**CS 4732/57322 Homework #4**

***Due electronically by midnight July 13th, 2020***.

For submission, if done on paper please scan and submit as a pdf. If done in word, please submit the .docx or .doc format.

**IMPORTANT**: Clearly indicate outside resources utilized and sign below. Failure to cite use of outside resources will be reported for appropriate disciplinary actions. Note that discussions with other students are encouraged; copying – with or without modifications – is unacceptable and will also be reported.

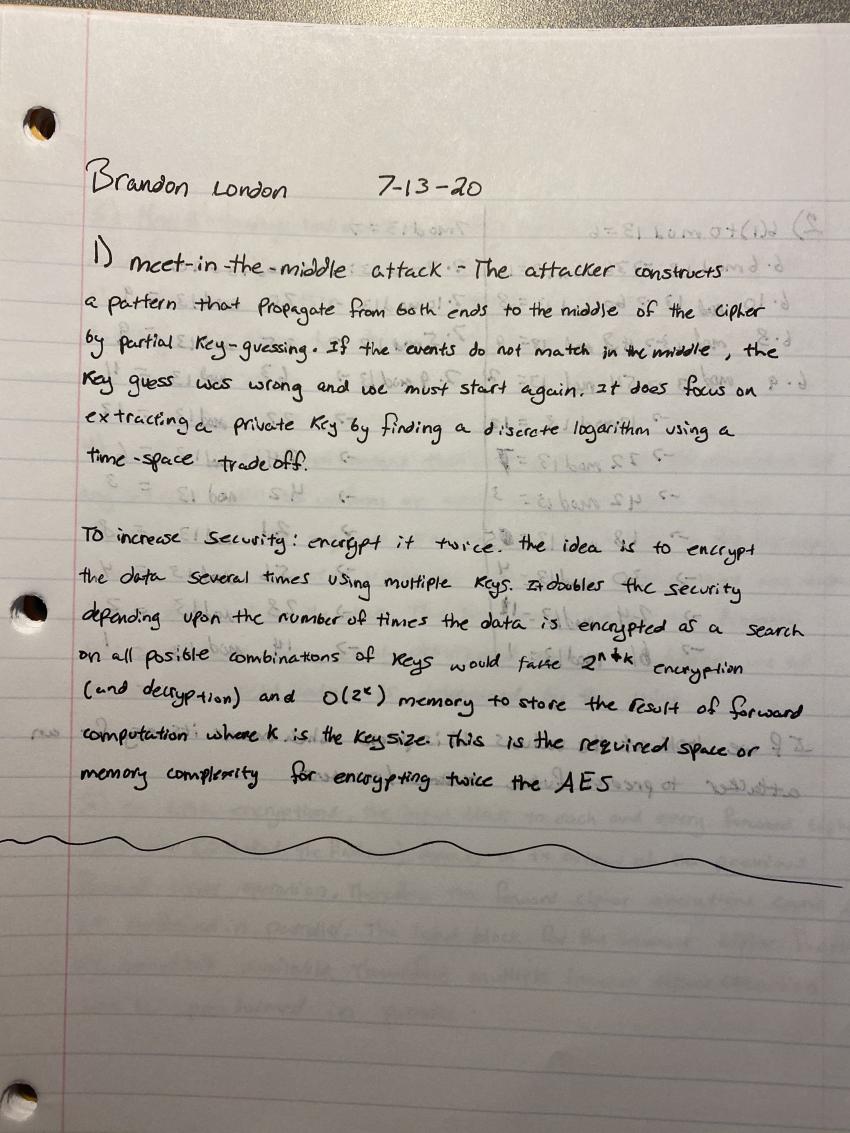
I discussed one or more problems with the following people:

