

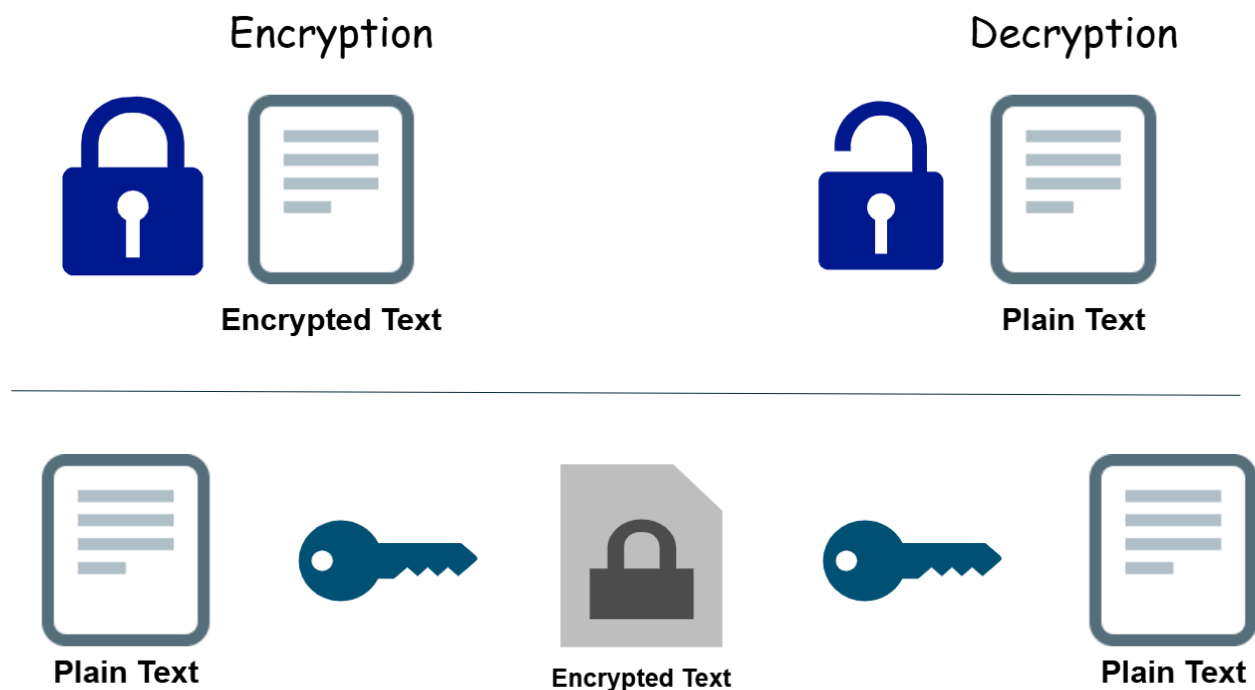
## What is Bcrypt?

### 👉 The Problem with Plain Text Passwords

When we store passwords in a database or transfer them over networks in plain text, it creates a security risk. Anyone who gains access to the database or intercepts the transfer can immediately see all passwords.

### 👉 Encryption (Two-way)\

- Encryption is like using a lock and key for your data
- You encrypt (lock) a password with a key when storing it
- You decrypt (unlock) it with the same key when verifying
- **Problem:** If someone steals the encryption key, they can decrypt all passwords



### 👉 Hashing (One-way)

- Hashing converts data into a fixed-length string of characters
- **Key difference:** Hashing is one-way - once hashed, you cannot convert back to the original
- To verify passwords: you hash what the user enters and compare the hashes
- Popular hashing algorithms include MD5 and SHA256, but they have vulnerabilities

## ➤ The Secure Solution

- **Bcrypt** is a specialized password-hashing function designed for security
- It's intentionally slow to prevent brute-force attacks
- It automatically incorporates "salt" to protect against rainbow table attacks

## 🔧 How Bcrypt Works

- When a user creates a password, Bcrypt hashes it
- The hashed result is stored in the database
- When the user tries to log in, Bcrypt hashes their entered password
- The system compares this hash with the stored hash
- If they match, the password is correct

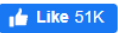
## 🔧 Bcrypt Example

You can see Bcrypt in action at <https://www.browsersling.com>

### Bcrypt Password Generator

cross-browser testing tools

World's simplest online bcrypt hasher for web developers and programmers. Just enter your password, press the Bcrypt button, and you'll get a bcrypted password. Press a button – get a bcrypt. No ads, nonsense, or garbage.

 Like 51K

**Announcement:** We just launched [Online Math Tools](#) – a collection of utilities for solving math problems. Check it out!

Password:  Rounds:

[\(undo\)](#)

```
$2a$10$8i.dYw9Uk/g88KVLSTkmf.fWuYBdPsTNB.QEUxy9q3ArGUJv  
aKI4m
```

Want to test bcrypt hashes and passwords?  
Use the [Bcrypt Hash Tester](#) tool!

- A Bcrypt hash looks like this:

`$2a$10$8i.dYW9Uk/g88KVLSTkmf.fWuYBdPsTNB.QEUxy9q3ArGUJvaKI4m`

- `$2a` indicates the Bcrypt version
- `$10` indicates the "cost factor" (number of rounds)
  - This means  $2^{10}$  (1,024) iterations, not just 10
  - More rounds = more secure but slower processing
- The rest is the salt and the hashed password combined

### 👉 Key features of Bcrypt

- Slow by design to prevent brute-force attacks
- Built-in salt protection
- Adjustable work factor to adapt to faster computers over time
- Industry standard for password security