```
[root@4b80cd864710 mydir]# ls
mydir2  securecopy.txt
[root@4b80cd864710 mydir]# cksum securecopy.txt
2766876939 488142 securecopy.txt
```

```
[root@4b80cd864710 mydir]# cksum securecopy.txt
1396946510 488143 securecopy.txt
[root@4b80cd864710 mydir]#
```

```
[root@4b80cd864710 mydir]# cd ~/mydir/mydir2
[root@4b80cd864710 mydir2]# find /root/mydir Rakn.txt
/root/mydir
/root/mydir/securecopy.txt
/root/mydir/mydir2
/root/mydir/mydir2/Rakn.txt
/root/mydir/mydir2/yourname.tx
Rakn.txt
[root@4b80cd864710 mydir2]#
```

```
[root@4b80cd864710 mydir2]# man useradd > useradd-man.txt
[root@4b80cd864710 mydir2]# grep "password" useradd-man.txt
        The number of days after a password expires until the account is permanently disabled. A value of 0 disables the account as soon as the
        password has expired, and a value of -1 disables the feature.
        Example: -K PASS_MAX_DAYS=-1 can be used when creating system account to turn off password aging, even though system account has no password
    -p, --password PASSWORD
        The encrypted password, as returned by crypt(3). The default is to disable the password.
        Note: This option is not recommended because the password (or encrypted password) will be visible by users listing the processes.
        You should make sure the password respects the system's password policy.
        The number of days after a password has expired before the account will be disabled.
        password, and same GID).
        The maximum number of days a password may be used. If the password is older than this, a password change will be forced. If not specified, -1
        The minimum number of days allowed between password changes. Any password changes attempted sooner than this will be rejected. If not
        The number of days warning given before a password expires. A zero means warning is given only upon the day of expiration, a negative value
        Shadow password suite configuration.
        can't update password file
[root@4b80cd864710 mydir2]#
```

Grep: