FIT3031
Information & Network Security
Assignment 1 – Semester 1, 2013

Assignment 1 consists of 2 parts:

- Part A
- Part B

Part A:

Part A of this assignment will comprise 5 quizzes to be conducted within the first hour of each of your allocated tutorial classes held in weeks 2 to 6 (both inclusive).

Each quiz consists of true/false, multiple-choice and short-answer questions. The lecture material covered in the week prior to the quiz will be the topic of the quiz. For example, LN1- Introduction will be the topic of quiz 1 held in week 2.

Part B:
Submission Guidelines

- **Deadline:** 3 PM, 19 April 2013
- **Submission format:** PDF only. You can use any freely available pdf converter to make a pdf file from an editable one.
- **Submission platform:**
  - Caulfield & South Africa – upload via Moodle
- **Files to be submitted:** You need to submit 1 file: *Assign1B-SUID*.pdf, for all questions, with your student ID (SUID) included in the file name, and a completed assignment cover sheet.
- **Late submissions ONLY via approved special consideration request**
- **Approval for special consideration request should be obtained before 3PM, 12 April 2012 [AEST].**
- **Late submissions**: An assignment handed in late without prior permission will receive a penalty of a 5% per day (including Saturday and Sunday) or part thereof, after the due date and time.

Plagiarism: *It is an academic requirement that your submitted work be original. Zero marks will be awarded for the whole submission if there is any evidence of copying, collaboration, pasting from websites, or copying from textbooks. –Plagiarism policy applies to all assessments.*

Marks

- Part A of the assignment is worth **5% of the total unit marks**, each quiz being worth **1%**
- Part B of the assignment is worth **15% of the total unit marks**.
  - Part B is consists of 6 questions and is **marked out of 40 nominal marks**.
  - For example, if you obtain 24 marks for Part B of this assignment, it will contribute (24/40)*15 = 9 marks to your final unit grade.
- Assignment 1 is worth **20% of the total unit marks**
  - For example, if you obtain 3.5 marks for Part A and 24 marks for Part B of this assignment, it will contribute 3.5+9= 12.5 marks to your final grade.

PART B: Assignment Questions

1. Assuming you can do 2^{20} encryptions per second, and key size is 40 bits:
   a. How long would a brute force attack take?
   b. Give a scenario where this brute force attack would be practical and another where it wouldn't.
   c. What happens if you double the key size? **[1+2.5+1.5= 5]**

2. Alice and Bob agree to communicate privately via email using a scheme based on RC4, but they want to avoid using a new secret key for each transmission. Alice and Bob privately agree on a 128-bit key *k.* To encrypt a message *m* consisting of a string of bits, the following procedure is used:
   i. Choose a random 80-bit value *v*
   ii. Generate the ciphertext $c=RC4(v \,||\, k) \oplus m$
   iii. Send the bit string $(v \,||\, c)$

   Where $(a \,||\, b)$ is the concatenation of *a* and *b* bits; and
   $a \oplus b = a$ XOR b;

   Answer the following:
   a. Suppose Alice uses this procedure to send a message to Bob. Describe how Bob can recover the message *m* from $(v \,||\, c)$ using *k.*
   b. If an adversary observes several values of $(v_1 \,||\, c_1)$, $(v_2 \,||\, c_2)$, … transmitted between Alice and Bob, how can he/she determine when the same key stream has been used to encrypt two messages?
   c. If Alice and Bob agree to use 16-bit Cipher Feedback (CFB) mode instead of RC4, and a bit error occurs in the transmission of a ciphertext; how far does the error propagate?

   [2+2.5+2.5 = 7]

3. Suppose John suggests the following way to confirm that the two of you are both in possession of the same secret key of length 128 bits. You create a random bit string whose length is the same as the length of the key, XOR it with the key, and send the result over the communication channel. John XORs the incoming block with the key (which should be same as your key) and sends it back. You check, and if what you receive is your original random string, then you have verified that John has the same secret key, yet neither of you has transmitted the key.
   a. Is there a flaw in this scheme?
   b. Illustrate your answer with an example.

   [1+2=3]

4. In this problem we shall compare the security services that are provided by digital signatures (DS) and message authentication codes (MAC). We assume that Oscar is able to observe all messages sent from Alice to Bob and vice versa. Oscar has no knowledge of any keys but the public one in case of DS. State whether and how DS and MAC protect against each attack. The value *auth (x)* is computed with a DS or a MAC algorithm, respectively.

a. **(Message Integrity)** Alice sends a message *x* = *"Transfer $1000 to Mark"* in clear text and also sends *auth (x)* to Bob. Oscar intercepts the message and replaces *"Mark"* by *"Oscar".* Will Bob detect this?
b. **(Replay)** Alice sends a message *x* = *"Transfer $1000 to Oscar"* in clear text and also sends *auth (x)* to Bob. Oscar observes the message and signature and sends them 100 times to Bob. Will Bob detect this?
c. **(Sender Authentication with cheating third party)** Oscar claims that he sent some message *x* with *auth (x)* to Bob, but Alice claims the same. Can Bob clear the question in either case?
d. **(Authentication with Bob cheating)** Bob claims that he received a message *x* with a valid signature *auth (x)* from Alice (e.g., *"Transfer $1000 from Alice to Bob")* but Alice claims she has never sent it. Can Alice clear this question in either case?

[2 + 2 + 2 + 2 = 8]

3. Users A and B use the Diffie-Hellman algorithm to exchange a shared key and generate public keys of their own. Consider a common prime number q=71 and α (a primitive root of q) =7. Determine the following:

    a. If user A has private key=5, what is A's public key?
    b. If user B has private key=12, what is B's public key?
    c. What is the shared key?

Show the full working process of your work in at least three steps in both encryption and decryption. Consult page 101 of the textbook.

[3+3+3=9]

6. Answer the following in relation to a scenario where Bob and Alice use Kerberos for mutual authentication:
    a. When Bob receives a ticket from Alice, how does he know it is genuine?
    b. When Bob receives a ticket from Alice, how does he know it came from Alice?
    c. Alice receives a reply; how does she know it came from Bob (and that it is not a reply of an earlier message from Bob)?
    d. What does the ticket contain that allows Alice and Bob to talk securely?

[2+2+2+2=8]