**To**: Receiver at Goldman Sachs

**From**: Ayush Kapoor (Undergrad at IIT Bombay) (contact: [ayushk681@gmail.com](mailto:ayushk681@gmail.com))

**Subject:** Observations and conclusions made for task 1.

Following are the decoded password strings.

|  |  |  |
| --- | --- | --- |
| Username | Hashed string | Decoded string |
| 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 |
| flamesbria2001 | 9b3b269ad0a208090309f091b3aba9db | Flamesbria2001 |
| oranolio | 16ced47d3fc931483e24933665cded6d | Oranolio1994 |
| spuffyffet | 1f5c5683982d7c3814d4d9e6d749b21e | Spuffyffet12 |
| moodie | 8d763385e0476ae208f21bc63956f748 | moodie00 |
| nabox | defebde7b6ab6f24d5824682a16c3ae4 | nAbox!1 |
| bandalls | bdda5f03128bcbdfa78d8934529048cf | Banda11s |

* Hashing algorithm used: **MD5**
* Level of Protection : **Level 2** (Just Hashing and encrypting the string)
* *Controls that can be implemented to make cracking difficult:*

1. Involving randomly generated salt that can be passed along with actual password to the hashing function.
2. Involving multiple hashing function in series with a random salt in each step to encrypt the password.

* *Organization’s password policies as per prediction:*

1. Minimum password length of 6 characters.
2. Involving letters in both lower and upper cases.
3. Involving numbers and symbols (!, @ etc)

* *Changes required in password policy:*

1. Minimum password length should be 8 characters.
2. Should not involve any combination with username.
3. Must include at least one symbol and number each.
4. Should check the password strength using rainbow table examples.