An Introduction to SSH

SSH Keys & SSH Config

Adam Batten
Cookies ‘n’ Code

Secure SHell (SSH)

Secure SHell (SSH)

SSH is a secure way to access another computer.

Secure SHell (SSH)

SSH is a secure way to access another computer.

```
[~] ssh abatten@ozstar.swin.edu.au
```

Secure SHell (SSH)

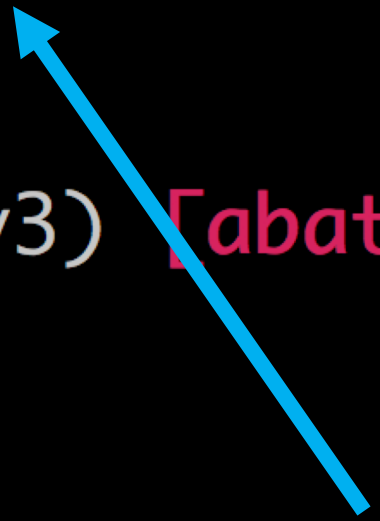
SSH is a secure way to access another computer.

```
[~] ssh abatten@ozstar.swin.edu.au

(py3) [abatten @ farnarkle1] [~]
```

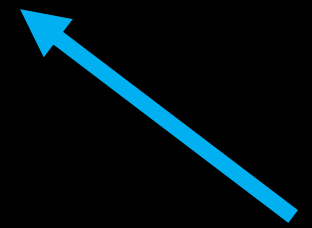
Secure SHell (SSH)

SSH is a secure way to access another computer.

```
[~] ssh abatten@ozstar.swin.edu.au

(py3) [abatten @ farnarkle1] [~]
```



This prompt interacts with my local machine



This prompt interacts with Ozstar

Why should I care about SSH Keys?

Why should I care about SSH Keys?

PASSWORDS ARE ANNOYING!

Why should I care about SSH Keys?

PASSWORDS ARE ANNOYING!

- Remembering passwords
- Typing your password everytime you SSH
- Typing your password everytime you copy via SSH
- Your password might not even be secure

Why should I care about SSH Keys?

PASSWORDS ARE ANNOYING!

- Remembering passwords
- Typing your password everytime you SSH
- Typing your password everytime you copy via SSH
- Your password might not even be secure

SSH Keys removes the need to enter passwords whilst still being secure

Why should I care about SSH Keys?

PASSWORDS ARE ANNOYING!

- Remembering passwords
- Typing your password everytime you SSH
- Typing your password everytime you copy via SSH
- Your password might not even be secure

SSH Keys removes the need to enter passwords whilst still being secure

Setting this up once will actually save you lots of time in the future.

Setting up SSH Keys for Ozstar

Setting up SSH Keys for Ozstar

Step 1: Generate a SSH key pair

```
ssh-keygen -t rsa
```

Setting up SSH Keys for Ozstar

Step 1: Generate a SSH key pair

```
ssh-keygen -t rsa
```

Step 2: Copy public key to Ozstar

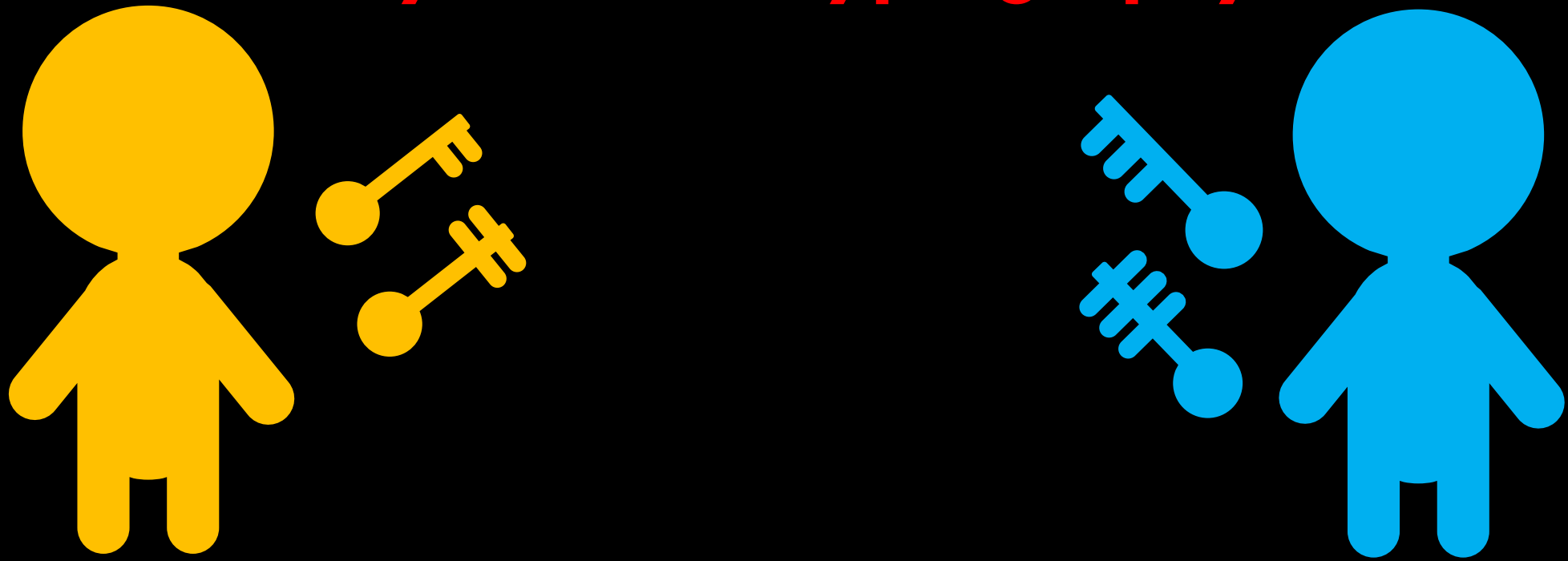
```
ssh-copy-id user@ozstar.swin.edu.au
```

(You may need to install ssh-copy-id although most have it by default.)

How do SSH Keys work?

How do SSH Keys work?

Asymmetric cryptography



How do passwords work?

Hash Functions

How do passwords work?

Hash Functions $\Longrightarrow$ "One Way" Function

How do passwords work?

Hash Functions ⟹ **“One Way” Function**

badpassword1 ⟹ DFCD345452ED879e

How do passwords work?

Hash Functions ⟹ **“One Way” Function**

badpassword1 ⟹ DFCD345452ED879e

Example:

Square root a number 3 times remove the decimal point, 0’s and 8’s then use the first 5 numbers.

27164 **24534** **23796**

How do passwords work?

Hash Functions ⟹ **“One Way” Function**

badpassword1 ⟹ DFCD345452ED879e

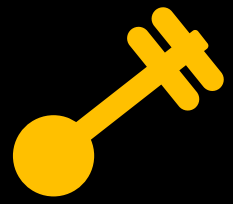
Example:

Square root a number 3 times remove the decimal point, 0’s and 8’s then use the first 5 numbers.

