What type of hashing algorithm was used to protect passwords?

MD5 hash function, which is designed as a cryptographic function.

What level of protection does the mechanism offer for passwords?

MD5 hash function maps a set of data to a bit string of a fixed size, the hash value, which is 128 bits. Verifies that a file has been unaltered by producing a digit representing the sum of the correct digits in the password before and after, and then comparing those digits. However, two distinct messages can hash to the same value and so is quite vulnerable.

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

* Anti-debug methods. Check the presence of tools used by crackers before the program is run. If the tools are detected the program is suspended. Either a debugger or debugger breakpoints are detected.
* Extra protected file. Encrypted and compress the executable file of an application so that when there is any attempted modification the file will not run. After protection, a special code is added to the structure.
* Stronger passwords made mandatory. Increased use of special characters, limited or no use of dictionary words, no sequential numbers or letters, no personal info such as birthdays or names, and increase the length of passwords.
* Key stretching algorithms. Significantly reduces the rate at which passwords can be tested by converting a password to a longer and more random key. Multiple methods to do this, such as applying a cryptographic hash function or block cypher repeatedly in a loop, and using cryptographic hash functions that have large memory requirements.
* Salting. A salt is randomly generated for each password and concatenated and processed with a cryptographic hash function. Salt must not be reused or too short. Makes it more challenging for a hacker to use lookup, reverse lookup, and rainbow tables.
* More secure encryption hash. Ideally, a hash function should return no collisions but MD5 hash function does have many collisions. Out of common functions, algorithms like SHA-2 and SHA-3 are considered to be more secure than MD5 and SHA-1.

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

Does not require capital letters, special characters, or numbers, and the minimum length seems to be 6 characters. Sequential or repeated numbers are allowed, and the policy does not discourage common passwords such as “password”, “qwerty”, and “qazxsw”.

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

* A minimum of 12 characters
* 2+ special characters
* 2+ letters
* 2+ numbers
* No sequential numbers
* Common passwords that include “password” or “qwerty” not allowed
* Warning to the user when years or a location are e.g. “London” or “2005”
* Passwords must be changed at regular intervals like every 6 months