Q: What type of hashing algorithm was used to protect passwords?

MD5

Q: What level of protection does the mechanism offer for passwords?

* MD5 is hash function.
* MD5 is generally a considerable mechanism for storing passwords in production.
* 128 bit hash is produced by MD5
* RSA Algo was behind production of MD5.
* 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.

Q: 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. By intake of minimum 15 characters for password as average password taken is 12 characters only.

Q: What can you tell about the organization’s password policy?

* The key length is at an average of 12.
* 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.

Q: What would you change in the password policy to make breaking the passwords harder?

* Keeping a threshold on length and caution over use of verbs are nouns or adjectives.
* Mandating minimum 3 special characters and minimum one capital letter.
* Not allowing sibling credentials to assist the password naming, like name / surname / date of birth / sex.