GX_____

Ollscoil na hÉireann, Gaillimh
National University of Ireland, Galway

Summer Examinations, 2009

Exam Code(s)	4IF1
	Bachelor of Science in Information Technology
Module Code(s)	CT437
Module(s)	Computer security and forensic computing
Paper No.	1
External Examiner(s)	Prof. J.A. Keane
Internal Examiner(s)	Prof. G. Lyons Dr. C. Mulvihill
Instructions:	Answer any four questions. All questions carry equal marks.
Duration	3 hrs
No. of Answer Books	1
No. of Pages	1
Department(s)	Information Technology

1
An entrepreneur developing software for the healthcare sector has secured funding and is setting up in the west of Ireland. You have been retained to provide initial advice on a security profile. Discuss elements of a report you might draft for this individual, making use of the following three headings: general IP protection (8 marks), regulatory compliance (8 marks), web and wireless exposure (9 marks).

2
(a) What is your understanding of the term 'steganography'? (6 marks)
(b) Is steganography difficult to detect in your opinion? (8 marks)
(c) Outline how a simple message might be concealed in an image using a least significant bit technique, and estimate how much information could be hidden in a single 1024*1024 image using this approach (11 marks)

3 'Security is often concerned with confidentiality and integrity'
(a) Give a brief outline of two significant properties of the Bell-LaPadula model (8 marks)
(b) In the context of the Chinese wall model, explain what is meant by a 'conflict set' (8 marks)
(c) Outline your understanding of the main elements of the BMA security policy (9 marks)

4
'Cryptography may or may not be secure'
(a) Explain what is meant by the terms 'symmetric key cryptography' and 'public key cryptography' (6 marks)
(b) Discuss how an on-line trading organisation might make use of public, private, and session keys in its dealings with customers, explaining the terms 'digital certificate' and 'digital signature' in the course of your answer (9 marks)
(c) You have access to a hard drive that is apparently encrypted. Given a plain text sample with a period of six bytes, and an encrypted sample with a period of twenty four bytes, outline how you might proceed to investigate the strength of the encryption, given that you suspect that a form of linear encryption is in place (10 marks)

5
(a) Give your understanding of the term 'phishing' (7 marks)
(b) What is meant by the use of 'fast-flux services' for phishing? (8 marks)
(c) The FTC has linked phishing to identity theft. What steps would you devise in order to lessen the likelihood of your company's employees becoming victims of phishing activities? In the course of your answer, explain the term 'educational landing page' (10 marks)

6
(a) Give your understanding of the 'Daubert Criteria' for scientific evidence (7 marks)
(b) Explain what is meant by a hash function and discuss why such functions are of use in digital forensics (8 marks)
(c) Outline the steps that you would take in imaging a disk and searching it for content, explaining the terms 'dd' and 'data carving' in the course of your answer (10 marks)

7
'The jury is still out on electronic voting'
Discuss this statement in the light of the relevant German Federal Constitutional Court decision in March 2009 (25 marks)

GX_____

Ollscoil na hÉireann, Gaillimh
National University of Ireland, Galway

Autumn Examinations, 2009

Exam Code(s)	4IF1
	Bachelor of Science in Information Technology
Module Code(s)	CT437
Module(s)	Computer security and forensic computing
Paper No.	1
External Examiner(s)	Prof. J.A. Keane
Internal Examiner(s)	Prof. G. Lyons Dr. C. Mulvihill

Instructions: Answer any four questions.

All questions carry equal marks.

Duration	3 hrs
No. of Answer Books	1
No. of Pages	1
Department(s)	Information Technology

1
An entrepreneur developing software for the bioengineering sector has secured funding and is setting up in the west of Ireland. You have been retained to provide initial advice on a security profile. Discuss elements of a report you might draft for this individual, making use of the following three headings: IP protection (8 marks), regulatory compliance (8 marks), audit trails (9 marks).

