FIT3031
Information & Network Security
Assignment 1 – Semester-B 2018

Submission Guidelines

- **Deadline:** Assignment 1 due on Monday 15th January 2018, 4:00 PM
- **Submission format:** PDF only. You can use any freely available PDF converter to make PDF file from editable one.
- **Submission platform:**
  - Clayton - Softcopy submission on **Moodle**.
- PLEASE INCLUDE **YOUR NAME** AND **SUID** WITHIN THE MAIN PDF SUBMISSION
- Files to submit: ***Assign-1_FirstName_LastName_SUID.pdf***
- **No late submissions ONLY via special consideration request**
- **Late submissions**: An assignment handed in late without prior permission will receive a late penalty of a 5% deduction 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

- *This assignment is worth **20%** of the total unit marks.*
- *The assignment is marked out of **60** nominal marks.*
- *For example, if you obtain **30** marks for this assignment, it will contribute*
- ***(30/60)*20=10 marks** to you final unit grade.*

Assignment Questions

1. **Question-1: [2+2+2+2+2] = 10 marks**

   a. We consider the security services **(A) confidentiality, (B) integrity, (C) authenticity, and (D) non-repudiation**, for a variety of simple protocols. The input is always the plaintext **x**. **y** is the packet sent from Alice to Bob. Describe which security services are achieved by the following protocols.

      1. y = [h(x), x], where h(x) denotes a (collision resistant etc.) hash function. **(2 marks)**

      2. y = [MAC(x), x], where MAC(x) denotes a secure message authentication code such as HMAC. **(2 marks)**

      3. y = [encS (h(x)), x], where encS () denotes a secure stream cipher. **(2 marks)**

      4. y = encB (x, h(x)), where encB () denotes a secure block cipher. **(2 marks)**

      5. y = encS (x, sig(xm)), where xm is the last block of a long message x; encS () denotes a secure stream cipher and sig(xm) is the signature of message x. **(2 marks)**

2. **Question-2: [3+3+2 = 8 Marks]**

   Assuming you can do **2^{30}** encryptions per second and **key size is 64 bits**:

   a. How long would a brute force attack take? (Both maximum and average values)

   b. Give a scenario where this would be practical and another where it wouldn't.

   c. What happens if you double the key size?

   Show the working process of your work in few steps.

3. **Question-3: [3+3+3 = 9 Marks]**

User **A** and **B** use 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 followings:

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 working process of your work in at least three steps. Consult lecture notes and the text book.

4. **Question-4: [2+3+3 = 8 Marks]**

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:

a. Choose a random 80-bit value ***v***

b. Generate the ciphertext $c=RC4(v \parallel k) \oplus m$

c. Send the bit string $(v \parallel c)$

<u>Answer the following:</u>

a. Suppose Alice uses this procedure to send a message to Bob. Describe how Bob can recover the message ***m*** from $(v \parallel c)$ using **k**.

b. b. If an adversary observes several values of $(v_1 \parallel c_1), (v_2 \parallel c_2)$ ……. 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+3+3 = 8 Marks]

5. **Question-5: [2+2 = 4 Marks]**

a. Is it possible to perform encryption operations in parallel on multiple blocks of plaintext in CBC mode? **Justify your answer.**

b. How about decryption? **Justify your answer.** **[2+2 = 4 Marks]**

6. Question-6: [2+2+2 = 6 Marks]

Consider **p=17** and **q=31** in the RSA encryption/decryption algorithm to be used to encrypt a message **M=15**. Using the algorithm, determine the followings:

a. Generate a public-private key pair.

b. Using the generated public key, encrypt the message to get the cipher text **C**.

c. Apply the private key on C to decrypt the original message **M**.

Show the working process of your work in at least three steps in both encryption and decryption. **[2+2+2 = 6 Marks]**

7. Question-7: [2+2+2 = 6 Marks]

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 the clear and also sends ***auth (x)*** to Bob. Oscar intercepts the message and replaces ***"Mark"*** with ***"Oscar".*** Will Bob detect this?

