Authentication is a way to prove who you are. It's like showing your ID to get into a secure area. There are three main methods:

1. **What you know**: This is something only you should know, like a password or a PIN. It's a secret you use to prove your identity.
2. **What you have**: This is something you physically possess, like an ID card or a special token. It's a piece of hardware you use to prove who you are.
3. **What you are**: This involves unique traits of your body, like your fingerprint, voice, or eye scan. It's based on your physical characteristics.

A combination of more than one type is known as multi-factor authentication.

Entropy is the measurement of a password's resistance against brute-force attack. The formula to compute entropy:

Entropy = L * log2N

Here,
L = length of a password
N = the total number of possible characters in a password

N = 26 for lowercase letters only passwords
N = 52 if a password is a combination of lowercase+uppercase letters
N = 62 if a password is a combination of lowercase+uppercase letters+digits
N = 72 if a password is a combination of lowercase+uppercase letters+digits+special characters (assuming there are 10 special characters)

Compute the entropy of the following passwords:

jelly+bread

lowercase letters = 26
Special characters = 10
Total = 26 + 10 = 36
Length of password = 11

Entropy = L * log2N
= 11 * log2(36)
= 56.9

entropy 56.9 bits

blasczwosKy

lowercase letters = 26
Uppercase letters = 26
Total = 26 + 26 = 52
Length of password = 11

Entropy = L * log2N
= 11 * log2(52)
= 62.7

entropy 62.7 bits

liverpool96ynwa

lowercase letters = 26
Digits = 10
Total = 26 + 10 = 36
Length of password = 15

Entropy = L * log2N
= 15 * log2(36)
= 77.5

entropy 77.5 bits

An **online attack** is an attack where an attacker guesses a password online. We could guard against online attacks by using a lockout policy, where after three or five or seven unsuccessful guesses, the account is locked out.

An **offline attack** is an attack where the attacker steals the password file and tries to crack the hashes offline by using a precomputed hash table. A higher entropy helps to prevent this type of brute-force guessing because it ensures that the attacker has to test more possible combinations.

A password needs to have both higher entropy and not be guessable. For example, JamesBond007 is a good password in terms of entropy but it is vulnerable against online attack as it is easily guessable.