**Cryptography:**

1. Our officers have obtained password dumps storing hacker passwords. After obtaining a few plaintext passwords, it appears that they are all encoded using different number bases.
   1. 01000100 00110001 01110110 00110001 01101110 00110001 01110100 01111001
   2. 0x426174746c334672306e744949
   3. UGF0aCAwZiBFeGlsZQ==
   4. 83 107 121 114 105 109
2. In order to make text more easily encrypted, it is essential to transform it into some sort of numeric state. A simple way to do this is by taking letters, transforming them into numbers by their place in the alphabet ( a -> 1, b -> 2, c -> 3, and so on), “ ” going to 27, and “\_” going to 28. For instance, the string “bad ” would go to the numbers (2,1,4,27). A program to automate this will make things vastly easier for you. Can you decrypt the flag?

(23, 5, 12, 12, 27, 20, 8, 5, 27, 6, 12, 1, 7, 27, 9, 19, 27, 8, 9, 4, 4, 5, 14, 27, 8, 5, 18, 5, 27, 2, 21, 20, 27, 6, 9, 18, 19, 20, 27, 23, 5, 27, 8, 1, 22, 5, 27, 19, 15, 13, 5, 27, 20, 5, 24, 20, 27, 20, 15, 27, 3, 15, 14, 6, 21, 19, 5, 27, 25, 15, 21, 27, 14, 15, 23, 27, 20, 8, 5, 27, 6, 12, 1, 7, 27, 9, 19, 27, 9, 14, 27, 6, 1, 3, 20, 27, 19, 5, 3, 18, 5, 20, 19, 28, 1, 18, 5, 28, 8, 9, 4, 4, 5, 14, 28, 9, 14, 28, 20, 8, 9, 19, 28, 12, 9, 19, 20, 27, 4, 15, 14, 20, 27, 9, 14, 3, 12, 21, 4, 5, 27, 20, 8, 5, 27, 16, 1, 18, 20, 19, 27, 20, 8, 1, 20, 27, 1, 18, 5, 27, 19, 5, 16, 5, 18, 1, 20, 5, 4, 27, 23, 9, 20, 8, 27, 19, 16, 1, 3, 5, 19)

1. Crpyto can often be done by hand, here’s a message you got from a friend, llkjmlmpadkkc with the key of thisisalilkey.
2. The one time pad can be cryptographically secure, but not when you know the key. We've given you the encrypted flag, key, and a table to encrypt UFJKXQZQUNB with the key of SOLVECRYPTO. Can you use the table below to solve it?



1. Our officers have obtained password dumps storing hacker passwords. After obtaining a few plaintext passwords, it appears that some sort of shift cipher was used.
   1. APY-FUVSG-4237
   2. UJS-ZOPMA-8931
2. Our officers have obtained password dumps storing hacker passwords. See if you can crack them.
   1. .-.. .. ..-. . / .. ... / .-- .... .- - / .... .- .--. .--. . -. ... / .-- .... . -. / -.-- --- ..- .----. .-. . / -... ..- ... -.-- / -- .- -.- .. -. --. / --- - .... . .-. / .--. .-.. .- -. ... .-.-.- / -. -.-. .-.. -....- -.- - -... -....- ....- --... ..--- ...-- .-.-..
3. Our officers have obtained an encrypted message. The forensics team was able to find a file that contains the string, "private" which was used to encrypt the message. Take it from here and obtain the plaintext message.
   1. Wrkfs4Iyej zzqnihkmy smeila ppweiv nmof @peyi1. Io kiefvne. Brxkqvtx Tarv W.

**Python:**

1. Find the last nine digits of the sum of the sequence of numbers created by appending the first n fibonacci numbers, where n ranges from 1 to 50. (The Fibonacci Sequence begins with 1, 1, 2 for the purpose of this problem.) For instance, here are the first few appended Fibonacci numbers:

1, 11, 112, 1123, 11235, 112358, 11235813, ...