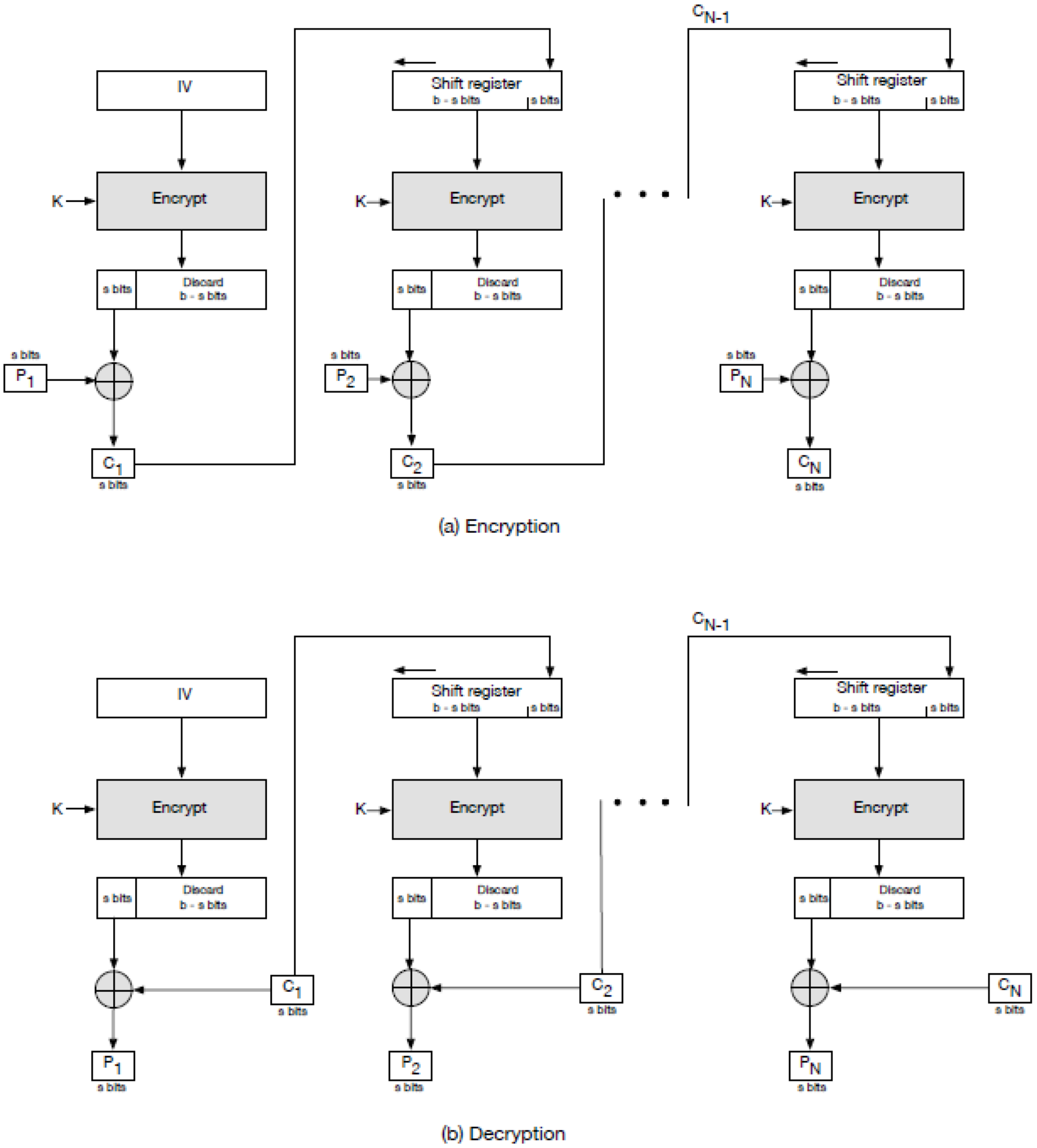
b. (Replay) Alice sends a message ***x = "Transfer $1000 to Oscar"*** in the clear and also sends ***auth (x)*** to Bob. Oscar observes the message and signature and sends them 100 times to Bob. Will Bob detect this?

c. (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 = 6 Marks]

8. Question-8:[3+2 + 2+2] =9 marks

Alice is using CFB mode of operation to encrypt a 16KB file to send it to Bob (1KB=1024 bytes).



(a) Encryption

(b) Decryption

Figure-CFB: s-bit Cipher Feedback Mode of Operation

Referring to the above figure of CFB, answer the following questions:-

- **a.** How many ciphertext blocks will be produced if Alice uses 8-bit CFB-DES (DES or Data Encryption Standard algorithm as the block cipher in Figure above)?
- **b.** How many ciphertext blocks will be produced if Alice uses 16-bit CFB-AES (AES or Advanced Encryption Standard algorithm as the block cipher in Figure above)?
- **c.** If there is an error in transmitted ciphertext block C1, how many plaintext blocks will be corrupted when Bob decrypts the file for 8-bit CFB-DES?
- **d.** If there is an error in transmitted ciphertext block C1, how many corrupted plaintext blocks when 16-bit CFB-AES is used?