

Message Prompts

✂ Cut these up and put them in a hat.

Cool snowflake

Painting of a person
in a hat

Photo of a wild horse

An article about bees

Map of Center City Philly

Photo of the sky

Audio file of a jungle bird

A comic strip

A blue horse

A zine about DIY skills

Illustration of a vegetable

Drawing of a rainbow

Birthday cake with a
cartoon character

A public domain novel

Photo of a carnival ride

Poem about a dog

Cute aliens

Graffiti you admire

Something you
consider cozy

Drawing of planet Earth

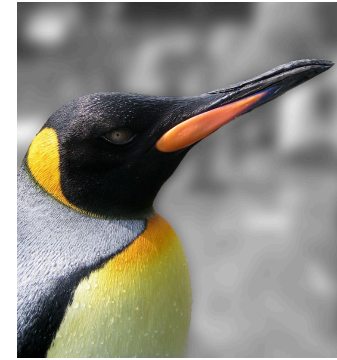


Photo CC-BY-SA Mark Dickson

Linux Lab: E-Z Command-Line Encryption

Iffy Books | 404 S. 20th St., PHL | iffybooks.net

① Find a partner

For this exercise you'll be exchanging encrypted messages with a partner, so find someone you want to work with.

② Choose a passphrase

We recommend using a passphrase with four or more randomly selected words.

You can use the Diceware list to generate random words. Simply roll a 6-sided die 5 times and look up the corresponding word:

https://www.eff.org/files/2016/07/18/eff_large_wordlist.txt



Write down a copy of the passphrase for each of you.

③ Pick something to send

Choose a message prompt from the hat, such as "photo of the sky." Do a web search and find something to send, then save the file to your Downloads folder.

If you're sending a short piece of text, you can create a plaintext file from the command line like so:

```
cd ~/Downloads
```

```
echo "My secret message ❤️" > plaintext.txt
```

④ Encrypt your file

Open a terminal window and **cd** to your Downloads folder.

```
cd ~/Downloads
```

Use an **OpenSSL** command like the one below to encrypt your file.

Replace **plaintext.txt** with the name of your file. (If the filename contains spaces, try putting it in double quotes.)

The backslash at the end of the first line below indicates that the command continues to the next line. We're using it here because the command is too wide to fit on the page; you can omit it.

```
openssl aes-256-cbc -a -in plaintext.txt \  
-out ciphertext.txt
```

The **-a** option selects Base64 format for the ciphertext output. Base64-formatted data uses a subset of 64 printable alphanumeric characters.

⑤ Exchange files with your partner

Use a USB flash drive or a short-term file locker like <https://hostb.org> to exchange encrypted files with your partner.

⑥ Decrypt the message from your partner

Save the file from your partner to your Downloads folder. Run the following command in the terminal to decrypt it, replacing **ciphertext.txt** with the name of the file.

```
openssl aes-256-cbc -d -a -in ciphertext.txt \  
-out plaintext_out.txt
```

🎉 Great job!