27164	**24534**	**23796**
3584	**1313**	**4207**

How do SSH Keys work?

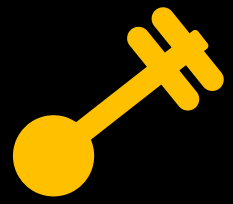
Public



Private

How do SSH Keys work?

Public



Private

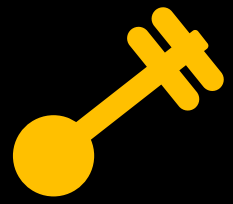
These keys “undo” each other in a mathematical operation.

Anything encrypted with one is decrypted with the other.

How do SSH Keys work?

Public

These keys “undo” each other in a mathematical operation.



Private

Anything encrypted with one is decrypted with the other.

Example:

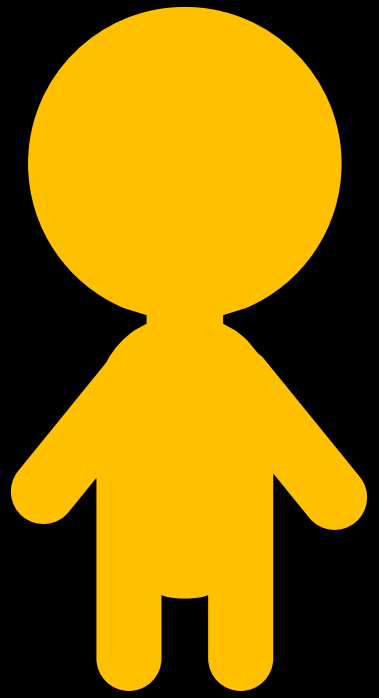
Say the ‘encryption’ process is to multiply by a number.

Then 3 and 1/3 could be key pairs.

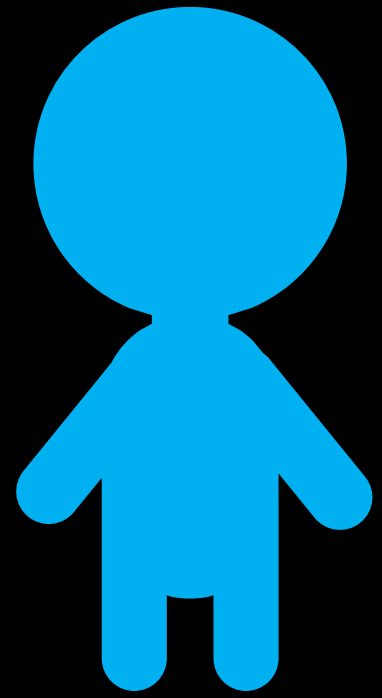
$$(3 \times y) \times \frac{1}{3} = \left(\frac{1}{3} \times y\right) \times 3 = y$$

How do SSH Keys work?

YOU

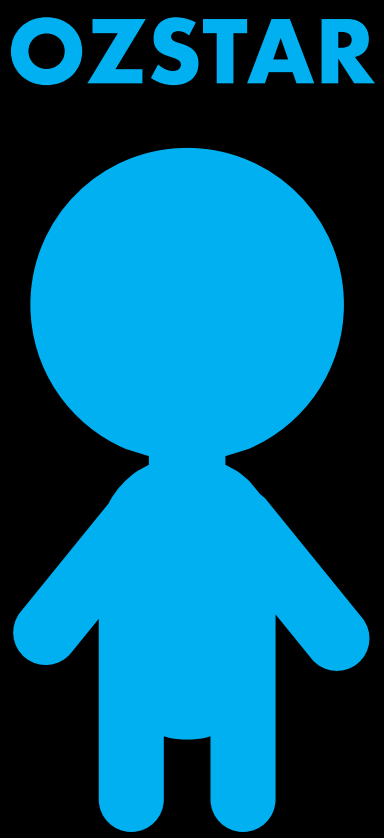


OZSTAR



Step 1: Generate a SSH key pair

```
ssh-keygen -t rsa
```



Setting up SSH Keys for Ozstar

Step 1: Generate a SSH key pair

```
ssh-keygen -t rsa
```

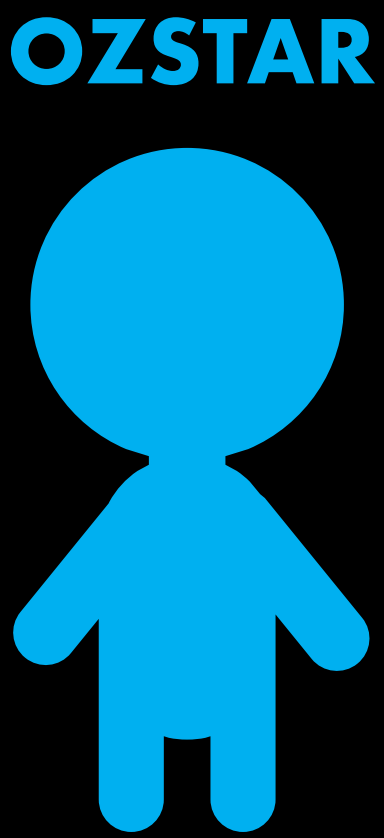
Step 2: Copy public key to Ozstar

```
ssh-copy-id user@ozstar.swin.edu.au
```

(You may need to install ssh-copy-id although most have it by default.)