You should be adding up the first 50 of these.

1. Create a program that asks the user to enter their name and their age. Print out a message addressed to them that tells them the year that they will turn 100 years old.

Extra: Add on to the previous program by asking the user for another number and printing out that many copies of the previous message. (*Hint:* [*order of operations*](http://www.mathsisfun.com/operation-order-pemdas.html) *exists in Python*)

Print out that many copies of the previous message on separate lines. (*Hint: the string "\n is the same as pressing the ENTER button*)

1. Can you decode the following string dGg0dF93NHNfczFtcEwz from base64 format to ASCII?
2. Keith’s friend wants to get a pizza. When Keith asked their friend what topping he should get, their friend wrote the following code down on a napkin, and told them that the solution would be his favorite topping. See if you can help Keith break the code.

import java.util.Scanner;

public static void main(String[] args)

{

Scanner s = new Scanner(System.in);

String input = s.next();

if(input.length() != 9)

{

System.out.println("WRONG: try again! ");

input = s.next();

}

else

{

String solution = change1(change2(input));

if(solution == "djckktjbq")

System.out.println("The flag is: " + input);

else

{

System.out.println("WRONG: try again! ");

input = s.next();

}

}

}

public static String change1(String w)

{

int[] vary = {4, 3, 5, 6, 1, 2, 3, 3, 1};

char[] temp = new char[9];

for(int i = 0; i < 9; i++)

{

temp[i] = (char)(w.charAt(i) + vary[i]);

}

return new String(temp);

}

public static String change2(String w)

{

int[] vary = {1, 7, 5, 3, 5, 4, 2, 6, 3};

char[] temp = new char[9];

for(int i = 0; i < 9; i++)

{

temp[i] = (char)(w.charAt(i) - vary[i]);

}

return new String(temp);

}

1. Given two integer numbers return their product. If the product is greater than 1000, then return their sum

**Password Cracking:**

1. Officers have obtained password dumps storing hacker passwords. After obtaining a few plaintext passwords, it appears that they overlap with the passwords from the **rockyou** breach.
   1. 8549137cd494c22ae87eef3e18a46986
   2. 0f96a320a8c0bf7e3f6d375b0d9d3a4c
   3. 1a8cb8d148b513dfa1d285077fc4e3fb
   4. 22a313110bf5b84c0a58eecc27deaa30
2. Our officers have obtained password dumps storing hacker passwords. It appears that they are all in the format: "SKY-KAIT-" followed by 4 digits. Can you crack them?
   1. c38d29e8899455c85ee03d11abbd262b
   2. ff8f9efad5c9f106ac39e5290d810c91
   3. 425206344bd204933a38236b715c498f
   4. ab37c335e51b2855cb5a11ca89041733
   5. 82dcf30f8c7c8d4f23961f7e0c1d3cee

**Social Engineering:**

Phishing Quiz [Game](https://phishingquiz.withgoogle.com/) - Solutions will be after each question!

<https://phishingquiz.withgoogle.com/>

**Networking**

1. Note: Read all instructions completely and carefully before proceeding.

Go to the website: <http://gaia.cs.umass.edu/wireshark-labs/alice.txt>.

Right click and select the save as option to save the file, “alice.txt,” on your computer.

Then go to this site:

<http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html>

and using the Browse function, find the file on your computer. Do not upload the file yet.

At this point, start a Wireshark packet capture. After the packet capture has begun, return to your browser and click to upload the file. After the congratulations message appears on the site, immediately end the packet capture. (The faster you do this, the less likely your packet capture will contain unnecessary packets to filter through.)

Hint: If you do it correctly, a certain protocol involving handshakes will show up in your packet capture.

Questions:

The flag you will be submitting must contain the following information:

1. What protocol is being used to deliver the text file? (Use capital letters)
2. What is the IP address of the device/server receiving the packets?
3. What is the port number of the device/server receiving the packets?

The formatting for the flag will look as follows:

flag{answer1\_answer2\_answer3}