Name: **Chebrolu Sai Prasanna Abhinav**

Crack leaked password database

Here is your task

Your job is to crack as many passwords as possible with available tools (e.g. use Hashcat). Here are your Task instructions:

1. Review the links provided in the additional resources (section 4) below to gain a background understanding of password cracking
2. Try to crack the passwords provided in the 'password dump' file below using available tools
3. Assess the 5 questions in the task instructions below in relation to the passwords provided (type of hashing algorithm, level of protection, possible controls that could be implemented, password policy, changes in policy)
4. Draft an email/memo briefly explaining your findings in relation to controls used by the organization and your proposed uplifts. We recommend spending about 1.5 hours on this task and keeping it at 1 page in length.

Your answer should be provided in the form of a draft email/memo explaining your findings and conclusions of controls currently used by an organization to prevent successful cracking of passwords and potential uplifts that you would propose to existing controls with justifications.

You must determine the following:

1. What type of hashing algorithm was used to protect passwords?
   A. MD5

2. What level of protection does the mechanism offer for passwords?

   - MD5 is an "**iterative**" hash function.
   - MD5 is generally a **considerable mechanism** for storing passwords in production.
   - MD5, produces a **128-bit hash.**
   - MD5 is born out of **RSA's algorithm** (defined in Internet RFC).
   - MD5 is a utility that can **generate a digital signature of a file**. MD5 belongs to a family of one-way hash functions called **message digest algorithms**. The MD5 system is **defined in RFC 1321**.
   - The algorithm takes as input a message of **arbitrary length** and produces as output a **128-bit "fingerprint" or "message digest"** of the input. It is conjectured that it is **computationally infeasible** to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest. The MD5 algorithm is **intended for digital signature applications**, where a large file must be **"compressed"** in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as **RSA**.

3. What controls could be implemented to make cracking much harder for the hacker in the event of a password database leaking again?

    - One way of making the password hard to crack is by **maintaining credentials from multitude of services in a manager** like dashlane because they tend to use **varied hashing** algorithms & even hashing over hashed passwords [e.g. md5(md5($plaintext))] to store and keep the **strength high**, meeting to the rigidity of a strong case for an algorithm to process.
    - **Reduce redundancy** across services such that in case of a leak out of one service doesn't make the **other passwords vulnerable**.
    - **Use alphanumeric character** with **special characters**.
    - Reducing occurrence of an **adjective on noun or verb** which is an obvious prey to brute force attacks.

4. What can you tell about the organization's password policy (e.g. password length, key space, etc.)?

    - It can be very well determined that the organization's **password policy is not up to the mark** as:
        - The key length is at an **average of 11**.
        - Although they do not allow spaces, the use of **special characters is probably resisted** to a set of common delimiters like '_'.
        - The use of **numbers increases the resistance** of password by a factor of **10 times the digit appears**.
        - The **lack of capital characters** splits the password strength by half.
        - **Not avoiding the occurrence of English verbs** like book, popular, eating, hero, life, John Wick, interest, expert in turn making the password vulnerable to brute force attacks.

5. What would you change in the password policy to make breaking the passwords harder?
    - Keeping a **threshold on length**.
    - **Caution** over use of **verbs are nouns or adjectives**.
    - **Mandating** minimum **3 special characters and minimum one capital letter**.
    - Applying a **hashing algorithm over another**, recursively to have a strong hashing function e.g. md5(strtoupper(md5($plaintext)))
    - **Not allowing sibling credentials to assist** the password naming, like name / surname / date of birth / sex.

Password Text:

```
experthead:e10adc3949ba59abbe56e057f20f883e
interestec:25f9e794323b453885f5181f1b624d0b
ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4
reallychel:5f4dcc3b5aa765d61d8327deb882cf99
simmson56:96e79218965eb72c92a549dd5a330112
bookma:25d55ad283aa400af464c76d713c07ad
popularkiya7:e99a18c428cb38d5f260853678922e03
eatingcake1994:fcea920f7412b5da7be0cf42b8c93759
heroanhart:7c6a180b36896a0a8c02787eeafb0e4c
edi_tesla89:6c569aabbf7775ef8fc570e228c16b98
liveltekah:3f230640b78d7e71ac5514e57935eb69
blikimore:917eb5e9d6d6bca820922a0c6f7cc28b
johnwick007:f6a0cb102c62879d397b12b62c092c06
flamesbria2001:9b3b269ad0a208090309f091b3aba9db
oranolio:16ced47d3fc931483e24933665cded6d
spuffyffet:1f5c5683982d7c3814d4d9e6d749b21e
moodie:8d763385e0476ae208f21bc63956f748
nabox:defebde7b6ab6f24d5824682a16c3ae4
bandalls:bdda5f03128bcbdfa78d8934529048cf
```

Security Algorithms used:

experthead:e10adc3949ba59abbe56e057f20f883e – MD5
interestec:25f9e794323b453885f5181f1b624d0b – MD5
ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4 –MD5
reallychel:5f4dcc3b5aa765d61d8327deb882cf99 –MD5
simmson56:96e79218965eb72c92a549dd5a330112 – MD5
bookma:25d55ad283aa400af464c76d713c07ad – MD5
popularkiya7:e99a18c428cb38d5f260853678922e03 – MD5
eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 – MD5
heroanhart:7c6a180b36896a0a8c02787eeafb0e4c – MD5
edi_tesla89:6c569aabbf7775ef8fc570e228c16b98 – MD5
liveltekah:3f230640b78d7e71ac5514e57935eb69 – MD5
blikimore:917eb5e9d6d6bca820922a0c6f7cc28b – MD5
johnwick007:f6a0cb102c62879d397b12b62c092c06 – MD5
flamesbria2001:9b3b269ad0a208090309f091b3aba9db – MD5
oranolio:16ced47d3fc931483e24933665cded6d – MD5
spuffyffet:1f5c5683982d7c3814d4d9e6d749b21e – MD5
moodie:8d763385e0476ae208f21bc63956f748 – MD5
nabox:defebde7b6ab6f24d5824682a16c3ae4 – MD5
bandalls:bdda5f03128bcbdfa78d8934529048cf – MD5

Cracked Passwords:

experthead:e10adc3949ba59abbe56e057f20f883e – 123456
interestec:25f9e794323b453885f5181f1b624d0b – 123456789
ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4 – qwerty
reallychel:5f4dcc3b5aa765d61d8327deb882cf99 – password
simmson56:96e79218965eb72c92a549dd5a330112 – 111111
bookma:25d55ad283aa400af464c76d713c07ad – 12345678

```
popularkiya7:e99a18c428cb38d5f260853678922e03 - abc123
eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 - 1234567
heroanhart:7c6a180b36896a0a8c02787eeafb0e4c - password1
edi_tesla89:6c569aabbf7775ef8fc570e228c16b98 - password!
liveltekah:3f230640b78d7e71ac5514e57935eb69 - qazxsw
blikimore:917eb5e9d6d6bca820922a0c6f7cc28b - Pa$$word1
johnwick007:f6a0cb102c62879d397b12b62c092c06 - bluered
```