2
(a) What is your understanding of the term 'steganography'? (6 marks)
(b) How does steganography differ from cryptography? (8 marks)
(c) Discuss any one technique employing steganography that would be suited to the following application: a short message to be transmitted composed of 100 or less characters (11 marks)

3 'Security is often concerned with confidentiality and integrity'
(a) Give a brief outline of two significant properties of the Bell-LaPadula model (8 marks)
(b) In commercial work, what is meant by the term 'Chinese wall'? (8 marks)
(c) Briefly discuss two security implications of the electronic patient record (9 marks)

4
'Cryptography may or may not be secure'
(a) Explain what is meant by the term 'public key cryptography' (6 marks)
(b) Discuss how a merchant might make use of public, private, and session keys in her dealings with customers, explaining the terms 'digital certificate' and 'digital signature' in the course of your answer (9 marks)
(c) You have access to a hard drive that is apparently encrypted. It is password protected. How might you approach the problem of accessing the contents of the laptop? (10 marks)

5
(a) Give your understanding of the term 'phishing' (7 marks)
(b) In your opinion why are phishing attacks effective? (8 marks)
(c) The FTC has linked phishing to identity theft. Why is identity theft a problem? (10 marks)

6
(a) Give your understanding of the 'Daubert Criteria' for scientific evidence (7 marks)
(b) Is it possible to conduct a full forensic examination of an iPhone in your view? (8 marks)
(c) Outline the steps that you would take in imaging a disk and searching it for content, explaining the terms 'dd' and 'data carving' in the course of your answer (10 marks)

7
'The jury is still out on electronic voting'
Discuss this statement in the light of the relevant German Federal Constitutional Court decision in March 2009 (25 marks)

Ollscoil na hÉireann, Gaillimh *GX_____*

National University of Ireland, Galway

Summer Examinations, 2010

Exam Code(s)	4IF1
	Bachelor of Science in Information Technology
Module Code(s)	CT437
Module(s)	Computer security and forensic computing
Paper No.	1
External Examiner(s)	Prof. M. O'Boyle
Internal Examiner(s)	Prof. G. Lyons Dr. J. Duggan Dr. C. Mulvihill

Instructions: Answer any four questions.

All questions carry equal marks.

Duration	3 hrs
No. of Answer Books	1
No. of Pages	1
Department(s)	Information Technology

Question 1
(a) Briefly explain the following terms ‘symmetric key cryptography’ and ‘asymmetric key cryptography’ (8 marks)
(b) Show how asymmetric cryptography and a hash can be used in digital signatures (8 marks)
(c) You have been tasked with getting a certificate for your company. Outline why you might interact with the following: Registration Authority, Key Escrow Agent (9 marks)

Question 2
(a) What is meant by the term ‘disaster recovery plan’? (8 marks)
(b) Briefly explain what is meant by RAID 3 and RAID 5 (8 marks)
(c) You are tasked with developing a backup strategy. Explain what is meant by a full backup, and indicate whether incremental or differential backups would be preferred if (1) speed of backup or (2) speed of recovery is a critical factor. (9 marks)

Question 3
(a) Explain what is meant by the term ‘password cracker’ (7 marks)
(b) In the context of an Intrusion Detection System, explain what is meant by ‘signature based’ and ‘behaviour based’ approaches (7 marks)
(c) Work files are typically deleted once a week by your users. However only 20% of the time does this prove to be a problem; in the remaining 80% of cases there is no cost. In the 20% of cases, it takes the user on average two hours work to restore the file’s contents, at a cost of 50 euro per hour. Determine the Single Loss Expectancy, the Annualised Rate of Occurrence, and hence calculate the Annual Loss Expectancy. (11 marks)

Question 4
(a) Explain what is meant by one, two and three factor authentication (7 marks)
(b) Discuss any two elements of the Bell-LaPadula formal model for access control (8 marks)
(c) You are developing a physical access control policy for your organisation. Discuss how the following might apply: access log, ID badges, door access system, video. (10 marks)

Question 5
(a) Explain the following terms: ‘Man-In-The-Middle attack’, ‘replay attack’ (9 marks),
(b) Distinguish between session and persistent cookies (7 marks),
(c) You have been tasked with developing a honeypot for your organisation. Explain what this means and how it would be used. (9 marks),

