1. cpacpactfJulius
   1. PROMPT: ‘Hcbg’ gq hsqr ‘Kmli’ gl PMR13, gql’r gr? Uygr, lm, rfyr’q ‘Xzyv’. Yjqm, rfc djye gq hsqr\_y\_uypksn{nnjeiIqD}
   2. HINT: Et tu, Brute?
   3. ROT3 -- [Caesar Cipher](http://www.xarg.org/tools/caesar-cipher/)
   4. ANSWER: just\_a\_warmup{pplgkKsF}
2. Stegono-saurus
   1. PROMPT: RAWR! No, just kidding. Let’s get down and read some great sociology. [A fascinating read in sociology](https://www.pactf.com/static/ctfproblems/ee5ee44b-bd07-4882-87d3-4082f8a1056d/Steg.32354ef5c46a.txt)
   2. HINT: Wait!! Is that a mistake there?
   3. Stenography
   4. ORIGINAL:  
      <https://archive.org/stream/essaysonsociolog00mann/essaysonsociolog00mann_djvu.txt>
   5. DIFFERENCE:  
      <https://www.diffchecker.com/ibu7thcc>
   6. Encoding issues account for weird ascii substitutions?
      1. Fix: <https://support.google.com/news/answer/61689?hl=en>
         1. They tried to fuck u up by switching it to a old on
   7. ADJUSTED DIFFERENCE WITH FIX:
      1. <https://www.diffchecker.com/ovuudvh3>
      2. THE FLAG IS STEGISCOOL!
   8. ANSWER: STEGISCOOL!
3. Intercepted ZIP
   1. PROMPT: We intercepted [a ZIP file](https://www.pactf.com/static/ctfproblems/581dca54-c4ee-4eca-ab44-e0a793dcf11a/intercepted.163a30aefb90.zip) that looks important.
   2. HINT: You may need to crack the password. But try to make the guesses educated, okay?
   3. I used John the Ripper (1.8.0-jumbo-1 OS X) and zip2john to crack the ZIP password
      1. <http://www.openwall.com/john/>
      2. Using zip2john, I retrieved the hash for the ZIP file
      3. Using John the Ripper, I used brute-force to check combinations with the hash
      4. The password to the ZIP file is (minus “”): “soylamejor”
      5. The flag (below) is found inside the file flag.txt
   4. ANSWER: Sazi3K4BwNU0pjRujeFYNxjNY
4. Dropped the file!
   1. PROMPT: Ah! Noo! I dropped my file!! It’s all scrambled now! Can you help me fix it? I left something in there for you![whoops!](https://www.pactf.com/static/ctfproblems/4811cb3b-055f-4240-87ab-5df8fe854003/Dropped%20a%20file!!.f7f97be1a5a2.dmg)
   2. HINT: Is this corrupted, damn!
   3. When using *file* in OS X, I get: “VAX COFF executable not stripped - version 25741” but it doesn’t help at all. Compressed .dmg?
   4. ANSWER:
5. Surfing Keys
   1. PROMPT: An agent in a tough spot managed to get to a terminal and quickly type in the password to RoboCorp’s new website, but alas! It wasn’t his computer, and the message seems jumbled up: qwfpgjurtypkyybrsvypaespyyir
   2. HINT: Look down. To your fingers. Look closely, and see the infinite number of possibilities for your keys, and find the right one.
   3. keyboard? There are a lot of ‘y’s
   4. ANSWER:
6. Too Much Resistance
   1. PROMPT: Black, blue, red, white!!! AHHHH! TOO MANY [COLORS!](https://www.pactf.com/static/ctfproblems/ede604fd-56bb-47eb-badf-6d662e2da7d6/colors.4353f7d93faa.txt)!
   2. <http://www.hobby-hour.com/electronics/resistorcalculator.php>

|  |  |  |  |
| --- | --- | --- | --- |
| Brown Brown Brown | 111 | ~~110~~ |  |
| Brown Black Yellow | 10 | ~~100~~ |  |
| Brown Black White | 10 | ~~-~~ |  |
| Brown Brown Brown | 111 | ~~110~~ |  |
| Brown Black Yellow | 10 | ~~100~~ |  |
| Brown Black White | 10 | ~~--~~ |  |
| Brown Brown Brown | 111 | ~~110~~ |  |
| Brown Black Yellow | 10 | ~~100~~ |  |
| Brown Black White | 10 | ~~--~~ |  |
| Brown Brown Blue | 11 | ~~11000000~~ |  |
| Brown Black Yellow | 10 | ~~100~~ |  |
| Black White Violet | 0 | ~~--~~ |  |
| Brown Brown Blue | 11 | ~~11000000~~ |  |
| Brown Brown White | 11 | ~~--~~ |  |
| Black White Violet | 0 | ~~--~~ |  |
| Brown Brown Green | 11 | ~~1100000~~ |  |
| Black White Violet | 0 | ~~--~~ |  |
| Brown Black Red | 10 | ~~1~~ |  |
| Brown Brown Violet | 11 | ~~110~~ |  |
| Brown Brown Black | 110 | ~~11~~ |  |
| Brown Brown Black | 110 | ~~11~~ |  |
| Brown Red Brown | 1 | ~~--~~ |  |
| Brown Brown Brown | 11 | ~~110~~ |  |
| Brown Brown Black | 11 | ~~11~~ |  |
| Brown Black Brown | 101 | ~~100~~ |  |

* 1. Tried getting binary from ohms, but didn’t work. (see middle column)
  2. HINT: What could they possibly mean?
  3. ANSWER:

1. You are a square
   1. PROMPT: It is a simple fact. If you want to solve this one, you gotta think like a [square](https://www.pactf.com/static/ctfproblems/9d01642f-0d57-400a-9a08-85a8071ee336/But_a_flipped_square.25c461a2ba47.txt).
   2. HINT: Be the **square**, invert your square!
   3. Some kind of square cipher?
   4. Some letters are kept there, and only some are changed?
   5. MESSAGE: For You Are A Square, the â€™ should be an apostrophe (’). Thank you.
   6. ANSWER:
2. Blaise de Infiltration
   1. PROMPT: Psst! It’s the monkey. I managed to steal some data from EvilCorp, but I had to book it before they caught me, so I didn’t have time to break it… At any rate, I’ve left the file for you [da-message](https://www.pactf.com/static/ctfproblems/acab3e6b-e8c9-4e49-a2ef-f8a301653d68/message.0c383ffad274.txt), so you should take a look at it when you get the chance. They mentioned it being some kind of french cipher from the 1500s, but then they were also talking about some turkish snack food in World of Warcraft, or something… Beats me.
   2. HINT: What’s the opposite of a Variant Beaufort?
   3. I used a vigenere cipher tool - I forgot the link…
      1. guballa.de/vigenere-solver????
   4. I entered the message provided into the tool to guess the encryption phrase: TOPKEK
   5. It also decrypts the message.
   6. Copy / Paste into a doc, use Find to search “flag”
   7. ANSWER: monkeyseemonkeydo
3. Lost Keys
   1. PROMPT: Hey, I’m Cameron Wong. I had a flag ready for you, but it seems that it’s locked away somewhere, and I’ve lost my keys… What I do have, though, is a [door](https://www.pactf.com/static/ctfproblems/e019b6b0-7e7f-4301-a457-14dc0219ecf3/door.df8630f732be.txt), maybe you can try getting into that?
   2. HINT: If your first instinct was to google my name and/or my username, you’re barking up the wrong tree! I’m way more narcissistic than that! Also, I hate typing spaces in keys, that’s just annoying.
   3. ANSWER:
4. Got Bits
   1. PROMPT: Ha-ha! I’ve encrypted it! With RSA! There’s no way you can get it now! [daSecret.](https://www.pactf.com/static/ctfproblems/214ae345-a893-42c1-b349-99dbcdfada4a/DaSecret.5461447ab629.txt)
   2. HINT: 512? Hope you started this problem early…
   3. MESSAGE: Got Bits is a solvable problem, but we would recommend that you start it extremely early in your timer, and work on other problems in the meantime. Don’t spend too much effort on it unless you have solved the other problems.
   4. Encrypted Message: Bjq7VTGKxF0+LiURUaXeB3CkCH71h16Dte88+SXnV/5f8JGMjyq/uLa1+AOZdRdWt2pQr18OZGUKniI5mx3p9w==
   5. RSA Public Key
      1. Original: MFswDQYJKoZIhvcNAQEBBQADSgAwRwJAYt+So56cdUWqe4kxjbBEyIuILWixN9T1tu4UiUVNhZMBU+5jXhq9G15BnMFtQ/7I7R1ksX2r9uDkuX1AKkqHkQIDAQAB
      2. Modulus:
         1. (hexadecimal) 62DF92A39E9C7545AA7B89318DB044C88B882D68B137D4F5B6EE1489454D85930153EE635E1ABD1B5E419CC16D43FEC8ED1D64B17DABF6E0E4B97D402A4A8791
         2. (decimal) 5178416544031690165845022236333913379644656355100034764044486334987809565683609021702601575779688934586761302716638309236782067258376606092039939961816977
      3. Exponent:
         1. (decimal) 65537
   6. I tried using GMP-ECM but stopped after ~3000 curves - no factors yet
   7. ANSWER:
5. Not-So-Random Randomness
   1. PROMPT: I’ve strengthened my RSA now! Now you got noo chance! [Encrypted.txt](https://www.pactf.com/static/ctfproblems/6492169c-939c-405f-9476-7d02f6cf3a03/encrypted.7422a7465ea2.txt)
   2. HINT: With this ‘completely’ random seed from my old debian. This 2048-bit RSA key is unbreakable.
   3. ANSWER:
6. Phillips Decryption Service
   1. PROMPT: Welcome to the PA decryption service! You can decrypt any message that was encrypted using [this key](https://www.pactf.com/static/ctfproblems/61641ee7-8ed5-4b32-8fff-eea35bd6f123/pub.a82ac1b8c0d1.pem)! Don’t bother trying to decrypt our [flag](https://www.pactf.com/static/ctfproblems/61641ee7-8ed5-4b32-8fff-eea35bd6f123/message.6813971fc864.txt), though, there’s no way you could ever get that! Oh, if you’re wondering, the server source can be found [here](https://www.pactf.com/static/ctfproblems/61641ee7-8ed5-4b32-8fff-eea35bd6f123/server.095732396454.py) nc 198.211.110.148 59292
   2. HINT: I wonder if we could just math out a way to get the original message?
   3. ANSWER:
7. Point-Slope Encryption
   1. PROMPT: We uncovered these [weird numbers](https://www.pactf.com/static/ctfproblems/44d5b155-d798-4384-98e6-aa2b1a03a1c4/points.c4344870fa17.txt) from Dr. Miles’ secret folder, but we don’t know what to do with it! Can you help us? We also found [this script](https://www.pactf.com/static/ctfproblems/44d5b155-d798-4384-98e6-aa2b1a03a1c4/encrypt.aede7dca64d0.py) and [this data](https://www.pactf.com/static/ctfproblems/44d5b155-d798-4384-98e6-aa2b1a03a1c4/handout.a5a82eb989d3.txt) in the same place, if it helps.
   2. HINT: That ‘s’ function seems like it does something familiar…
   3. ANSWER: