
Off-Campus Access Using S/Key

In order to permit access to OwlNet or RUF accounts from off-campus computer systems, Rice uses a security system, called S/Key. This document explains how to obtain a copy of the S/Key program for an PC, Macintosh microcomputer, or UNIX machine, how to initialize S/Key (by picking a challenge string and password) and then how to use S/Key to generate one-time session passwords every time you need to access your account from a remote computer.



RICE

Table of Contents

Background on S/Key Security	3
Who needs to Use S/Key?	3
Obtaining the S/Key Calculator	3
DOS	4
Macintosh	4
UNIX	4
Initializing S/Key	4
Connecting to Rice	4
Connecting with S/Key	6
S/Key Service Policy	6
Long Distance Account Access	6
Problems or Questions	7
Faculty, Staff, and Graduate Students:	7
Undergraduates:	7

**If you have any
comments or
suggestions about
this document, send
them to
problem@rice.edu
via electronic mail.**

Background on S/Key Security

The S/Key system is a security method that was established to ensure that OwlNet and RUF user passwords are not transmitted in clear text across potentially insecure networks on their way to Rice. This measure is taken to prevent system security compromises, while at the same time allowing OwlNet users to get to their accounts from remote sites. Note: S/Key password sharing will result in permanent account termination.

The passwords generated by the S/Key program are “one-time” passwords that change from one use to the next, and are based on a challenge string provided by the S/Key login program and the user's S/Key password. The use of these “one-time” passwords prevents system compromises resulting from stolen passwords since all passwords expire immediately, so that risk is minimized if one is stolen on an insecure network.

If you have any feedback about the S/Key system, send electronic mail to director@owlnet.rice.edu. If you have any questions about the use of the program beyond the procedures covered in this document, contact the Consulting Center at 713.348.4983, or stop by 103 Mudd Lab.

S/Key password sharing will result in permanent account termination.

Who needs to Use S/Key?

You need to use S/Key if you are connecting to OwlNet or RUF from a computer network outside of Rice. However, if you are connecting to Rice from the Rice modem pool (from the 713 numbers or from the 800 number), you are connecting directly to Rice and will **not** need to use S/Key.

Note: S/Key is the only approved method for connecting to OwlNet from remote sites. Attempts to circumvent the S/Key system are a violation of OwlNet policy.

You **will** need to use S/Key if:

- If you have a computer at home, but want to connect to your OwlNet or RUF account while you are attached to a different Internet Service Provider (like AOL, Compuserve or Prodigy).
- If you are at another university and are logged in via an account at that university and want to access your OwlNet or RUF account.

You **will not** need to use S/Key if:

- If you have a computer at home and are connecting to Rice via the Rice modem pool (via a Charon or Lethe account).
- If you are out of state and are connecting to Rice via Rice's 800 number or one of the (713) numbers (making a long-distance call), because you are connecting directly to Rice.

Obtaining the S/Key Calculator

The S/Key calculator is available for DOS, Macintosh, and UNIX platforms. There is also a web calculator that can be used with a Java capable browser such as Netscape (version 3.x) or Internet Explorer. Connect to URL:

`http://www.ruf.rice.edu/skey/` or `http://www.owlnet.rice.edu/skey/`

If you can use the web S/Key calculator, you should do that. It will work for both OwlNet and RUF, but you must **be sure to select the button for MD4 calculation.**

Otherwise, using ftp you can transfer the calculator program from the ftp site, **ftp.rice.edu**. If you need help with ftp, call the Consulting Center, 103 Mudd Lab **713.348.4983**.

To download the software on a Mac use Fetch to login to **ftp.rice.edu** and log in as **anonymous** and password **userid@rice.edu** where *userid* is your userid.

To download the software on a PC running Windows open Internet Explorer and go to

```
ftp://ftp.rice.edu
```

Once you are connected, change into the directory

```
/skey.
```

Once there, you will notice that there are 3 sub-directories, `unix`, `dos`, and `mac`. Change into the appropriate sub-directory for the type of machine with which you will be using S/Key.

DOS

In `dos` directory you will find several files: `ctkey.exe`, `key.exe`, `keyapp.exe`, `popkey.exe`, `termkey.exe`. All of the programs are for DOS except **keyapp.exe**, which is for Windows. Of these DOS programs, **ctkey.exe** is the easiest to use. (`Ctkey.exe` is a memory resident program. Before you begin your session, you need to run `ctkey` and choose a hotkey. Later, when connecting, you will be able to press that hot key, type your S/Key password and the S/Key challenge string, and `ctkey` will automatically enter your password for you.) Download in binary mode the file is appropriate for you.

Macintosh

The `mac` directory contains a file called **skey+.sit.hqx**. This file is binhex encoded and it is a Stuffit™ archive. In order to expand this file to its usable form, you will need Stuffit Expander™, which is free. To obtain a copy of Stuffit Expander™, you can download one from Aladdin Systems website <http://www.aladdinsys.com> or any other Internet Macintosh software archive.

UNIX

The following binary files are located in the `unix` sub directory: `skey.linux` for Linux, `key.sunos` for SunOs, `key.next` for NextStep, `key.rs6k` for RS/6000, `key.solaris` for Solaris, and the source code, `skey.src.tar`.

Initializing S/Key

Before you can use S/Key the first time, you must set your S/Key password. **This must be done while you are at Rice. Once you are at the remote site, it is too late.** This password should *not* be the same as your login password for your OwlNet account. It need not be long or complex - 6 to 8 characters is sufficient. It should be memorable, but not easily guessed. You will need an S/Key calculator to complete the setup. If you do not have S/Key software installed on your computer (or on the computer you will be connecting from at the remote site) you may use the Java S/Key calculator by pointing your Java capable web browser at <http://www.owlnet.rice.edu/skey>.

Connecting to Rice

1. Log in to **snowy.owlnet.rice.edu**. You can do this by SSHing from a workstation, compute server, Mac, or PC. For example,

```
short-eared% ssh snowy.owlnet.rice.edu
```

Note for RUF users: You should connect to **fence.ruf.rice.edu** via SSH.)

2. Once you have authenticated to snowy (or fence for RUF users) with your unix username and password issue the command **keyinit -s**.

```
snowy% keyinit -s
```

3. You will be prompted for your OwlNet (or RUF) unix password. Enter it and hit <return>.

4. You will be asked to enter a sequence count from 1 to 10000. This number will be the first half of your “challenge string” and will decrement by one each time you connect. When it reaches -1 you will no longer be able to log on and will have to reset the counter by repeating the S/Key setup procedure. A sequence count of 999 is probably sufficient for most users.

```
Enter sequence count from 1 to 10000: 999
```

5. You will be asked to enter a key. **This will not be your password and you will not have to remember it.** It is merely the second part of the challenge string. The program will suggest a default key. If you wish to use that key, you may just press <return> at the prompt. Otherwise, you may enter a series of letters and numbers (6 to 8 characters) and hit <return>.

```
Enter new key [default csaST1X]: flumph5
```

6. The program will output your challenge string.

```
s/key 999 flumph5
```

7. At this point you will need to use your S/Key calculator and will pick your password. Into the “Challenge” field of the calculator you will type (or copy and paste) the challenge string. In our example, this would be “999 flumph5”. Into the “Secret Password” field you will type the password you wish to have (6 to 8 characters, easy to remember, not easy to guess.) **This is the password you will have to remember.** Finally, if you have an option to compute with MD4 or compute with MD5 (as you do on the Java S/Key Calculator) be sure to select “**compute with MD4.**”

8. The S/Key calculator will generate a string of six short English words. This string is your one-time password. For example,

```
APE HOLD PUSH CANE PUB SANG
```

9. Return to the keyinit program running on snowy.owlnet. It should be showing a prompt that looks like

```
s/key access password:
```

Type in (or copy and paste) the six words from the S/Key calculator's One Time Password field and hit <return>. Make sure to get the complete string. The result will look something like this

```
s/key access password: APE HOLD PUSH CANE PUB SANG
```

10. The keyinit program will output a verification that will look something like this:

```
ID username s/key is 999 flumph5
```

```
Next login password: APE HOLD PUSH CANE PUB SANG
```

It is important to have the MD4 hash algorithm selected in the S/Key program instead of MD5, if the choice is presented.

11. You have successfully initialized your S/Key password. Note that you never tell snowy your password directly. You only tell snowy the one-time password that your secret password generates. Log out of snowy.

Connecting with S/Key

Connecting with S/Key is straightforward and easier than the setup procedure.

1. Connect to **snowy.owlnet.rice.edu** via SSH. (RUF users should connect to `fence.ruf.rice.edu`.)
2. Enter your username and password and press <return>.
3. You will be presented with a challenge string that looks something like this:

```
s/key 998 flumph5
```

4. Type (or paste) the challenge string into your S/Key calculator. Note: the “s/key” is not part of the challenge. In our example the challenge string is “998 flumph5.”
5. Type your secret S/Key password into the S/Key calculator. Generate the one-time password, being sure to “compute with MD4.”
6. The S/Key calculator will generate a list of short capitalized words. These words are your one time password and you need to enter them at the password prompt on snowy. If you would like to see the words as you type or paste them, press <return> at the Password: prompt, and you will get a new prompt (as in the example below).

```
login: janedoe
s/key 998 flumph5
(s/key required)
Password: (echo on)
Password: EAR CAST FURY KNEE BORN BELT
```

If you do not press <return> at the initial password prompt, the six words will not be displayed, making it more difficult to enter them correctly. Note that the one-time password is case sensitive, and must be entered exactly as it appears in the S/Key program.

7. You are now logged in to Owlnet (or RUF). If you wish to use another Owlnet compute host, such as **forest.owlnet.rice.edu** or **jungle.owlnet.rice.edu** you may reach them by typing

```
ssh forest
```

at the snowy prompt.

S/Key Service Policy

S/Key password sharing will result in permanent account termination. Password sharing puts the system at risk to security break-ins.

Long Distance Account Access

Please contact your divisional representative by phone if you are not in the Houston area, do not have a terminal server account, and need access to your account via S/Key. A list of divisional representatives is available at <http://www.rice.edu/Computer/facultystaff.html>. If you are unable to contact your representative you can contact the Consulting Center in Mudd 103 at 713.348.4983.

Problems or Questions

Faculty, Staff, and Graduate Students:

If you have a problem, contact your divisional representatives by sending an e-mail message to problem@rice.edu detailing your question. Your query is examined by a staff dispatcher for severity and assigned to the appropriate staff. This is the most effective communication method since computing support staff are often working in the field and unreachable by phone. In addition, the dispatcher is aware of who is on vacation or out ill.

Undergraduates:

If you have a problem, contact your computing support representative by sending an e-mail message to problem@rice.edu detailing your question. Your query is automatically assigned to your College Computing Associate (CCA).

If you need immediate assistance during normal business hours, you can call the Consulting Center at 713.348.4983. During the semester, the Consulting Center has limited evening and weekend hours as well.

To report emergencies, which are urgent system-wide problems (i.e.: all Wiess' network connections are down or all the PCs in a lab are non-functional), contact the Operations Center at 713.348.4989. Staff work 24 hours a day, 365 day a year and can page appropriate administrators for major network or computing problems.

More information is available at <http://www.rice.edu/Computer/student.html>