Question 6
(a) Explain the concept of ‘chain of custody’ (7 marks),
(b) Explain what is meant by ‘disk imaging’ (7 marks),
(c) You suspect that someone in the organisation has been using image-based steganography to export information. Is there anything you can do to combat the use of this technology? (11 marks)

Question 7
An entrepreneur developing software for the financial sector has secured funding and is setting up in the west of Ireland. You have been retained to provide initial advice on a security profile. Discuss a report you might draft, making use of the following three headings: general IP protection (8 marks), social networking policy (8 marks), employee training (9 marks).

GX_____

Ollscoil na hÉireann, Gaillimh
National University of Ireland, Galway

Autumn Examinations, 2010

Exam Code(s)	4IF1
	Bachelor of Science in Information Technology
Module Code(s)	CT437
Module(s)	Computer security and forensic computing
Paper No.	1
External Examiner(s)	Prof. M. O'Boyle
Internal Examiner(s)	Prof. G. Lyons
	Dr. J. Duggan
	*Dr. C. Mulvihill
<u>Instructions</u>:	Answer any <u>four</u> questions.
	All questions carry equal marks.
Duration	3 hrs
No. of Answer Books	1
No. of Pages	1
Department(s)	Information Technology

Question 1
(a) Briefly explain the term 'public key cryptography' (8 marks)
(b) Explain what is meant by the term 'digital signature' (8 marks)
(c) Explain the operation of a certificate revocation list (9 marks)

Question 2
(a) What is meant by the terms 'hot site' and 'cold site'? (8 marks)
(b) Briefly explain what is meant by RAID 0 and RAID 1 (8 marks)
(c) You are tasked with providing 1000GB of storage via a RAID 1 mirroring scheme. If the disks are standardised at 500MB, explain how many will be needed (9 marks)

Question 3
(a) Explain what is meant by the term 'dictionary attack' (7 marks)
(b) Explain why logs are useful in security work? (7 marks)
(c) Work files are typically deleted once a week by your users. However only 40% of the time does this prove to be a problem; in the remaining 60% of cases there is no cost. In the 40% of cases, it takes the user on average three hours work to restore the file's contents, at a cost of 100 euro per hour. Determine the Single Loss Expectancy, the Annualised Rate of Occurrence, and hence calculate the Annual Loss Expectancy. (11 marks)

Question 4
(a) Explain what is meant by the term 'Mandatory Access Control'? (7 marks)
(b) Explain what is meant by a 'Chinese wall' (8 marks)
(c) You are developing a physical access control policy for your organisation. Discuss any three elements that might apply. (10 marks)

Question 5
(a) Explain the following terms: 'Trojan Horse', 'Worm' (9 marks),
(b) Explain what is meant by a 'keystroke logger' (7 marks),
(c) You have been tasked with developing a honeynet for your organisation. Explain what this means and how it would be used. (9 marks),

Question 6
(a) Explain what is meant by the 'chain of custody' (7 marks),
(b) Explain what is meant by 'jailbreaking' (7 marks),
(c) It appears that someone in the organisation has been using USB sticks to make unauthorised copies of information. Is there anything you can advise in connection? (11 marks)

Question 7
An entrepreneur developing software for the biomedical engineering sector has secured funding and is setting up in the west of Ireland. You have been retained to provide initial advice on a security profile. Discuss a report you might draft, making use of the following three headings: general IP protection (8 marks), laptop policy (8 marks), password policy (9 marks).

