Computer Science 530 - Assignment #1 -- Fall 2020

Due: Wednesday, September 16, 2020, 11:00 p.m.

1. Why do we use encryption modes of operation to convert block ciphers into stream ciphers? What is important about the initialization vector (IV) in a stream cipher, and what happens if the IV is known by the adversary? Explain your answer. What happens if the same IV is used multiple times? Can a protocol be designed so it is just as safe to use the same IV to encrypt a message stream, as it is to use a different IV for the stream each time? Explain your answer.
2. In RSA, an encryption key of e = 3 can be used so long as (p-1)(q-1) is not divisible by 3. For p = 11 and q = 23, let e = 3. Find d. Show how one enciphers the plaintext m = 4 with e = 3 into a value for c. Then show that deciphering c with d yields m again.
3. When using XOR with a random key as a method of encryption why is it important that they key be used only once? What is the method of encryption called? Even if the key is used only once, what is the biggest vulnerability with the use of a simple XOR in most security protocols?

INSTRUCTION:

The report must be submitted by 11:00 p.m. on September 16, 2020. The report should be approximately 3 pages, or roughly 1200 to 1500 words. To submit your report you will use the USC DEN D2L (https://courses.uscden.net/d2l/home/18546) submission mechanism. You will use this method regardless of whether you are an on-campus student or a DEN student. Please be sure to include your name in the body of the assignment (i.e. within the Word, PDF, or Text File).

How to submit Assignment #1:

- STEP 0. Be sure to include you name in the body of your assignment.
- STEP 1. Please login to DEN, and select csci530.
- STEP 2. Please select "Assignment" in the menu.
- STEP 3. Please select "view/Complete Assignment #1".
- STEP 4. Please select "File To Attach" to attach your report. (NOTE: PDF, MS WORD, ASCII TEXT ONLY! Other formats are NOT acceptable.)
- STEP 5. Please select "Submit" button. (If you select *SAVE* button instead of *submit*, then the TA cannot view your report for grading.)

It is the individual student's responsibility to follow the submission instruction. Submissions that do not follow this instructions, e.g., submitted late, or only "Saved" and not submitted. may be penalized or may not be graded at all. Note that the submission box for the assignment may dissapear from the class web site at 11PM on September 18t (i.e. the submission deadline plus 48 hours).

For the three reading reports in this course (of which this is one), students may receive an automatic extension of 48 hours total that may be applied across the three homework assignments. If you turn in one of your assignments 8 hours late, then you will only have 40 hours remaining in extensions to use on subsequent assignments. I suggest not using the whole 48 hours on the first assignment, because if you have an unforseen scheduling issue that arises later in the semester, it will be your problem. Late assignments (beyond any extension) will be assesed 1 full letter penalty per day they are late, and if the topic of an assignment is covered in the lecture following the due date, then the assignment will not be accepted beyond that lecture.

GUIDELINE:

This is a lot to cover in so few words - so our advice is to write a first pass at your answer that is longer, and then edit out material that is redundant or not to the point. The use of tables can be very effective in conveying your ideas in a small area, but the tables must be integrated with your textual discussion, and not the only item in your submission.