DUBLIN CITY UNIVERSITY

AUGUST/RESIT EXAMINATIONS 2016/2017

MODULE: CA4005 - Cryptography and Security Protocols

PROGRAMME(S):

CASE - BSc in Computer Applications (Sft.Eng.)
CPSSD - BSc in ComputationalProblem SolvandSW Dev.
ECSAO - Study Abroad (Engineering and Computing)
ECSA - Study Abroad (Engineering and Computing)

YEAR OF STUDY: 4,O,X

EXAMINERS: Geoffrey Hamilton (Ph:5017)
Prof. David Bustard
Dr. Ian Pitt

TIME ALLOWED: 3 hours

INSTRUCTIONS: Answer all 5 questions. All questions carry equal marks.

PLEASE DO NOT TURN OVER THIS PAGE UNTIL INSTRUCTED TO DO SO

The use of programmable or text storing calculators is expressly forbidden.
Please note that where a candidate answers more than the required number of questions, the examiner will mark all questions attempted and then select the highest scoring ones.

Requirements for this paper (Please mark (X) as appropriate)

- □ *Log Tables*
- □ *Graph Paper*
- □ *Dictionaries*
- □ *Statistical Tables*
- □ *Thermodynamic Tables*
- □ *Actuarial Tables*
- □ *MCQ Only - Do not publish*
- □ *Attached Answer Sheet*

QUESTION 1 *[Total marks: 20]*

1(a) [6 Marks]

Describe the general operation of *stream ciphers*, describing in particular how they perform encryption and decryption (using a diagram if necessary). What properties must the *keystream* have for the stream cipher to be considered secure?

1(b) [7 Marks]

Describe the *Cipher Block Chaining* (CBC) mode of operation for block ciphers (use diagrams if necessary). What is the role of the *Initialisation Vector* (IV)? What are the dangers if an IV is:

- altered by an attacker
- known to an attacker
- reused with the same key

1(c) [7 Marks]

Compare and contrast the *Output Feed Back* (OFB) and *Cipher Feed Back* (CFB) modes of operation for block ciphers with respect to the following (use diagrams if necessary):

- Encryption
- Decryption
- Error propagation

[End Question 1]

QUESTION 2 *[Total marks: 20]*

2(a) [7 Marks]

Describe the *Merkle Damgård construction* which is often used in the implementation of hash functions. What properties are required for a hash function to be considered to be cryptographically secure and why?

2(b) [7 Marks]

What properties are required for a *cryptographically secure pseudorandom number generator*? Describe the Blum Blum Shub pseudorandom number generator, and explain why it is cryptographically secure.

2(c) [6 Marks]

Describe how a hash function can be used to implement a cryptographically secure pseudorandom number generator.

[End Question 2]

QUESTION 3 ***[Total marks: 20]***

3(a) [6 Marks]

Compare and contrast the RSA cryptosystem with the Rabin cryptosystem.

3(b) [5 Marks]

Consider a toy Rabin cryptosystem in which the public key $N = 77$. Describe how encryption is done in the Rabin cryptosystem and use this to encrypt the message 29.

3(c) [9 Marks]

Describe how decryption is done in the Rabin cryptosystem using the prime factors of the modulus, and how this can be made faster by choosing these prime factors to satisfy specific properties. Use this decryption technique to find all possible decryptions for the ciphertext value 37 when the public key $N = 77$ as above. In practice, how would we determine which of the possible decryptions of a ciphertext is the correct one?

[End Question 3]

QUESTION 4 ***[Total marks: 20]***

Consider the following protocol that allows entities A and B to mutually authenticate each other using a shared secret key $K_{A,B}$.

1. $A \rightarrow B : A, N_A$
2. $B \rightarrow A : B, N_B, \{N_A\}_{K_{A,B}}$
3. $A \rightarrow B : \{N_B\}_{K_{A,B}}$

4(a) [4 Marks]

Explain the use of nonces in this protocol.

4(b) [8 Marks]

Describe a *reflection* attack on this protocol.

4(c) [8 Marks]

Describe two techniques, that do not require the use of additional keys, for preventing the reflection attack described in your previous answer.

[End Question 4]

QUESTION 5 ***[Total marks: 20]***

5(a) [7 Marks]

Describe how message origin authentication is achieved when sending messages using PGP. Show the sequence of steps which must be followed on both message generation and message reception to achieve this (use diagrams if necessary).

5(b) [7 Marks]

Describe how message confidentiality is achieved when sending messages using PGP. Show the sequence of steps which must be followed on both message generation and message reception to achieve this (use diagrams if necessary).

5(c) [6 Marks]

Describe the PGP trust model. Compare and contrast this with the X.509 PKI trust model.

[End Question 5]

[END OF EXAM]