COMS 4180 Network Security Spring 2016 Written Assignment 1

Due Wednesday Feb 10th, 2016, 10:00pm Eastern time.

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

Submission Instructions

- Assignments will be submitted in Canvas.
- 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: jld2017.pdf
- Please put your name on the first line of the file.

7 problems, 50 points total

1. (16 points, 4 points for each part)
Suppose AES (or any block cipher) is used to encrypt data. Which mode of encryption (from lecture 1 slides/readings) is best suited for each of the following scenarios and why? If more than one mode is suitable, pick one and explain why.
a. Streaming data (audio or video) between a server and client transmitted using RTP over UDP.
b. Sending a 32 byte secret key between a server and a client over a connection using TCP for the transport layer.
c. Sending a 1MB file between a server and a client over a connection using TCP for the transport layer.
d. Disk encryption on a backup server storing system log files where the files are individually encrypted with one key used across all files.

2. (10 points)
Read the study conducted on public keys (rsa_mod_eprint.pdf file, title "Ron was wrong, Whit is right"). What is the security implications of the distribution of RSA moduli the authors found?

3. (8 points, 4 points for each part)
Given a block cipher B with a secret key K, a hash function H, and a public key algorithm P with the private and public keys privkey and pubkey, respectively: (the specific algorithms do not matter for this problem).
a. list the steps to encrypt and sign a file
b. list the steps to verify the signature on the file

4. (5 points)
Use bc, an arbitrary precision calculator, to compute a shared key using Diffie-Hellman key exchange. (Pretend you are both Alice and Bob.) Use $p = 2^{61} - 1$ and g = 23489.
Alice and Bob's secret numbers are ***SA*** = 93573 and ***SB*** = 23903.
Use the script command to show each step.
bc is on the clic machines in /usr/bin/bc
Use "man bc" and "bc -h" for assistance.

5. (4 points)
When selecting a new cryptographic algorithm as a standard, why is simplicity of the algorithm/ease of understanding the algorithm important?

6. (4 points)
a. (2 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?
b. (2 points) Of AES and Diffie-Hellman, which one is it more critical to replace with a quantum-safe algorithm and why?

7. (3 points)
Suppose in an implementation of ECDH the time it takes to compute the shared secret increases as the values used for the keys increase. Is this a security issue? Explain why or why not.