

As always: SHOW WORK to receive credit.

1. Would you use a Caesar Cipher (or a secret decoder ring) to safeguard your valuable data? Explain, citing two reasons.

2. A) A sequence of random numbers follows: 3,0,9,9,7,2,1,3,3,0,9,9,7,2,1,3,3,0,9,9...  
Can you guess which digit will be next?

B) A sequence of random numbers follows: 6,5,5,1,8,6,1,4,1,7,4,0,9,2,7,3,6,1,4...  
Can you guess which digit will be next?

C) Are both of these truly random? Which one offers more security?

3. If there were 400,000 English words which were 6 *letters* or less, what percentage of all possible 6 *character* expressions would be utilized? Assume there are 18 valid special characters.

4. How many years would it take, statistically, to crack a 128-bit AES key by brute force?

5. A) Name the elements of a symmetric encryption scheme.

B) Which one of these elements actually provides the security of your data?

C) You are Alice. If you need to have a private chat with Bob and a separate private chat with Carroll, will you use the same symmetric key to secure both conversations? Why?

6. Look up "Symmetric-Key Algorithm" on Wikipedia. List 3 examples of symmetric block ciphers and 3 examples of symmetric stream ciphers.

<u>Block</u>	<u>Stream</u>
1.	1.
2.	2.
3.	3.

7. Perform the following **Exclusive Or (XOR)** operation:

$$\oplus \begin{array}{cccc} 0001 & 0011 & 1100 & 0111 \\ \underline{1010} & \underline{1001} & \underline{0010} & \underline{0111} \end{array}$$

8. A) Perform symmetric encryption given the parameters below:

PT (ASCII coded message) -> Green  
Symmetric Key (ASCII) -> v\$B6H  
Encryption Algorithm -> XOR

B) Is the resulting Cipher Text (CT) discernible as ASCII?

C) Now, decrypt the CT using the Symmetric Key.

Is this the result you expected? \_\_\_\_\_