Step 1: Generate a SSH key pair

```
ssh-keygen -t rsa
```

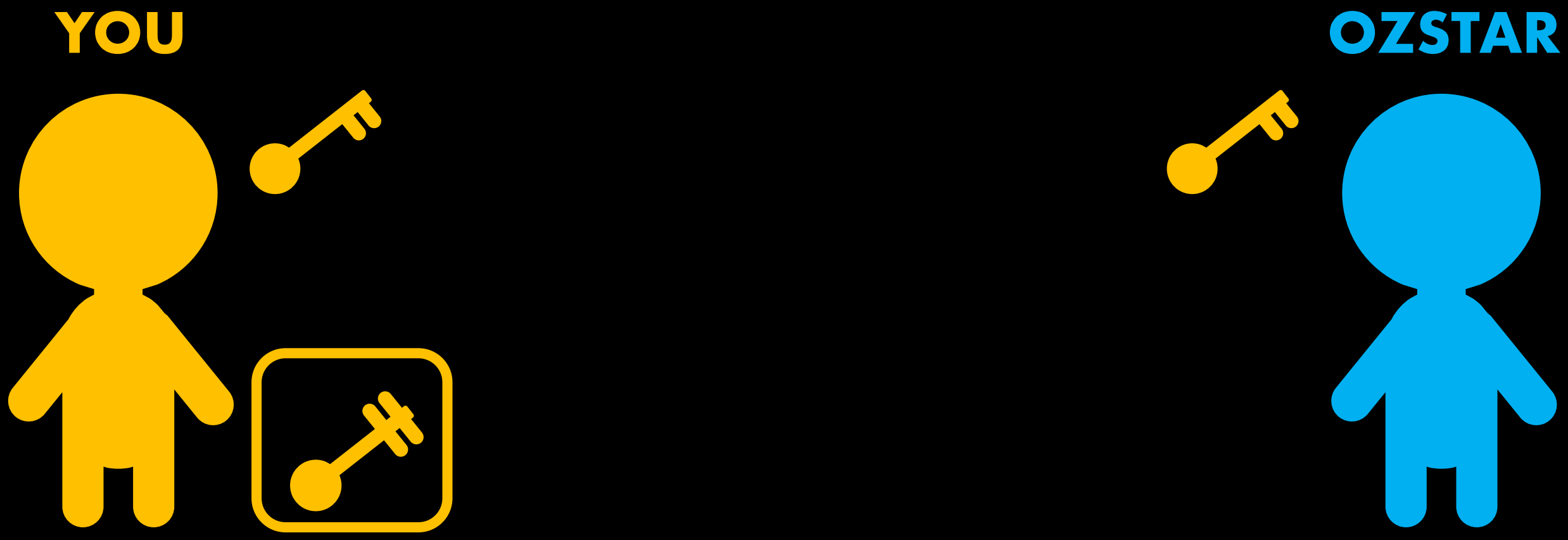


Step 1: Generate a SSH key pair

```
ssh-keygen -t rsa
```

Step 2: Copy public key to Ozstar

```
ssh-copy-id user@ozstar.swin.edu.au
```



Setting up SSH Keys for Ozstar

Step 1: Generate a SSH key pair

```
ssh-keygen -t rsa
```

Step 2: Copy public key to Ozstar

```
ssh-copy-id user@ozstar.swin.edu.au
```

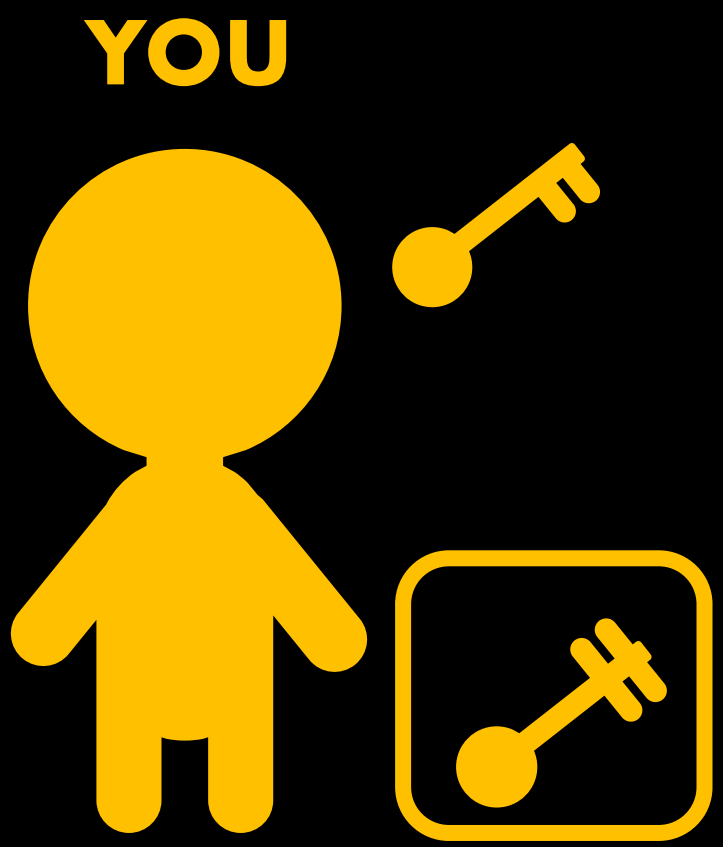
(You may need to install ssh-copy-id although most have it by default.)

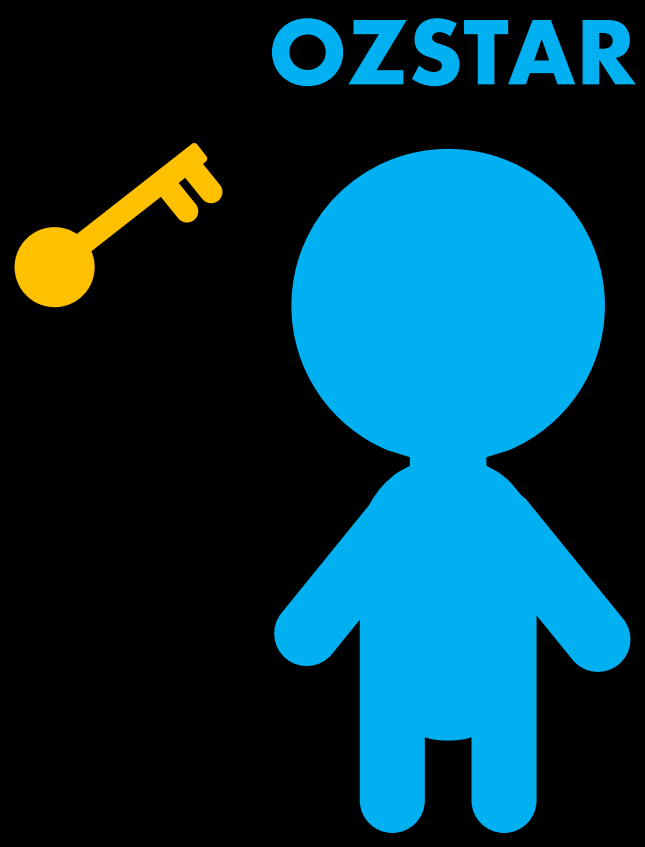
YOU

OZSTAR

Attempt to login to Ozstar

```
ssh user@ozstar.swin.edu.au
```





Attempt to login to Ozstar

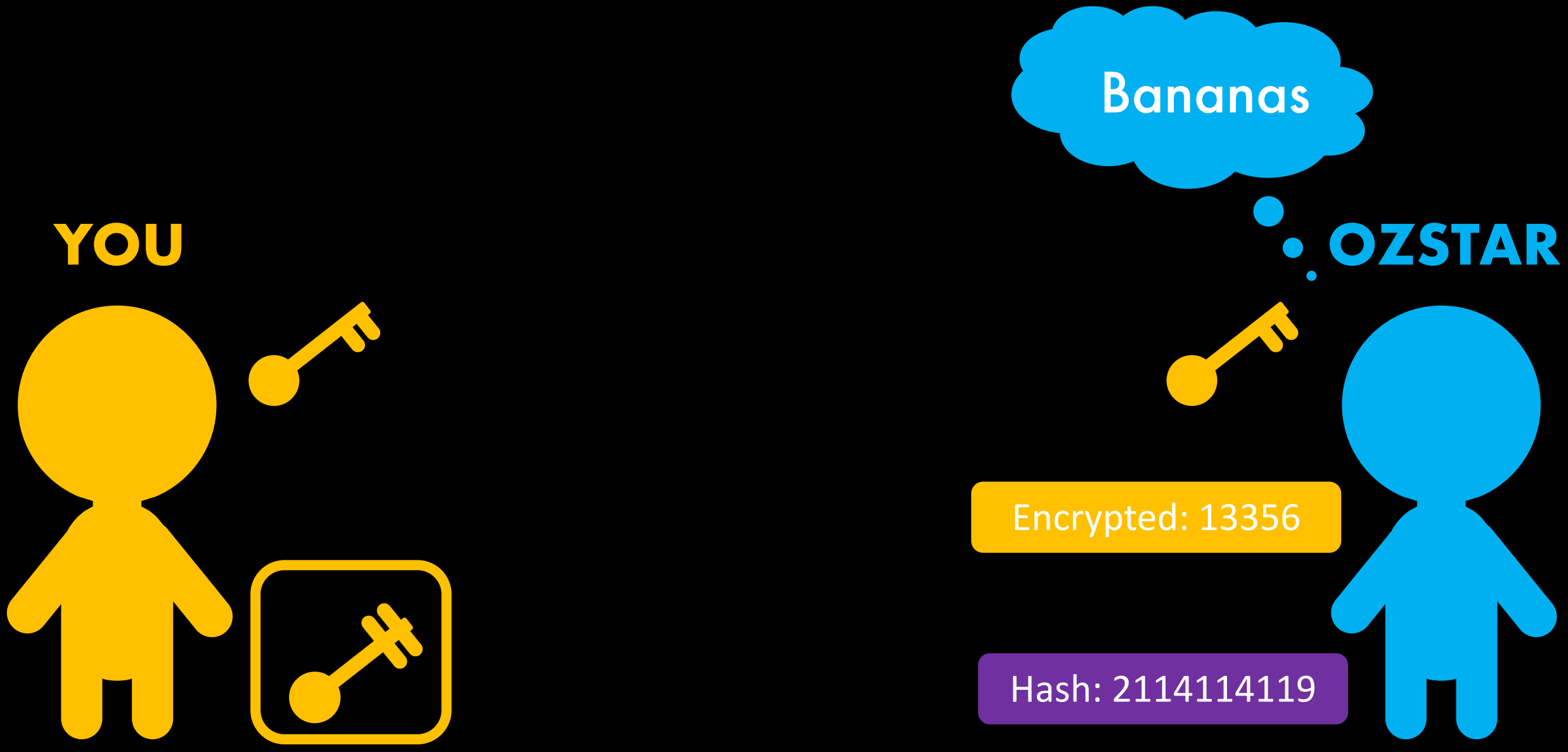
```
ssh user@ozstar.swin.edu.au
```

Attempt to login to Ozstar

```
ssh user@ozstar.swin.edu.au
```

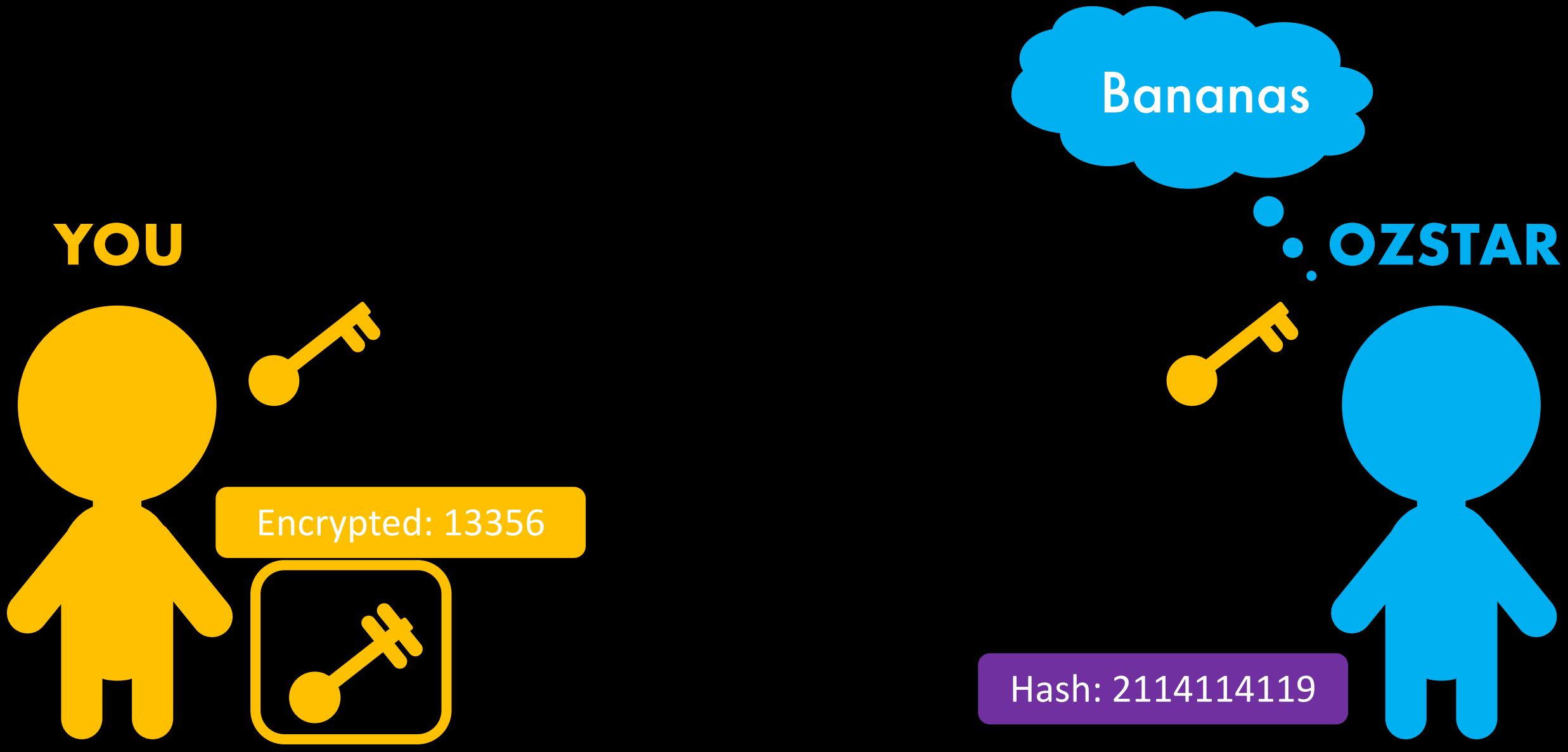
Attempt to login to Ozstar

```
ssh user@ozstar.swin.edu.au
```