*GX*_____

Ollscoil na hÉireann, Gaillimh
National University of Ireland, Galway

Summer Examinations, 2010/2011

Exam Code(s)	4IF1 Bachelor of Science in Information Technology
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	1
External Examiner(s)	Prof. M. O'Boyle
Internal Examiner(s)	Prof. G. Lyons Dr. J. Duggan Dr. C. Mulvihill*
Instructions:	Answer any four questions. All questions will be marked equally.
Duration	3 hrs
No. of Answer Books	1
No. of Pages	1
Department(s)	Information Technology

1 (a) Explain what is meant by a 'security policy document' and outline three suitable components (6 marks)
(b) Risk analysis is important in security work. Explain what is meant by 'single loss expectancy' and 'annual loss expectancy' in this context (6 marks)
(c) Given the following three risk factors: flooding, lack of ID for employees, encrypted laptop theft, discuss how you might approach ranking them for the purposes of risk analysis – an intuitive analysis is enough (8 marks)

2 (a) Explain what is meant by the term 'sanitised information' (6 marks)
(b) What inference problems do you see in applying a 'no read up' access policy at the level of an individual column in a database? (6 marks)
(c) Consider a database that provides a 'no write down' access policy at a granularity of row. What options are available if a user wishes to insert a row with a key that already exists but at a higher clearance than the user possesses? (8 marks)

3 (a) In the context of public key cryptography, what is meant by the terms 'public key' and 'private key' (6 marks)
(b) Could authentication and confidentiality be maintained between two parties through the proper use of two public and two private keys? (6 marks)
(c) In the context of steganography, suggest any two ways that information can be hidden in an image. Given a 24 bit image with three colours (RGB), estimate how much information can be hidden using a least significant bit technique (8 marks)

4 (a) Explain what is meant by 'two factor' and 'three factor' authentication (6 marks)
(b) Explain what is meant by 'rainbow table' and 'dictionary' hash attacks (6 marks)
(c) In the context of ATM security and two factor authentication, outline any two attacks with which you are familiar. What steps would you recommend to be taken in order to lessen the likelihood of their success? (8 marks)

5 (a) Explain why log files are important in forensic work (6 marks)
(b) “The arrival of SSD has made imaging more problematic”. Is this the case? (6 marks)
(c) You are presented with a company laptop that has several encrypted files that an employee refuses to decrypt. Outline several steps that you might take in order to address this situation (8 marks)

6 (a) Explain what is meant by 'DNS cache poisoning' (6 marks)
(b) Explain what is meant by 'ARP cache poisoning/ARP spoofing' (6 marks)
(c) Discuss how Transport Layer Security (TLS) might help in certain circumstances with DNS cache poisoning (8 marks)

7 “A new threat landscape is emerging with super/smartphones and tablets”.
Discuss this statement. (20 marks)

NUI Galway
OÉ Gaillimh

Semester II Examinations 2011/ 2012

Exam Code(s)	4IF1
Exam(s)	Bachelor of Science in Information Technology
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	
Repeat Paper	No
Discipline(s)	Information Technology
Course Co-ordinator(s)	
Internal Examiner(s)	Professor G Lyons Dr. M Madden Dr C Mulvihill*
External Examiner(s)	Professor M. O'Boyle
No. of Pages	3
Duration	**3 hours**
Instructions:	Attempt any four questions. All questions will be marked equally.

Requirements:
MCQ
Handout
Statistical/ Log Tables
Cambridge Tables
Graph Paper
Log Graph Paper
Other Materials

Release to Library: Yes

PTO

1

(a) Describe the process of capturing information from a suspect PC using the headings (1) sanitizing the forensic disk (2) imaging the suspect disk (3) hashing (4) disk analysis (8 marks)

(b) Discuss the importance of trustworthy (received:) headers in email (6 marks)

(c) A suspect disk contains a scrubbing program. In your opinion does this mean that all hope of recovering any data whatsoever is gone? (6 marks)

2

(a) Give any five properties that a hash function should satisfy (6 marks)

(b) Outline the number theory that underlies an RSA asymmetric encryption scheme, explaining what is meant by Euler's totient (or Phi) function in the course of your discussion (8 marks)

(c) Sketch how a period-finding routine might be used by a quantum computer to defeat an RSA scheme (6 marks)

3

(a) Give your understanding of Public Key Infrastructure using the headings (1) Registration Authority (2) Certification Authority (3) Certificate Revocation List and OCSP (4) Digital Signature (8 marks)