Jacob

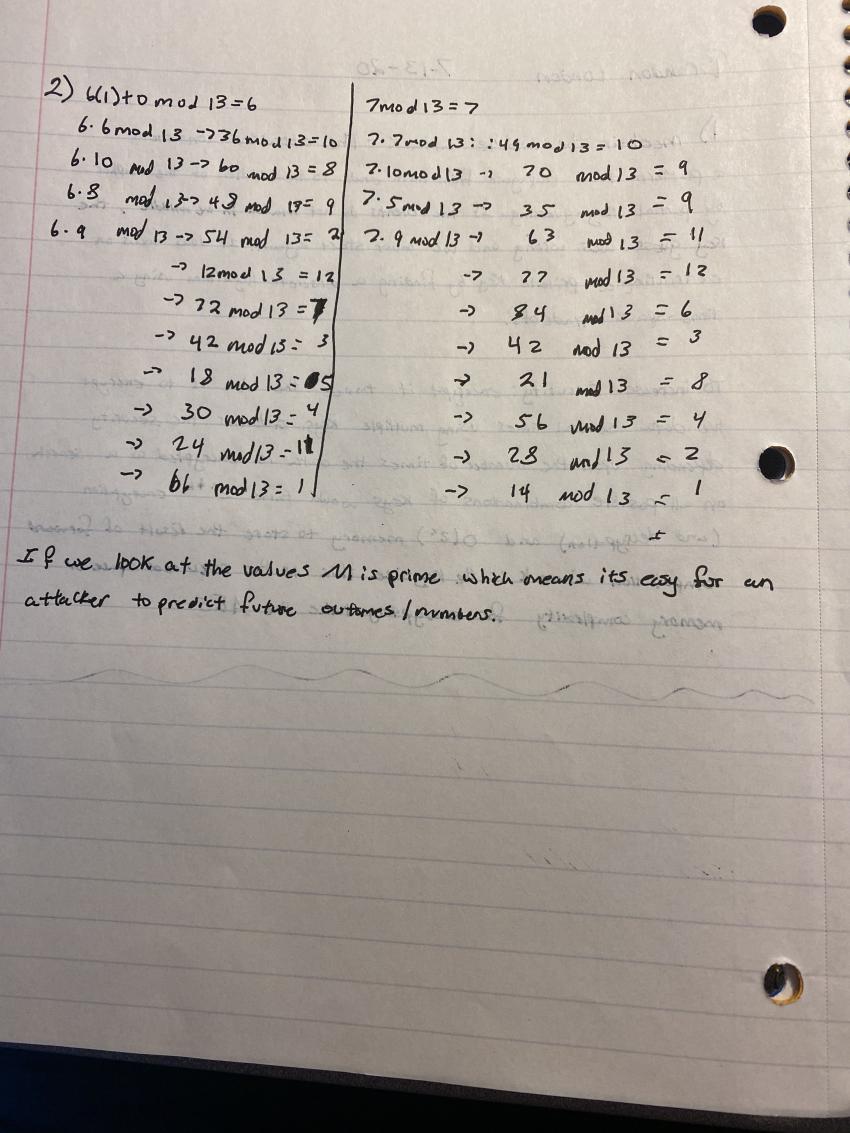
I hereby certify that any outside resources utilized, other than the textbook and class materials, are clearly cited. All other material I provide for this homework submission is my own original work.

*Printed name*

1. (8 points) Explain what a meet-in-the-middle attack is in broad terms. Suppose we tried to increase the security of AES by encrypting twice, how much space do you think it would need (just describe it, I do not need specific numbers)?



2. (12 points) While it is desirable to have a PRNG have a full period, that does not guarantee good randomness. Consider a linear congruential generator using the settings of a = 6, m = 13 and another one with a = 7, m = 13. Write out the full two sequences out for their periods. After looking at the sequences, do you feel more comfortable with one or the other?