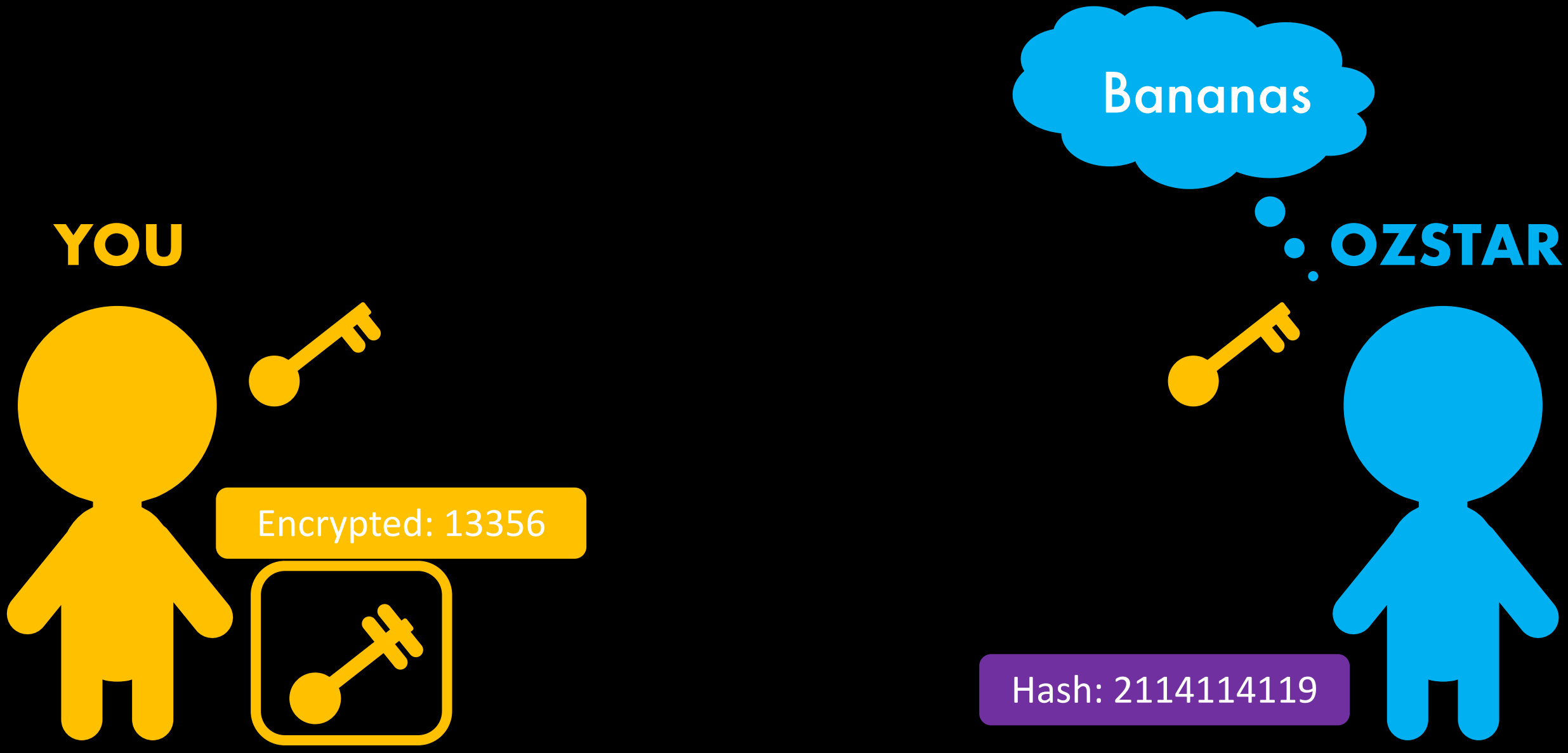
Attempt to login to Ozstar

```
ssh user@ozstar.swin.edu.au
```



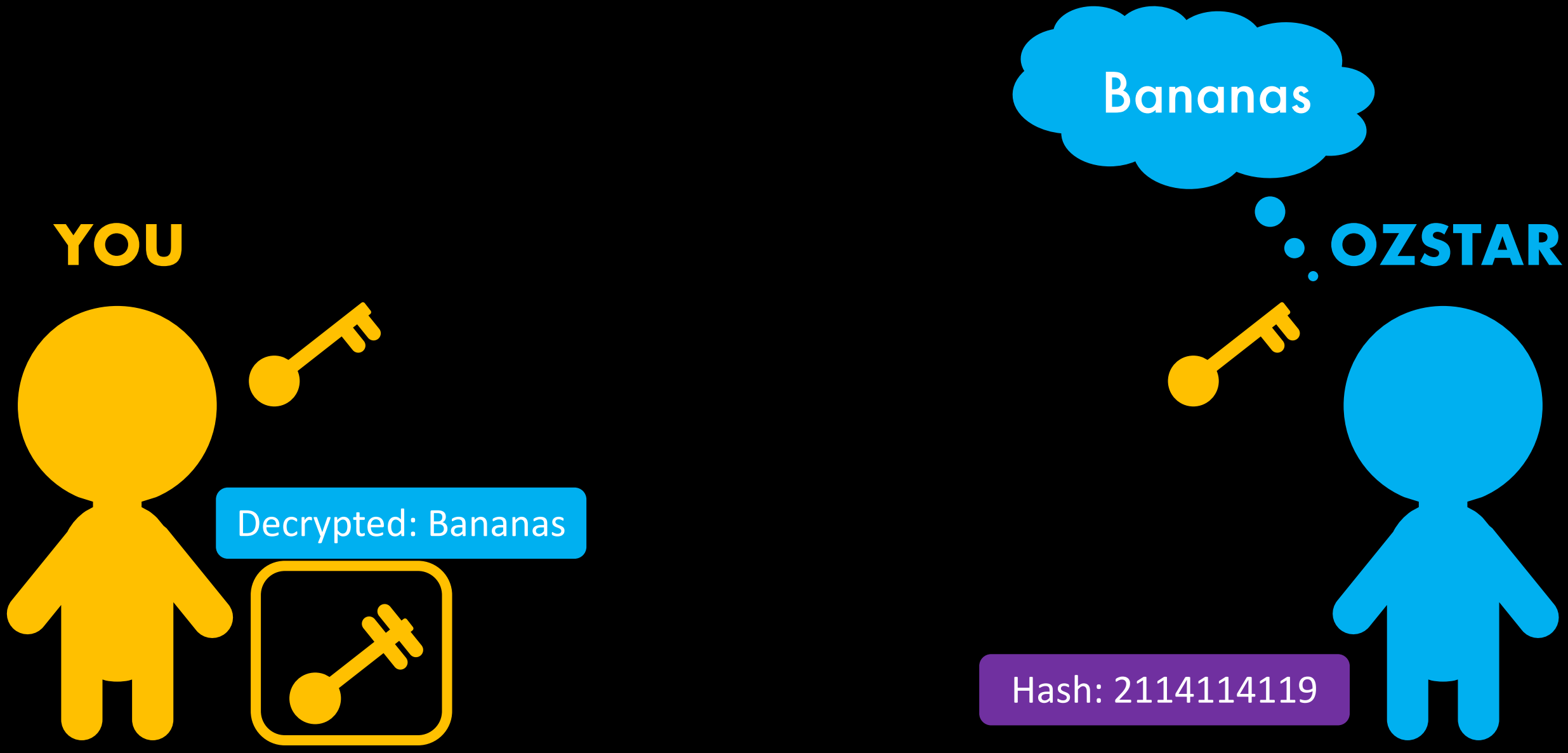
Attempt to login to Ozstar

```
ssh user@ozstar.swin.edu.au
```



