UNIVERSITY OF CANBERRA

8019 Computer and Network Security

Semester 2, 2016

Assignment 1

Instructions:

1. **How to write your assignment?**.

   Follow the template provided on units Moodle site. Answer all questions, as per the format described below.

   - State the question along with its Number e.g., 2b, 2c. Also, put total points. Bold the question.
   - Provide your answers in a bounding box, directly below the Question. Please see below for two sample questions.

   1.a What is the difference between passive and active security threats? (3 points)

Solution: **Passive attacks** have to do with eavesdropping on, or monitoring, transmissions. Electronic mail, file transfers, and client/server exchanges are examples of transmissions that can be monitored. **Active attacks** include the modification of transmitted data and attempts to gain unauthorized access to computer systems.

   3.d What is a message authentication code? (2 points)

Solution: An authenticator that is a cryptographic function of both the data to be authenticated and a secret key.

2. **Best Strategies to do the assignment:** For each of the question, go back and read the relevant section in the text book. If it does not make sense in the first go, I would suggest read it a few times to understand the contents. Then, carefully read the question in the assignment and relate it to the text. You can find answers to all questions in the text. So carefully reading it a few times, and making an effort to understand the text is quite crucial and important and can help you solve all problems in the assignment.

3. I would expect you to **write down your answers in your own words**. You can use the exact same technical terms as in the book, but, please provide the generic description in your own words (not directly copied from the text book).

4. **Due Date: Week 7 21 Sep 2016 at 5pm**. Submit Only the pdf file. Name your file as *Ass1_CNS_ID_FirstName.pdf*. For example, *Ass1_CNS_434816_Munawar.pdf*

1. **Chapter 1: Overview**
   (a) $\boxed{\text{2 points}}$ List and briefly define categories of passive and active security attacks.

Total for Question 1: 2

2. **Classic Encryption**
   (a) $\boxed{\text{1 points}}$ What are the two basic functions used in encryption algorithms?
   (b) $\boxed{\text{1 points}}$ What are the two general approaches to attacking a cipher?
   (c) $\boxed{\text{2 points}}$ List and briefly define types of cryptanalytic attacks based on what is known to the attacker.
   (d) $\boxed{\text{2 points}}$ What are two problems with the one-time pad?
   (e) $\boxed{\text{2 points}}$ Calculate the determinant mod 26 of $\begin{pmatrix} 20 & 2 \\ 5 & 4 \end{pmatrix}$.
   (f) $\boxed{\text{3 points}}$ Encrypt the message "meet me" using the Hill cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. Show your calculations and the result.
   (g) $\boxed{\text{3 points}}$ Show the calculations for the corresponding decryption of the ciphertext in above part to recover the original plaintext.
   (h) $\boxed{\text{2 points}}$ Using the Vigenere cipher, encrypt the word "explanation" using the key "leg".
   (i) $\boxed{\text{5 points}}$ The following ciphertext was generated using a simple substitution algorithm. Given that the plaintext is in English language, can you decrypt this message by exploiting the characteristics of English Language (eg, alphabet e is the most recurring in plain text).
   53305))6*;4826)4.)4);806*;48860))85;;]8*;:*883 (88)5*;46(;88*96*?;8)*(;485);5*2:*(;4956*2(5*4)88*;4069285);)68)4;1(9;48081;8:81;4885;4)485528806*81 (9;48;(88;4(?34;48)4;161;:188;?;

Total for Question 2: 21

3. **One Time Pad** This problem explores the use of a one-time pad version of the Vigenre cipher. In this scheme, the key is a stream of random numbers between 0 and 26. For example, if the key is 3 19 5 $\cdots$, then the first letter of plaintext is encrypted with a shift of 3 letters, the second with a shift of 19 letters, the third with a shift of 5 letters, and so on.
   (a) $\boxed{\text{3 points}}$ Encrypt the plaintext "sendmoremoney" with the key stream
   9 0 1 7 23 15 21 14 11 11 2 8 9
   (b) $\boxed{\text{3 points}}$ Using the ciphertext produced in part (a), find a key so that the cipher text decrypts to the plaintext "cashnotneeded".

Total for Question 3: 6

4. Block Ciphers
   (a) $\boxed{\text{3 points}}$ Which parameters and design choices determine the actual algorithm of a Feistel cipher?

Total for Question 4: 3

5. **AES**
   (a) $\boxed{\text{2 points}}$ What is the difference between Rijndael and AES?
   (b) $\boxed{\text{1 point}}$ What is the purpose of the State array?
   (c) $\boxed{\text{1 point}}$ Briefly describe the key expansion algorithm.

6. Given the plaintext 000102030405060708090A0B0C0D0E0F and the key 01010101010101010101010101010101.

(a) 2 points Show the original contents of State, displayed as a 4×4 matrix.

(b) 2 points Show the value of State after initial AddRoundKey.

(c) 2 points Show the value of State after SubBytes.

(d) 2 points Show the value of State after ShiftRows.

(e) 2 points Show the value of State after MixColumns.

Total for Question 6: 10

7. Public Key Encryption

(a) 3 points What are three broad categories of applications of public-key cryptosystems?

(b) 3 points What requirements must a public-key cryptosystems fulfill to be a secure algorithm?

(c) 2 points What is a trap-door one-way function?

(d) 3 points Perform encryption using the RSA algorithm, as in Figure 9.5, for the following parameters:

c.

$$p = 7; q = 11, e = 17; M = 8$$

(e) 3 points Perform decryption using the RSA algorithm, as in Figure 9.5, for the following:

$$p = 17; q = 31, e = 7; C = 128$$

(f) 3 points Perform decryption using the RSA algorithm, as in Figure 9.5, for the following:

$$p = 11; q = 13, e = 11; C = 106$$

(g) 3 points In a public-key system using RSA, you intercept the ciphertext $C = 10$ sent to a user whose public key is $e = 5$, $n = 35$. What is the plaintext M?

(h) 4 points In a RSA cryptosystem, the public key of Alice is $e = 47, n = 4757$. Find the private key of Alice. Hint: First use trial-and-error to determine p and q; then use the extended Euclidean algorithm to find the multiplication inverse of 47 modulo $\phi(n)$.

Total for Question 7: 24

8. Hash Functions

(a) 2 points What is the role of a compression function in a hash function?

Total for Question 8: 2

9. Message Authentication and Digital Signatures

(a) 2 points What two levels of functionality comprise a message authentication or digital signature mechanism?

(b) 1 points When a combination of symmetric encryption and an error control code is used for message authentication, in what order must the two functions be performed?

(c) 2 points What is the difference between a message authentication code and a one-way hash function?

(d) 1 points Is it necessary to recover the secret key in order to attack a MAC algorithm?

(e) 2 points What requirements should a digital signature scheme satisfy?

Total for Question 9: 8

Question:	1	2	3	4	5	6	7	8	9	Total
Points:	2	21	6	3	4	10	24	2	8	80
Score:										