Assignment 1
ELEC5616: Computer and Network Security

Luke Anderson
luke@lukeanderson.com.au
University of Sydney

May 18, 2017

Date Due:

- 2nd June 23:59 - Deadline for feedback.
  Assignments submitted before this time will be marked with feedback before the exam.
- 16th June 23:59 - Final Deadline for assignment.

Instructions:

- You are to work on this assignment in groups of 1 or 2.
  These groups do not have to be the same as those for your project.
- This assignment is to be submitted via e-learning with your answers typed (not handwritten).
- Late assignments will not be accepted.
- Make sure you understand each of your answers well, they are excellent exam preparation.
- Please make sure the names and SIDs of each person in the group are provided.

1 Poker and Cyphers (25 marks)

A. **Attacks (5 marks)**
Playing in your regular Friday night poker match, you notice collusion between Slim Jim and Rusty Joe. Every time Slim Jim scratches his left eye, Rusty folds; and every time Slim Jim coughs, Rusty Joe bets the house. Using this information you fleece both of them for their pocket money. What class of attack did you use?

B. **PRNGs (5 marks)**
After Slim Jim and Rusty Joe realise what's going on, the only way you all agree to play is over the Internet. Your first attempt is to download PokerXP from MickySoft. The designers of PokerXP didn't take *ELEC5616*, and it turns out they used the UNIX rand() linear congruential generator to shuffle the deck. How long will it take for Slim and Rusty to get their revenge?

C. **PRNGs II (5 marks)**
You now decide to have your own poker program written, so you contract the design out to Network Security Associates. They decide to use MD5 to generate random numbers for you, and initialising it with the time in seconds since January 1, 1970, XORed with the binary representation of "POKER". What do you think of the security of this?

D. **Hash Functions (5 marks)**
Show how one can construct a reasonable MAC out of a hash function.

E. **Polyalphabetic Substitution Cyphers (5 marks)**
Working for a small South American intelligence agency you are supplied with an intercepted ciphertext message. How might you be able to determine whether a polyalphabetic substitution cipher was used as opposed to a modern symmetric cipher (such as Rijndael) without decrypting the message? If it was indeed a vignere cipher, statistically how might you be able to determine whether the plaintext was sent by a Columbian paramilitary group or a Californian drug dealer? (Hint: the Columbians speak Spanish and the American speaks English).

2 General Questions (25 marks)

A. **DoS (5 marks)**
Explain the principle behind a denial of service attack.

B. **Timing Attack (5 marks)**
What is a timing attack? How can a timing attack be used against naive implementations of RSA.

C. **RSA (5 marks)**
The Mafia family you belong to is holding elections for a new boss. It is suggested that each member of the family votes privately by encrypting their nomination (either "Sammy the Knife", "Big Kevsta" or "Teflon Hook") with the family's 4096-bit RSA public key (which is well known) and then e-mail the ciphertext in. If everyone can read everyone else's e-mail, is this system still secure?

D. **Attacks on Asymmetric Algorithms (5 marks)**
Is the rate at which we're improving attacks on asymmetric cryptosystems greater or less than symmetric cryptosystems? What is the end game for attacks on asymmetric algorithms?

E. **Avalanche Effect (5 marks)**
Explain the avalanche effect in DES, with reference to the three major building blocks which cause it to occur.
(Hint: two are 'black boxes' and the third is the overall structure).

3 Protocols (25 marks)

Commitment schemes allow Alice to commit a value x to Bob. The scheme is *secure* if the commitment does not reveal any information about the committed value to Bob. At a later time, Alice can *open* the commitment and convince Bob that the committed value is x. The commitment is *binding* if Alice cannot convince Bob that some other value $x' \neq x$ is the committed value.

Consider the following commitment scheme:

Commitment: Alice chooses a random r the same size as x and calculates $y = h(x \| r)$, where h is a hash function (e.g. MD5). She sends the values r and y to Bob.

Open: Alice sends x to Bob, and Bob calculates $y = h(x \| r)$.

A. Show that the proposed scheme is binding. *(7 marks)*

B. Show that the proposed scheme is insecure, i.e. that the scheme reveals information which allows Bob (with some work) to determine the committed value. *(7 marks)*

C. Suggest a modification to the scheme to secure the protocol. *(11 marks)*

4 Question 4: Network and Software Security (25 marks)

A. **SSL (5 marks)**
You visit a website which uses SSL with a 256-bit certificate. Is it secure?

B. **Salting Passwords (5 marks)**
Explain how password salting increases the security of password files. What is the difference between a salt and a secret salt?

C. **OS Fingerprinting (5 marks)**
Explain how operating systems can be precisely identified across a network.

D. **Internet (10 marks)**
In a page, address both sides of the following statement: "It would be good for security if everyone on the Internet ran the same operating system".

This is the end of the assignment.