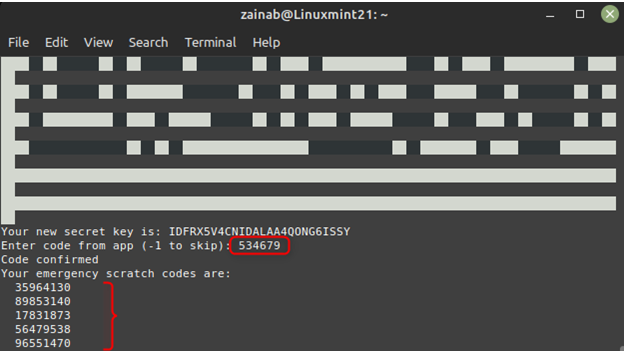
# 2-Factor Authentication

Google Authenticator is a software-based authenticator that generates codes for your accounts. It is based on 2FA (2-Factor Authentication) to ensure the security of your accounts beyond the username and passwords.

1. **You must be sure that your system has exact time (first config timedatectl)**
2. Install google authenticator : **yum install libpam-google-authenticator**
3. Run command to config it : google-authenticator



1. Configure 2FA for SSH: The next step is to modify the PAM configuration file for the SSH daemon *(/etc/pam.d/sshd*). Run the following command to open the config file:

#vim /etc/pam.d/sshd (add below line)

auth required pam\_google\_authenticator.so

if you want all users just login with convert (auth substack password-auth) to (auth substack )

1. Config sshd (/etc/ssh/sshd\_config) add below lines
   1. vim /etc/ssh/sshd\_config

KbdInteractiveAuthentication yes

ChallengeResponseAuthentication yes

AuthenticationMethods keyboard-interactive

1. restart sshd

* systemctl restart sshd