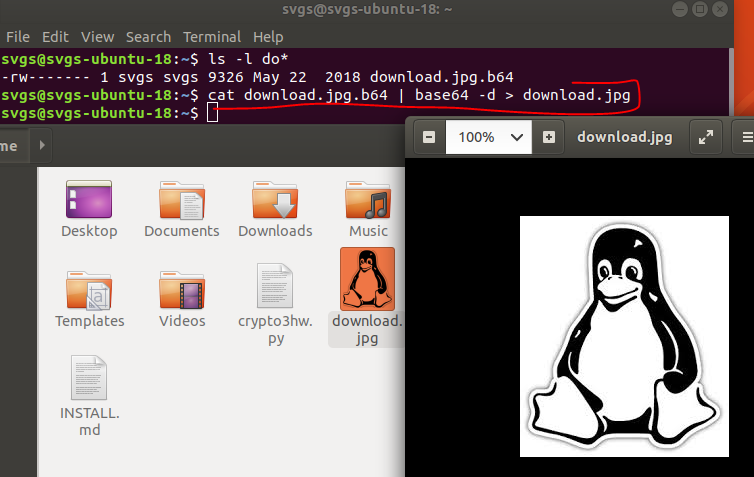
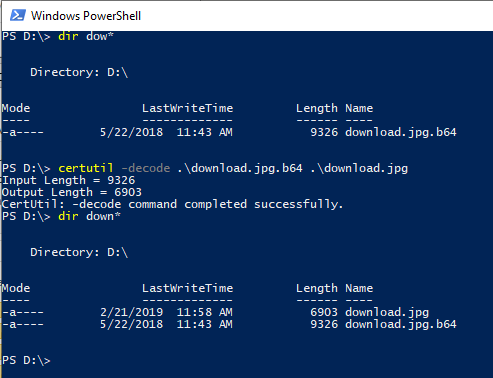
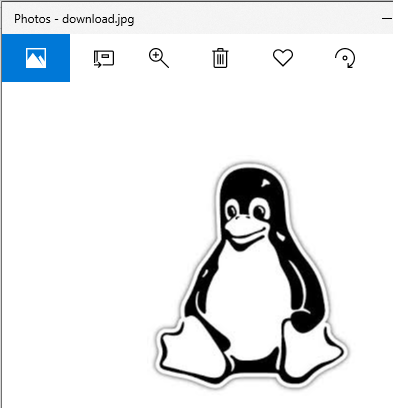
# Cryptography Homework 1 Key

## For Turn in

1. The file, document.jpg.b64 is a Base64 encoded file. Decode it and describe the picture. The base64 app on Linux is easiest. In Windows you can use certutil.exe or PowerShell.  
     
     
   I show answers using Linux, Windows’ certutil.exe, and PowerShell. The students only need to do one.

Linux is easiest (at least for me.)  
cat download.jpg.b64 | base64 -d > download.jpg  


In Windows, certutil.exe is also easy.  
certutil -decode download.jpg.b64 download.jpg

This is the file download.jpg, opened from FileExplorer.  


This code works in PowerShell. The “[Convert]::FromBase64String” is a call to .Net.  
$b64Text = Get-Content("D:\download.jpg.b64")  
$decodedBytes = [Convert]::FromBase64String($b64Text)  
$decodedBytes | Set-Content download.jpg -Encoding Byte 

1. Alice decides on a key, and then whispers the key into Bob’s ear. What kind of encryption are they using, most likely? (Symmetric or asymmetric, 50/50 chance.) Suppose Eve is in the room and may be able to overhear what Alice whispers. How can Alice and Bob improve their key exchange?

They are probably using a symmetric algorithm, since Alice must give the key to Bob.

The purpose of this question was just to get the students thinking about the key exchange problem. In later lessons we’ll talk about using public key encryption to securely (almost) exchange keys. Here, the answer about how to improve the key exchange could be almost anything.