Updates

• Lab 1 part 1 due TOMORROW at 5:00 PM!
• Lab 1 final due on Friday the 20\textsuperscript{th} at 5:00 PM.
• Miles’ office hours next week will be moved.
  – Expect an email with specific time/location.
• Reminder:
  – Current Event and Security Review are both due by April 27\textsuperscript{th} at 5:00 PM.
  – Each week that goes by you give up 1 extra credit point.
Lab 1 Notes/Hints

• When running gdb, be sure to do the commands in the appropriate order:
  – catch exec
  – r
  – b foo
  – c
• The ‘r’ MUST be before you create the break points otherwise you get a seg fault.
• Make sure you don’t bog yourself down on one sploit. If you’re stuck, move on to another one.
• sploit4 is not necessarily harder than sploit3.
• Don’t procrastinate with sploits4-7. They are much harder.
What is this?
It’s a Scytale!

• Used by ancient Greeks and Spartans.
Security Through Obscurity
What is this?
Caesar Cipher (or shift cipher)

- Used by ancient Romans (first recorded use by Caesar).
- In April 2006, fugitive Mafia boss Bernardo Provenzano was captured in Sicily partly because some of his messages, written in a variation of the Caesar cipher, were broken. Provenzano's cipher used numbers, so that "A" would be written as "4", "B" as "5", and so on.
Upgraded Shift Cipher

• Plaintext: ABCDEFGHIJKLMNOPQRSTUVWXYZ
• Cipher: ZEBRASCDFGHIJKLMNOPQTUVWXY

• Adds an extra level of security on top of Caesar Cipher.
Vigenère Cipher - 1467
Vigenère Cipher

Plaintext: ATTACKNOW
Key: LEMONLEMO
Cipher: LXFOPVEFR

• Used by the Confederate army during the Civil War.
• Consistently cracked....
• They liked to use the keys: “ManchesterBluff”, “CompleteVictory”, and “ComeRetribution”