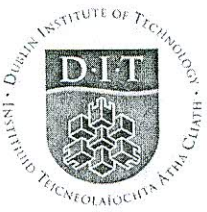

DUBLIN INSTITUTE OF TECHNOLOGY

DT228 BSc. (Honours) Degree in Computer Science

Year 4

WINTER EXAMINATIONS 2015/2016

ADVANCED SECURITY 1 [CMPU4007]

DR. FREDRICK MTENZI
DR. DEIRDRE LILLIS
MR. KEVIN FOLEY

MONDAY 11TH JANUARY 4.00 P.M. – 6.00 P.M.

ANSWER **THREE** QUESTIONS OUT OF **FOUR**.

ALL QUESTIONS CARRY EQUAL MARKS. ONE (1) COMPLIMENTARY MARK WILL BE GIVEN.

1. (a) It is widely believed among security experts and according to top-secret documents revealed by former contractor Edward Snowden that the USA and British intelligence agencies have successfully cracked much of the online encryption relied upon by hundreds of millions of people to protect the privacy of their personal data, online transactions and emails. Discuss Cryptographic techniques and mechanisms you will use to mitigate online surveillance.

(11 marks)

(b) (i) Explain the purpose of *s-boxes* in *DES*.

(4 marks)

(ii) Using the DES s-boxes, and with the aid of figure 1, show that $S_1(011000) = 5$, $S_2(001001) = f$, $S_3(010010) = d$ and $S_4(111101) = 2$.

(8 marks)

(12 marks)

(c) In the context of Biometric user authentication, explain the terms, enrolment, verification, and identification.

(10 marks)

2. (a) (i) Discuss the types of information which might be derived from a traffic analysis attack.

(4 marks)

(ii) Giving examples, explain how it is possible to gain a competitive advantage in business or military by analyzing the information obtained from traffic analysis.

(4 marks)

(iii) How can traffic analysis be prevented?

(4 marks)

(12 marks)

(b) (i) Explain, using illustrations where possible, how a key distribution center operates and its problems.

(4 marks)

(ii) Briefly explain the difference between a session key and a master key? Is there any security significance in reducing the lifetime of a key?

(3 marks)

(7 marks)

(c) Explain how the RSA algorithm works. Discuss four possible approaches to attacking the RSA algorithm.

(14 marks)

3. (a) (i) Discuss important design considerations for a *stream cipher*.

(6 marks)

(ii) Why it is not desirable to reuse a stream cipher key?

(4 marks)

(10 marks)

(b) Discuss in detail the challenges and considerations when implementing cloud encryption.

(23 marks)

4. (a) The useful lifetime of the DES was about 20 years (1977 – 1997), how long do you predict the useful lifetime of AES to be? Justify your answer.

(10 marks)

(b) Using the Playfair Cipher and keyword MONARCHY encrypt the following plaintext message.

secure office

(8 marks)

(c) In the last few years we have witnessed the rise of Cryptocurrencies as an alternative payment option. Cryptocurrencies are peer-to-peer and decentralized, and are currently all based on the first cryptocurrency, Bitcoin. Discuss the merits and regulatory ramifications of using Cryptocurrencies.

(15 marks)

DES S-Box

S_1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Figure 1: DES S-Box