(b) There is a suggestion that your key generation mechanism is not generating sufficiently random material. By considering recent work at EFF and Michigan, or otherwise, discuss the implications of this situation. (6 marks)

(c) Tom has hashed a file for 'authentication purposes' and then encrypted this file with Mary's public key for 'confidentiality purposes'. Tom believes that he can still decrypt this message. Advise on this particular use of hashes and keys. (6 marks)

4

(a) Discuss any three areas that you would expect to be addressed in a typical corporate security policy document for an SME. (6 marks)

(b) Your company has decided to implement a Chinese Wall policy. Explain what this policy means. (6 marks)

(c) You are to review security policy in two environments. In the first, information leakage is considered the biggest risk; in the second untrustworthy information has been identified as a high risk factor. In which environment would you expect that (1) a no write down policy and (2) a no write up policy would be in place? (8 marks)

<u>**PTO**</u>

5

(a) Explain what is meant by the terms (1) Confidentiality (2) Integrity and (3) Availability (6 marks)

(b) Your company has decided to mandate whole-disk encryption. Give one argument in favour of and one argument against this decision. (8 marks)

(c) What do you understand by the terms 'Annual Loss Expectancy' and 'Acceptable Loss'? Consider a formal risk analysis that produces a prioritised table of identified risks. Do you agree that mitigation measures that have a low cost and high impact should appear towards the top of this table? (6 marks)

6

(a) Solid State Drive technology poses problems for current forensic practice – do you agree? (8 marks)

(b) A suspect claims that they cannot remember the password for an encrypted document. What options are available to you as an investigator? (6 marks)

(c) You are tasked with explaining to bank staff how a phishing attack works. Briefly outline the main points that you would expect to make in connection. (6 marks)

7

"Personal information is increasingly available to interested parties through things like social networking sites and smartphone-resident information mined by downloaded apps." Discuss this statement. (20 marks)

Semester II Examinations 2012/ 2013

Exam Code(s)	4IF1
Exam(s)	Bachelor of Science in Information Technology
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	
Repeat Paper	No
Discipline(s)	Information Technology
Course Co-ordinator(s)	
Internal Examiner(s)	Professor G Lyons Dr. M Madden Dr. C Mulvihill*
External Examiner(s)	Professor M. O'Boyle
No. of Pages	3
Duration	**3 hours**
Instructions:	Attempt any four questions. All questions will be marked equally.

Requirements:
MCQ
Handout
Statistical/ Log Tables
Cambridge Tables
Graph Paper
Log Graph Paper
Other Materials

Release to Library: Yes

PTO

1

(a) Develop an intuitive explanation of the mathematics that underlies RSA, touching on the Euler-Fermat theorem in the course of your answer. (8 marks)

(b) 'So–called *probabilistic encryption*, such as is found in ElGamal (key elements) and in RSA-OAEP (padding) can make an exhaustive plaintext attack difficult'. By considering a domain containing only limited plaintexts, outline why such an attack is less likely to succeed if such encryption is employed. (6 marks)

(c) Alice encrypts an assignment with Bob's public encryption key. She then signs the encrypted assignment with her private signature key. Both the encrypted assignment and the signature are then sent to Bob in a message. This is intercepted. An attacker replaces Alice's signature with his and then forwards the message to Bob. Is this possible in your view and, if so, advise Alice on how to deal with this scenario. (6 marks)

2

(a) Give your understanding of the term 'Feistel Cipher'. (6 marks)

(b) A block cipher can be operated in so-called *electronic codebook* mode. Discuss any one attack against this mode of operation, suggesting when it might be useful. (6 marks)

(c) 'In so-called *cipher feedback* mode, decryption of a block cipher takes place using the encryption algorithm of the block cipher' Explain why this is so. (8 marks)

3

(a) Consider a new electronic commerce application implementing a *first-price sealed bid* auction, where each party submit exactly one secret bid and the highest one wins. In the application, parties in fact submit a hash of their bid as a commitment. After the competition closes, they are required to reveal their actual bids. Suppose that there are exactly two bidders, Alice and Bob. Show how knowledge of a hashing collision could give Bob an advantage if Alice reveals her bid first. (8 marks)

