the stored hash. If the hashes match, the user is allowed in, if they don’t match then the user is prompted to retry their password.



**LAB:**

**1)** Determine what type of hash algorithm is being used for the below samples. Here’s a website with sample hash types: <https://hashcat.net/wiki/doku.php?id=example_hashes>

|  |  |
| --- | --- |
| 8743b52063cd84097a65d1633f5c74f5 |  |
| c73d08de890479518ed60cf670d17faa26a4a71f995c1dcc978165399401a6c4:53743528 |  |
| b89eaac7e61417341b710b727768294d0e6a277b |  |
| $ASN$\*1\*20000\*80771171105233481004850004085037\*d04b17af7f6b184346aad3efefe8bec0987ee73418291a42 |  |

**2)** There are many online resources to hash plaintext. One such website is <https://www.md5hashgenerator.com/> Use this website to create hashes for the following plaintext passwords using the specified hash algorithm:

|  |  |  |
| --- | --- | --- |
| DuluthHuskies | MD5 |  |
| HermantownHawks | MD5 |  |
| DuluthEastGreyhounds | SHA256 |  |
| DuluthDenfeldHunters | SHA512 |  |

**3)** Now let’s try the opposite and see if you can figure out what the plaintext passwords are for the following hashes. A site like <https://www.crackstation.net> might be helpful. Find the password and the hash algorithm used:

|  |  |  |
| --- | --- | --- |
| **HASH** | **ALGORITHM** | **PLAINTEXT PASSWORD** |
| 66d040632ba3e1ae771ddced2f6e0505 |  |  |
| 16790e14f10f2a3b251acb4d0e86e6661ec37b8d |  |  |
| d51fe8cb7e8862bb66803afa414d4230e999b82d |  |  |
| 092BF371D0BE6B15F8E2DCF61288CC96 |  |  |

**4)** One more category of hashes. These are called Ciphers. Ciphers are cryptographic algorithms used to encode or decode information, typically involving the substitution or rearrangement of letters or symbols. They are employed to ensure the confidentiality and integrity of data, providing a means of secure communication and protecting sensitive information from unauthorized access.

Ciphers have a rich history dating back thousands of years, with ancient civilizations like the Egyptians and Greeks developing rudimentary encryption techniques. Over time, ciphers evolved and became more sophisticated, playing pivotal roles in wartime communications, espionage, and the development of modern cryptographic systems.  
A site like <https://www.dcode.fr/cipher-identifier> might help in identifying what type of cipher was used.

|  |  |  |
| --- | --- | --- |
| **Code** | **Cipher Tip** | **PLAINTEXT PASSWORD** |
| 10010001110100010001 0100010001 00000 0000100000000100110101100 000100100001110001110010010000 | Mmmm “Bacon”…try to decode using a bacon cipher |  |
| Lmafgok yohqgl nijyetgq | Vigenere Ciphers need a key to decode…try using GenCyber |  |
| Ebgngvat yrggref perngr guvf pvcure | ROT13 is much like a Ceasar Cipher |  |
| fc efrn i irnstico omo.Tenlpeedope ifaihahe snt | Rail fence ciphers need multiple pieces of information…in this case the key is 4 and offset is 2 |  |
| 0N1Y 7H3 8357 H4CK3r5 741K W17H 7H15 | Leet speak is what hackers use? |  |
| 83 105 109 112 108 101 32 116 101 115 116 32 102 111 114 32 71 101 110 67 121 98 101 114 | ASCII can be used in obfuscation |  |
| 67%20114%20112%20118%20105%20106%2032%20102%20119%2032%20121%20122%20117%20117%20118%20101%2032%20100%20118%20106%20106%20114%20120%20118%20106%2032%20119%20102%20108%20101%20117 | Challenge…there are multiple layers to this |  |

**BONUS:** You’re getting stronger with the password cracking force...but can you figure out what the plaintext version of the following two hashes are? Hint: The message may be “encoded.” <https://cryptii.com/> or https://www.dcode.fr/en or CyberChef.io might be helpful websites. And you might need to decode first then get a hash to crack…

|  |  |
| --- | --- |
| RUQ2QkM3MjY2NzRCREM0MDU3NEREODE3OUNBMzg4QzQ= |  |
| ..... -.-. . -.. -.-. ----- --... -.. ..--- ...-- -... ----- --... -.. ....- ..--- ..--- -... ....- ---.. ..-. ...-- ..-. ---.. ----. ----. --... .- .- ..... --... --... .---- ..--- ..--- ..--- -.... --... --... ----. -.-. .- ....- ..--- ....- -.. ..-. ----. . ..--- .---- -.. -.. .---- ----- .- ---.. .- .- ----. -.... -... ..-. ..... -... .- -.-. ..-. . ....- ....- .---- ----- .---- ---.. -.... .- -... -.-. ..-. ..-. ..-. ----- -.-. .---- --... ..-. ..... ..... -... -.... .---- -.... ..... -.... -.-. ..... . . .- -.. ..-. .- ....- -.-. ----- -.... .- ...-- --... ..... .---- -.-. --... ..... .- ....- ---.. ..-. ..... ..--- ....- ..-. .- ---.. . .- -.... |  |
|  |  |