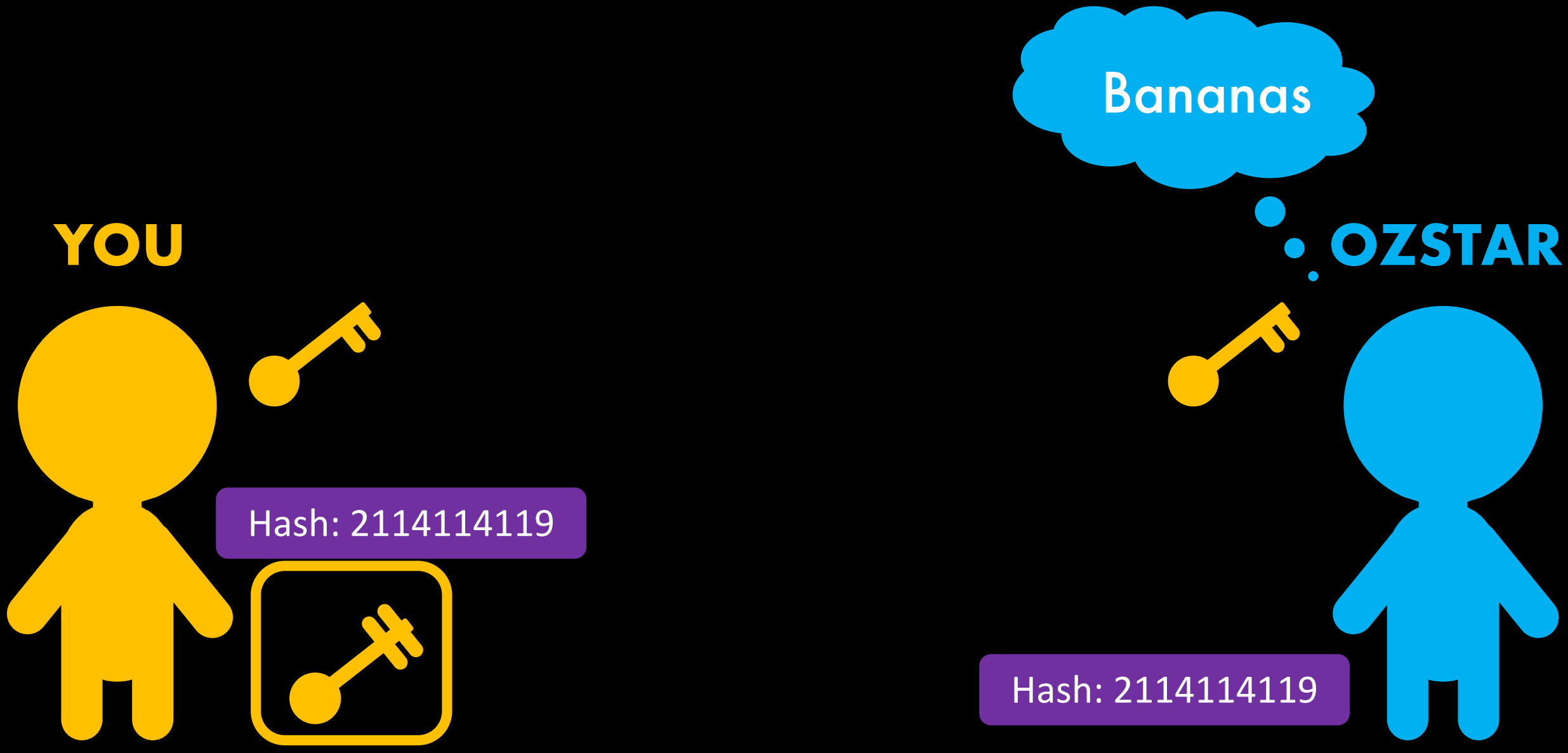
Attempt to login to Ozstar

```
ssh user@ozstar.swin.edu.au
```



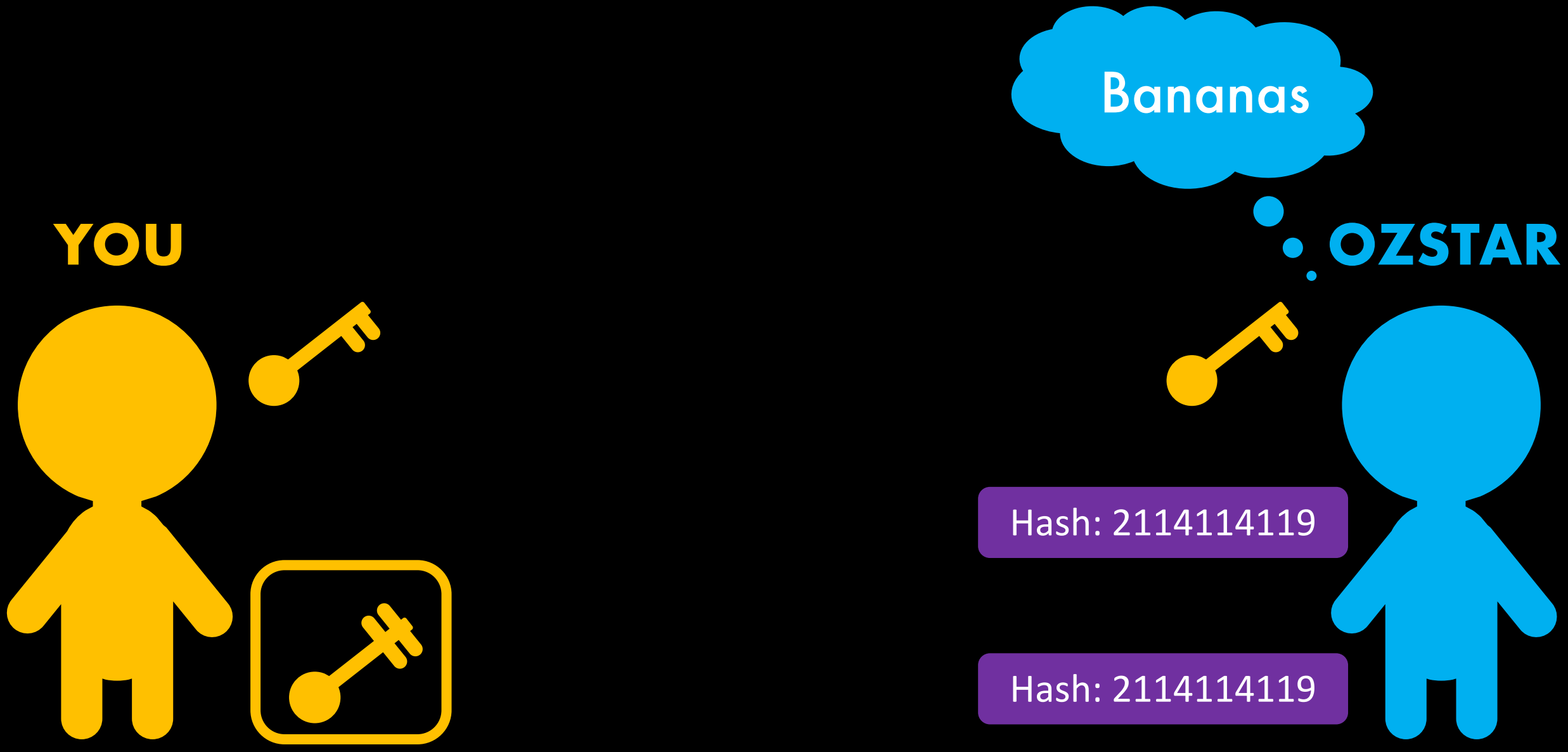
Attempt to login to Ozstar

```
ssh user@ozstar.swin.edu.au
```

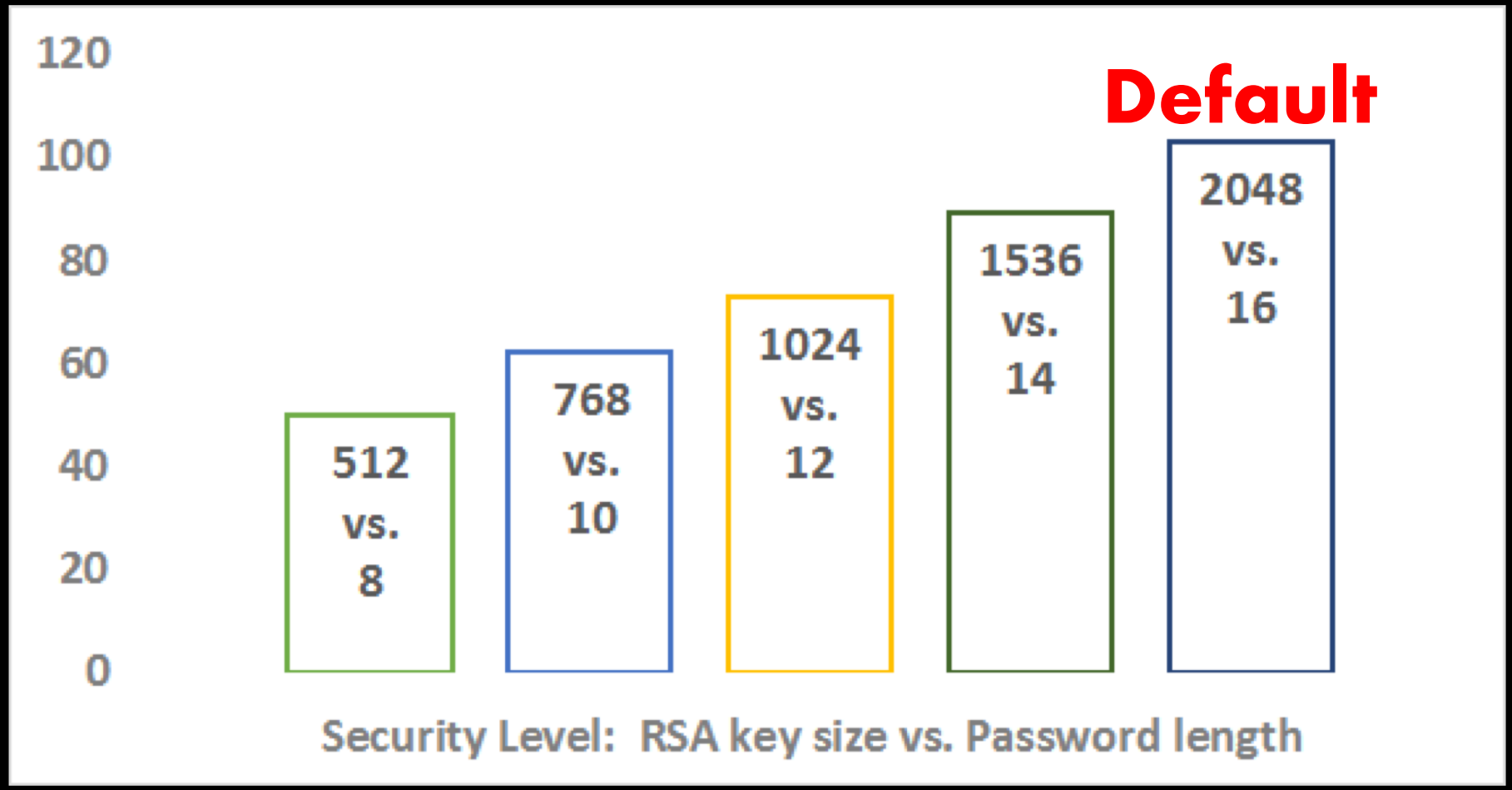


Attempt to login to Ozstar

```
ssh user@ozstar.swin.edu.au
```

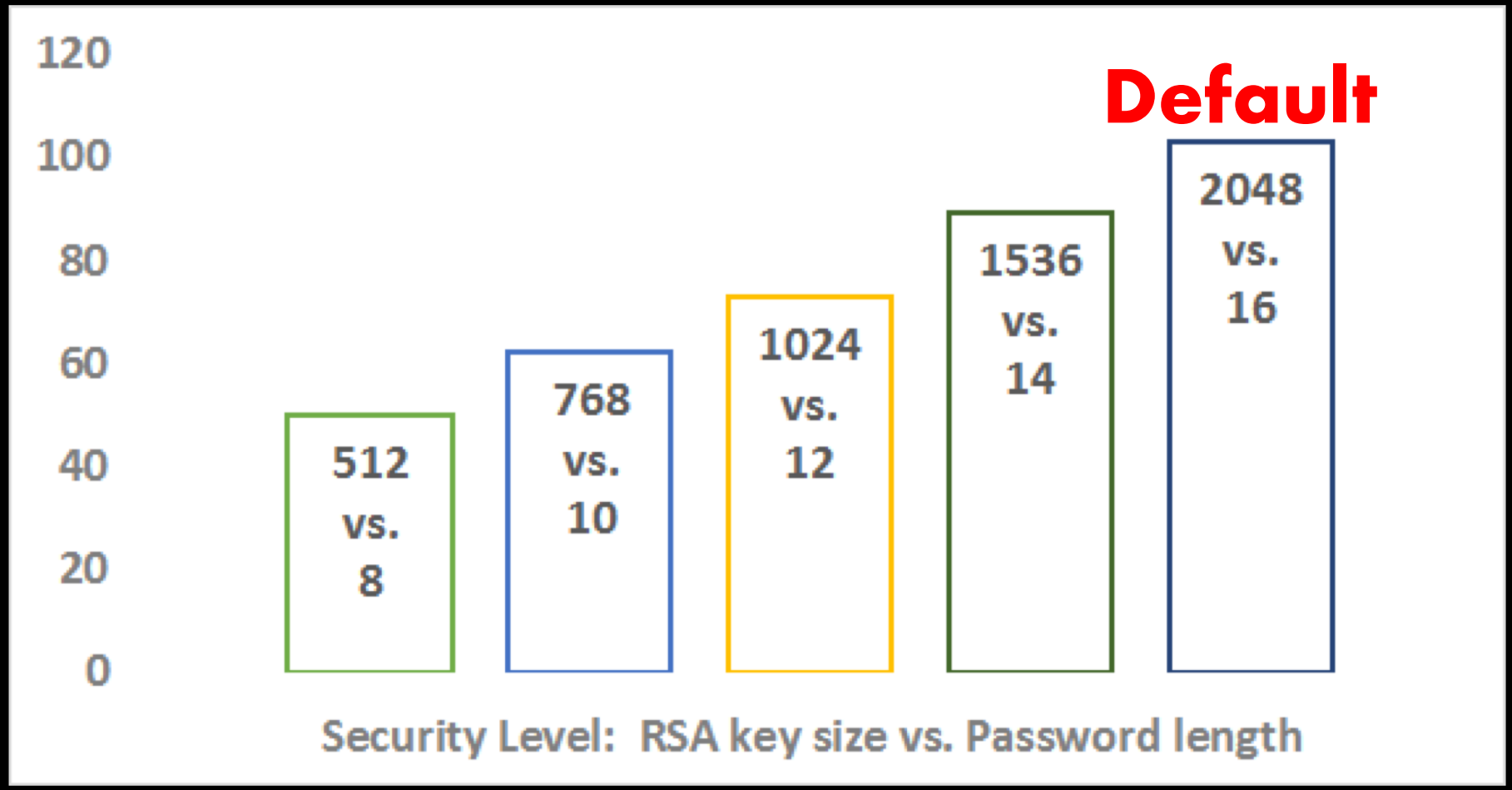


How strong are SSH keys?



The default ssh key is as strong as a 16 character password.

How strong are SSH keys?



The default ssh key is as strong as a 16 character password.
i.e."safe" until around 2030

SSH Config

SSH Config

```
[~] cd .ssh/
[~/.ssh] ls
config  id_rsa  id_rsa.pub  known_hosts
[~/.ssh]
```

SSH Config

```
[~] cd .ssh/
[~/.ssh] ls
config   id_rsa   id_rsa.pub   known_hosts
[~/.ssh]
```

Inside your .ssh folder you should see 4 files:

1. `config` — This is your ssh config file
2. `id_rsa` — This is your private key (DO NOT SHARE THIS!)
3. `id_rsa.pub` — This is your public key
4. `known_hosts` — This is a list of known places you ssh

SSH Config

Your SSH config contains the settings for everything when you SSH into a remote server.

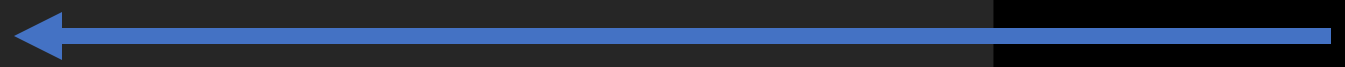
```
Host firsthost
    SSH_OPTION_1 custom_value
    SSH_OPTION_2 custom_value
    SSH_OPTION_3 custom_value

Host secondhost
    SSH_OPTION_1 custom_value
    SSH_OPTION_2 custom_value
    SSH_OPTION_3 custom_value
```

SSH Config

```
1  Host oz
2    Hostname ozstar.swin.edu.au
3    User abatten
4    ForwardX11 yes
