1. Bit A has a 30% chance of being a 1 and a 70% chance of being a 0. Bit B has a 20% chance of being a 1 and a 80% chance of being a 0.

XNOR is an operation which is the opposite of XOR. That is:

1 XNOR 1 = 1; 1 XNOR 0 = 0; 0 XNOR 1 = 0 and 0 XNOR 0 = 1.

* 1. What is the chance A XNOR B is a 1?
  2. What is the chance A XNOR B is a 0?
  3. Would you expect A XNOR B to have more, less or the same entropy as A XOR B?

1. Briefly describe two expected impacts of quantum computing on our ability to communicate securely.
2. Consider Risk Assessments:
3. What are the 9 steps of a risk assessment?
4. Given the following LZW decompression algorithm, what is the resulting dictionary and output if the indicated values are received. Assume that A = 65, B = 66, C = 67, etc. The dictionary starts at 256.

read a character k

output k

w = k

loop

read a character k

entry = dictionary entry for k

output entry

add w + first char of entry to the dictionary

w = entry

endloop

Received Values: 65 66 67 256 258 257

Part II: You plan to send data over a covert channel (or hide it within another message): How would compressing the data with lossless compression before sending it help keep it hidden?

1. Determine a Huffman encoding of each symbol:

G A B A D A G B A G F B B B D F E A E F

1. You are doing a risk analysis for a delivery corporation. For each concern listed below, give a "threat", a "vulnerability", and a "risk" associated with it. (You may need to add some of your own details to them.)
   1. You are concerned that a driver might be in an accident which isn't his fault and that the company may be sued.

* Threat
* Vulnerability
* Risk
  1. You are concerned about customers entering the building on rainy days and slipping on the floor and breaking a leg.
* Threat
* Vulnerability
* Risk

1. Consider transmitting bits through a BB84 type quantum channel Why must roughly half the bits be discarded? Be able to do an example
2. What is a "Ping Scan"? What is a "Port Scan"?
3. I client has asked you to assess the password security of its users. For this work, they gave you a password file with 1024 hashes (They also gave you a lot of money, but that is not part of the problem). You have a dictionary with 32 million words in it which you plan to use for this project. Each password is about 128 bits long and has a 1/64 chance of being in your dictionary.
4. If the passwords are salted, what is the probability at least one of them will be found in the dictionary?
5. If the passwords are salted, about how many hashes would you expect to calculate before finding one of them? (You don't care which one.)
6. If the passwords are salted, about how many hashes would you expect to calculated before finding the "administrator" password?