Check Out my cracked hashes based on the given "Password dump" by Goldman Sachs here:

**Dear Goldman Sachs,**

After trying to crack all the leaked hashes, I found several vulnerabilities in your password policy and this Memo conclude all the findings and suggestions to improve your password policy.

1)What type of hashing algorithm was used to protect passwords?

* **SHA-256, SHA-3, bcrypt and Message Digest (MD5)** are the standard cryptographic hash functions to provide data security for authentication. All the passwords which are compromised were using MD5 which is weaker and prone to collisions.

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

* 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.
  + It was very easy to crack with hashcat rockyou.txt or crack station wordlist and hash suite charset. I would suggest that you use a very strong password encryption mechanism to create hashes for the password based on SHA.

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 to combine multiple algorithms to make the hash stronger like **[ SHA-256(MD5(password)].**
* Reducing the 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.)?

* After cracking the password, we find the following things about the organization's password policy:
  + The key length is at an **average of 11.**
  + **Avoiding the occurrence of English verbs and nouns** like book, popular (Commo words).
  + Include special characters, Capital and Small letters, numbers in your password.

5) What would you change in the password policy to make breaking the passwords harder?

* You can include several new things in your password policy. My recommendations are:
* Applying a **hashing algorithm over another**, recursively to have a strong hashing function like **(Example: [ SHA-256(MD5(password) ] ).**
* Avoid common words, nouns and verbs. Longer passwords are better. Use a minimum **of 3 special characters and a minimum one capital letter and one number.** Don't reuse your passwords
* Do not let users include their username, actual name, date of birth and other personal information while creating a password.



**TO:**

**My Password Policy for Goldman Sachs(Virtual Internship)**

**08th September, 2021**

**https://www.linkedin.com/in/manikandankb/**

**manikandankb18@gmail.com**

**MANIKANDAN K B**

**+91 9952524502**

username

**SMITH**