5    ServerAliveInterval 300
6
7  Host raijin
8    Hostname raijin.nci.org.au
9    User ab3463
10   ForwardX11 yes
```

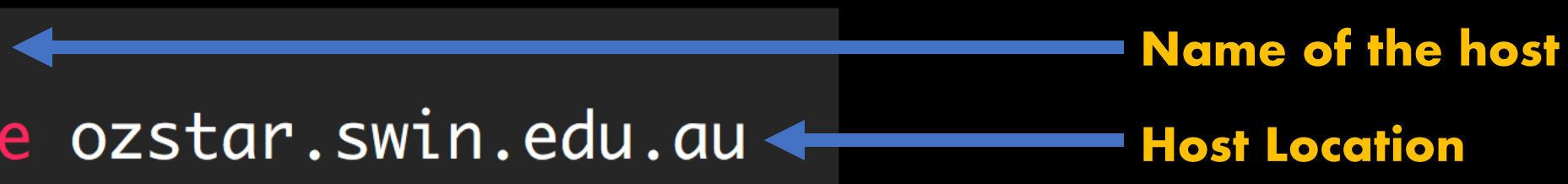
SSH Config

```
1  Host oz
2    Hostname ozstar.swin.edu.au
3    User abatten
4    ForwardX11 yes
5    ServerAliveInterval 300
6
7  Host raijin
8    Hostname raijin.nci.org.au
9    User ab3463
10   ForwardX11 yes
```



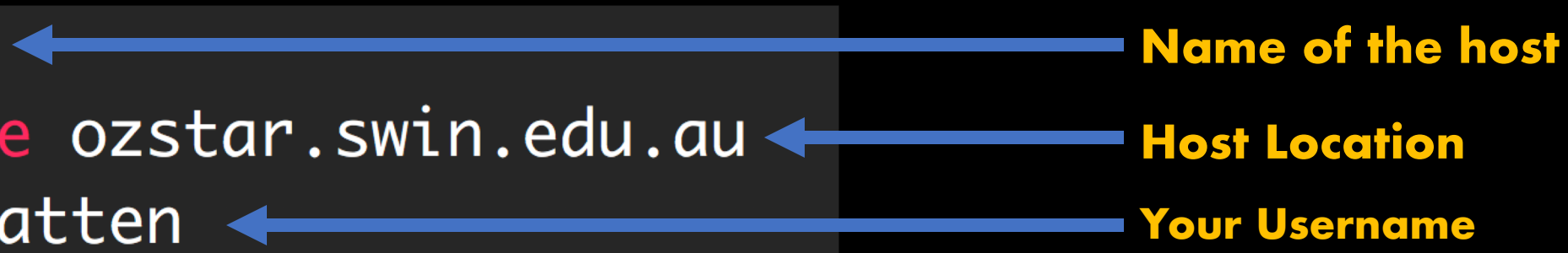
SSH Config

```
1  Host oz
2    Hostname ozstar.swin.edu.au
3    User abatten
4    ForwardX11 yes
5    ServerAliveInterval 300
6
7  Host raijin
8    Hostname raijin.nci.org.au
9    User ab3463
10   ForwardX11 yes
```



SSH Config

```
1  Host oz
2    Hostname ozstar.swin.edu.au
3    User abatten
4    ForwardX11 yes
5    ServerAliveInterval 300
6
7  Host raijin
8    Hostname raijin.nci.org.au
9    User ab3463
10   ForwardX11 yes
```



SSH Config

```
1  Host oz
2    Hostname ozstar.swin.edu.au
3    User abatten
4    ForwardX11 yes
5    ServerAliveInterval 300
6
7  Host raijin
8    Hostname raijin.nci.org.au
9    User ab3463
10   ForwardX11 yes
```

SSH Config

Without SSH Config

```
[~] ssh abatten@ozstar.swin.edu.au -X -Y
```

SSH Config

Without SSH Config

```
[~] ssh abatten@ozstar.swin.edu.au -X -Y
```

Using SSH Config

```
[~] ssh oz
```