1) Assume your lastname in lowercase is your password. If someone chose a random password of the same length as you, what is the entropy of their password?

If your lastname has *n* letters from the English alphabet, then the total possible passwords that are *n* letters long when choosing from 26 characters is:

26^n

The entropy is the number of bits needed to represent 26^n possible values, i.e.

$\log_2(26^n)$

1) Assume your firstname in lowercase is your username. All usernames are the same length as yours. A 128-bit MD5 hash is used to store passwords (no salt). Given a hash value, what is the worst case time for an attacker to find the password if can calculate 10^9 hashes per second?

There are 26^n possible passwords. A brute force attack involves calculating the hash of all of them at a speed of 10^9 per second. Hence the time in seconds is:

$26^n/10^9$

1) An attacker wants to use pre-calculated hashes to speed up password cracking. How much space is needed to store all pre-calculated values, uncompressed (no rainbow table)?

The attacker must store the 26^n possible passwords (n Bytes) and their 128-bit (16 Byte) hash. Hence the total size is:

26^n (n + 16) Bytes