COMS 4180 Network Security Spring 2018 Written Assignment 1

Due Wednesday Feb 7th, 2018, 10:00pm Eastern time.

- This assignment is to be done individually.
- NO LATE SUBMISSIONS WILL BE ACCEPTED.

Submission Instructions

- Assignments will be submitted in Courseworks.
- Submit one file containing all of your answers. The file formats accepted are pdf, word (.docx, .doc) and plain text with a .txt extension.
- The file name will be <your uni>.<extension> example: zyx2018.pdf
- Please put your name on the first line of the file.

9 questions, 50 points total

For questions 1-3, the exact block cipher used in the mode does not matter. Assume AES (or any 16 byte block cipher) is used.

1. (2 points)
For performance, is it better to use CTR mode or CBC mode to encrypt streaming data (audio or video) between a server and client? Explain why.

2. (5 points)
Suppose plaintexts P1 and P2 are each encrypted using CBC mode with the same key and same IV. Let C1 and C2 be the resulting ciphertexts. Given both ciphertexts, can any information be gained about the plaintexts? If yes, explain what information can be obtained and show how it is obtained. If no, explain why not.

3. (5 points)
For CTR mode, is it ever possible to splice ciphertext from two different files together and not have the splice detected when the files are decrypted? If yes, how/why (be specific about the type of file) and explain under what conditions. If no, why not?

4. (3 points)
While NIST recommends a standard block cipher (AES), NIST has never held a competition to select a standard stream cipher. Why is having only a standard block cipher sufficient (why is it not necessary to have a standard stream cipher)?

5. (15 points, 5 points for each part)

- Let B be a block cipher.
- Let K denote the key used in B.
- Let H be a hash function
- Let X be a public key cipher.
- Let Bpriv and Bpub be Bob’s public and private keys for X
- Let Apriv and Apub be Alice’s public and private keys for X

Alice and Bob are connected over a network. Alice wants to encrypt and sign a file, and send the encrypted file along with its signature to Bob. Bob needs to be able to read the file and verify the file came from Alice. The file must be encrypted with B. Alice will choose the value of K.
Using only B,H,X and the keys,

a. Explain how K can be known to both Alice and Bob.
b. Explain how Alice encrypts and signs the file.
c. Explain how Bob verifies the signature on the file.

6. (3 points)
Explain why in Diffie-Hellman the values the entities exchange in order for each to compute the same secret value can be sent in the clear. (In the lecture slides, this is T_a that Alice sends to Bob and T_b that Bob sends to Alice).

7. (3 points)
Why is it necessary to start developing standards for cryptographic algorithms that will run on today's computers but remain secure when quantum computation is practical?

8. (4 points)
In this question, it does not matter what the cipher is or if it is a symmetric or asymmetric key cipher. Consider a cipher using a key, K, of length b bits to encrypt data. Given plaintext, P, containing n bytes, why is it necessary that the cipher be implemented so that the time the cipher takes to encrypt P be the same regardless of the value of K?

9. (10 points)
Pick one of the estream finalists from the assigned reading in lecture 1 and summarize the algorithm in one page or less. You may include a diagram, but cannot copy verbatim from the assigned reading.