SSH सार्वजनिक कुञ्जी उत्पादन गर्ने प्रक्रिया (Generating Your SSH Public Key)

धेरै Git सर्भरहरू SSH सार्वजनिक कुञ्जीहरूको प्रयोग गरेर प्रमाणीकरण गर्छन्। प्रत्येक प्रयोगकर्ताले आफ्नो सार्वजनिक कुञ्जी प्रदान गर्नुपर्ने हुन्छ, र त्यसका लागि पहिलो चरण कुञ्जी उत्पादन गर्नु हो। यदि तपाईंको सिस्टममा पहिले नै कुञ्जी छैन भने, नयाँ कुञ्जी उत्पादन गर्नुपर्नेछ। यो प्रक्रिया सबै अपरेटिङ सिस्टमहरूमा समान हुन्छ।

# पहिले कुञ्जी जाँच गर्नुहोस्

पहिले, तपाईंले जाँच गर्नुहोस् कि तपाईंको ~/.ssh फोल्डरमा पहिले नै कुञ्जी छ कि छैन। यो फोल्डरमा निजी र सार्वजनिक कुञ्जीहरू हुन्छन्।

$ cd ~/.ssh

$ ls

authorized\_keys2 id\_dsa known\_hosts

config id\_dsa.pub

यदि तपाईंले **id\_rsa** वा **id\_dsa** जस्ता फाइलहरू र त्यससँग मेल खाने .pub एक्स्टेन्सन भएको फाइल फेला पार्नुभयो भने, त्यसले तपाईंको निजी र सार्वजनिक कुञ्जी प्रतिनिधित्व गर्छ। .pub फाइल सार्वजनिक कुञ्जी हो र बाँकी निजी कुञ्जी हो।

# नयाँ कुञ्जी उत्पादन गर्नुहोस्

यदि यी फाइलहरू छैनन् भने, तपाईंले ssh-keygen कमाण्ड प्रयोग गरेर नयाँ कुञ्जी उत्पादन गर्न सक्नुहुन्छ। यो लिनक्स/म्याकOSमा SSH प्याकेजसँगै आउँछ र विन्डोजमा Git स्थापना गर्दा उपलब्ध हुन्छ।

$ ssh-keygen -o

Generating public/private rsa key pair.

Enter file in which to save the key (/home/schacon/.ssh/id\_rsa):

Created directory '/home/schacon/.ssh'.

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in /home/schacon/.ssh/id\_rsa.

Your public key has been saved in /home/schacon/.ssh/id\_rsa.pub.

* पहिलो चरणमा, यो कुञ्जी कहाँ भण्डारण गर्ने भनेर सोध्छ। यदि तपाईंले केही परिवर्तन गर्नुभएन भने, यो ~/.ssh/id\_rsa मा भण्डारण हुन्छ।
* पासफ्रेज दिने विकल्प पनि आउँछ। यदि तपाईं पासफ्रेज राख्न चाहनुहुन्न भने, खाली छोड्न सक्नुहुन्छ। तर, पासफ्रेज राखेमा, **-o विकल्प प्रयोग गर्नुहोस्**, जसले कुञ्जीलाई बलियो ढाँचामा भण्डारण गर्छ।

# सार्वजनिक कुञ्जी पठाउनुहोस्

प्रत्येक प्रयोगकर्ताले आफ्नो सार्वजनिक कुञ्जी (id\_rsa.pub) Git सर्भरको एडमिनलाई पठाउनुपर्छ।

सार्वजनिक कुञ्जी फाइलको सामग्री यसरी हेर्न सकिन्छ:

$ cat ~/.ssh/id\_rsa.pub

सार्वजनिक कुञ्जी केही यसरी देखिन्छ:

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAklOUpkDHrfHY17SbrmTIpNLTGK9Tjom/BWDSU

GPl+nafzlHDTYW7hdI4yZ5ew18JH4JW9jbhUFrviQzM7xlELEVf4h9lFX5QVkbPppSwg0cda3

Pbv7kOdJ/MTyBlWXFCR+HAo3FXRitBqxiX1nKhXpHAZsMciLq8V6RjsNAQwdsdMFvSlVK/7XA

t3FaoJoAsncM1Q9x5+3V0Ww68/eIFmb1zuUFljQJKprrX88XypNDvjYNby6vw/Pb0rwert/En

mZ+AW4OZPnTPI89ZPmVMLuayrD2cE86Z/il8b+gw3r3+1nKatmIkjn2so1d01QraTlMqVSsbx

NrRFi9wrf+M7Q== schacon@mylaptop.local

# थप जानकारी

यदि तपाईंलाई थप जानकारी चाहिन्छ भने, GitHub को [SSH कुञ्जी उत्पादन गर्ने गाइड](https://docs.github.com/en/authentication/connecting-to-github-with-ssh/generating-a-new-ssh-key-and-adding-it-to-the-ssh-agent) हेर्न सक्नुहुन्छ।

यस प्रक्रियाले प्रत्येक प्रयोगकर्तालाई Git सर्भरमा SSH मार्फत सुरक्षित रूपमा पहुँच दिन सक्षम बनाउँछ।