Using mkpasswd to Generate Password Hashes

- mkpasswd is a command-line utility for generating password hashes using various cryptographic algorithms. It is part of the whois package on many UNIX-like systems and provides a simple way to create password hashes compatible with UNIX authentication mechanisms.

Basic Syntax

- The general syntax of `mkpasswd` is:

```
mkpasswd -m <algorithm> <password> -s
```

- `-m <algorithm>`: Specifies the hashing algorithm.
- `<password>`: The plaintext password to be hashed.
- `-s`: Prompts for the password securely.

Generating Password Hashes

- The following table summarizes how to generate password hashes with different algorithms:

Algorithm	Command
Yescrypt	`mkpasswd -m yescrypt mypassword -s`
bcrypt	`mkpasswd -m bcrypt mypassword -s`
SHA-256	`mkpasswd -m sha-256 mypassword -s`
SHA-512	`mkpasswd -m sha-512 mypassword -s`
MD5	`mkpasswd -m md5 mypassword -s`

Using a Custom Salt

- Most password hashing schemes require a salt to prevent precomputed attacks (rainbow tables).
- You can specify a custom salt with the -S option:

```
mkpasswd -m sha-512 mypassword -S mysalt -s
```

- Ensure that the salt meets the length and character requirements of the chosen algorithm.

Verifying Password Hashes

- To verify if a given plaintext password matches a previously generated hash, you can use the crypt(3) function in a script or programming language that supports password hashing, such as C, Python, or Go.