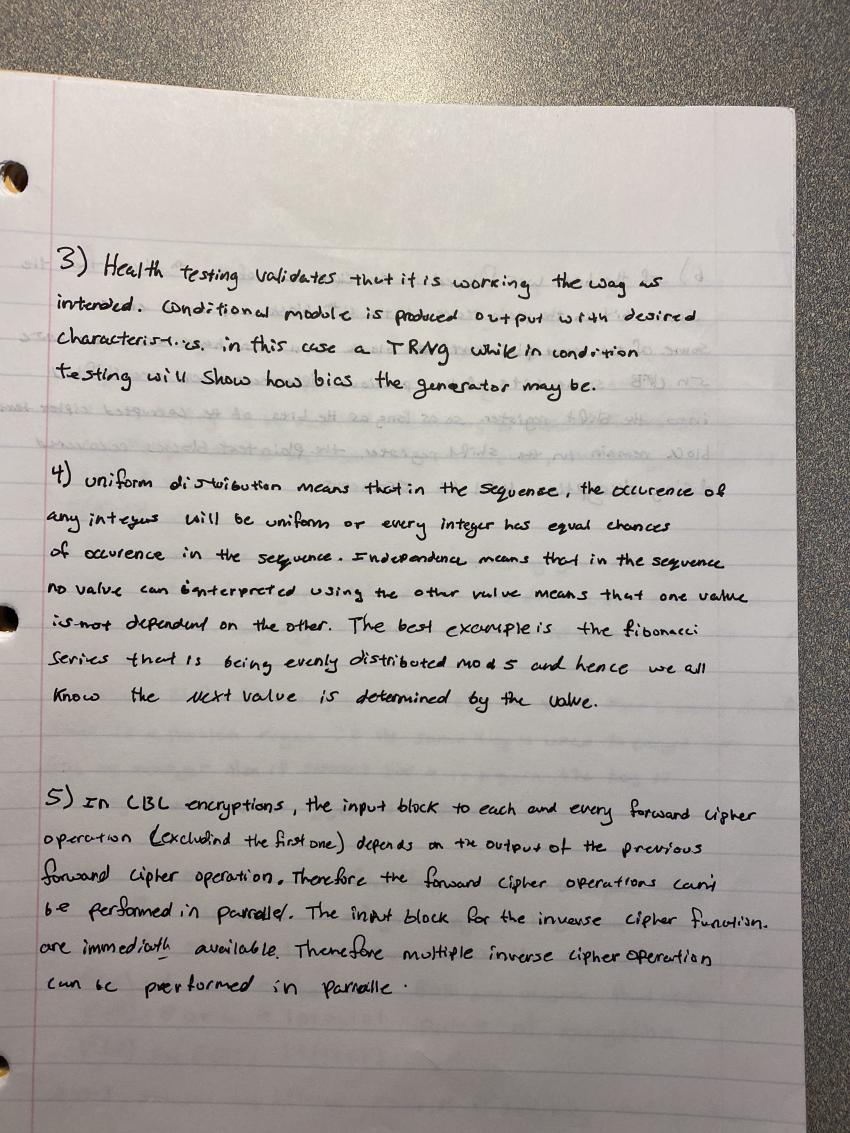


3. (10 points) What is the difference between condition testing and health testing in regards to TRNGs. Give an example of a bitstream that would pass health testing but not conditioning and explain why.

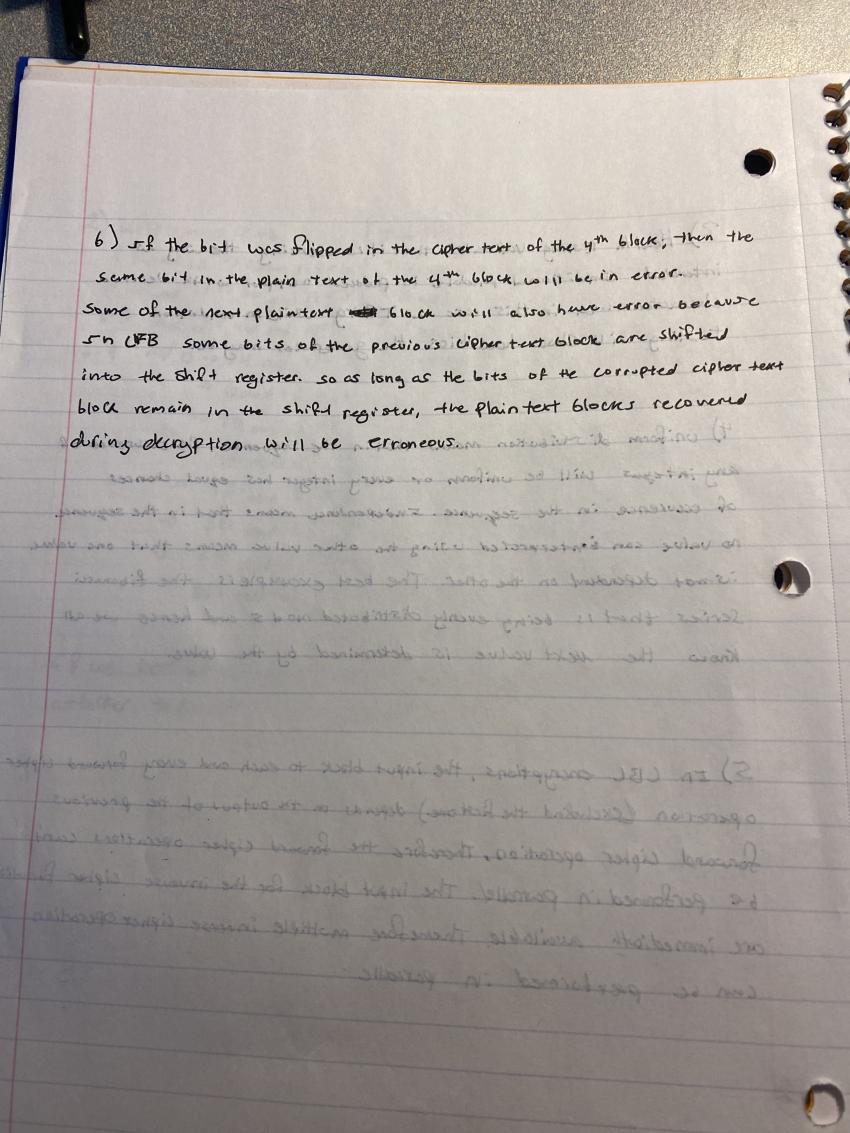
4. (8 points) In regards to whether or not a sequence is random, two criteria would be uniform distribution and independence. Define the two, then give me an example of a sequence (at least 10 bits long) that has a uniform distribution but violates independence. Relate to me the independence.

5. (6 points) Is it possible to perform encryption on multiple blocks of plaintext in parallel in CBC mode? What about decryption? Justify your answer.

**ANSWER FOR 3,4,5 IS BELOW**



6. (6 points) In transit a bit is flipped in a ciphertext that was created using a block cipher in CFB mode. What will be the result when we decrypt the text? Suppose that the message is 10 blocks in size, with the 4th block having a bit that was flipped.



7. (10 points) Why is it a bad idea to reuse a stream cipher key (in this case, the stream cipher is just exclusive or’ing your key with the plaintext)? Explain with an example using two plaintext bitstreams of 8 bits involving the reuse of a key bitstream of also 8 bits. Then XOR the resulting two ciphertexts. What property does it have? This might be hard to see, but look at the two plaintexts in relation to it.

