**Why BCrypt?** Most popular password storage schemes are based on fast hashing algorithms such as **MD5** and **SHA-1**. BCrypt is a computationally expensive adaptive hashing scheme which utilizes the **Blowfish block cipher**. It is ideally suited for password storage, as its slow initialization time severely limits the effectiveness of brute force password cracking attempts. How much overhead it adds is configurable (that's the adaptive part), so the computational resources required to test a password candidate can grow along with advancements in hardware capabilities.