(b) 'To achieve non-repudiation with symmetric keys in the context of message authentication codes a trusted third party should be employed'. Sketch how this might work. (6 marks)

(c) In the context of low-level penetration tests of a company, explain what is meant by the term 'ARP cache poisoning' and list one way it could be used as an attack and one way to prevent it. (6 marks)

PTO

4

(a) In connection with FIPS PUB 140-2, security requirements for cryptographic modules, distinguish briefly between non-deterministic and deterministic random number generators. Why in your view are there no FIPS approved non-deterministic random number generators? (8 marks)

(b) Freshness in a communication is generally provided by clock, sequence number, or nonce mechanisms. Explain any one of these three schemes. (6 marks)

(c) Give a brief account of zero-knowledge entity authentication using any example of your own devising to illustrate the relevant probabilities. Explain the term 'independent event' in the course of your answer. (6 marks)

5

(a) Give your understanding of the three terms confidentiality, integrity and availability in the context of computer security. (6 marks)

(b) What type of access environment might be expected to enforce 'no read up' (the ss-property) and 'no write down' (the *-property) between subjects and objects? Explain what is meant by 'no read up' and 'no write down' in the course of your answer. (6 marks)

(c) The hospital is considering installing and customising a computer system for patient records. They have identified integrity of data as the single most important issue for their domain. Would a scheme such as that in **5 (b)** be the most suitable for their needs? If not, what would you suggest? (8 marks)

6

(a) Explain what is meant by the 'Daubert Criteria' and why they apply to computer forensics. (6 marks)

(b) You have been told that a well-known steganographic program has been downloaded by an employee in your organisation. Would you consider this worthy of investigation and, if so, how would such an investigation be likely to proceed in the light of your company's policies and procedures? (6 marks)

(c) 'Recent work by Müller and Spreitzenbarth has shown that RAM contents from smartphones can be recovered via cold boot attacks'. Discuss the implications of this statement. (8 marks)

7

'Embedded devices, logs and large-scale data mining lead to a future where there is no privacy'. Discuss this statement. (20 marks)

NUI Galway
OÉ Gaillimh

Autumn Examinations 2012/ 2013

Exam Code(s)	4IF1
Exam(s)	Bachelor of Science in Information Technology
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	
Repeat Paper	Yes
Discipline(s)	Information Technology
Course Co-ordinator(s)	
Internal Examiner(s)	Professor G Lyons Dr. M Madden Dr C Mulvihill*
External Examiner(s)	Professor M. O'Boyle
No. of Pages	3
Duration	**3 hours**
<u>Instructions</u>:	Attempt any four questions. All questions will be marked equally.

Requirements:
MCQ
Handout
Statistical/ Log Tables
Cambridge Tables
Graph Paper
Log Graph Paper
Other Materials

Release to Library: Yes

PTO

1

(a) Describe the process of capturing information from a suspect PC using the headings (1) sanitizing the forensic disk (2) imaging the suspect disk (3) disk analysis (8 marks)

(b) Discuss the importance of trustworthy (received:) headers in email (6 marks)

(c) A suspect disk contains a scrubbing program. In your opinion does this mean that all hope of recovering any data whatsoever is gone? (6 marks)

2

(a) Give any three properties that a hash function should satisfy (6 marks)

(b) Outline the number theory that underlies an RSA asymmetric encryption scheme, explaining what is meant by Euler's totient (or Phi) function in the course of your discussion (8 marks)

(c) Give your understanding of the term ‘freshness’ (6 marks)

3

(a) Give your understanding of Public Key Infrastructure using the headings (1) Registration Authority (2) Certification Authority (3) Certificate Revocation List (4) Public and private keys (8 marks)

(b) You are told that a certificate is untrusted. What does this mean? (6 marks)

(c) Tom has hashed a file for 'authentication purposes' and then encrypted this file with Mary's public key for 'confidentiality purposes'. Tom believes that he can still decrypt this message. Advise on this particular use of hashes and keys. (6 marks)

4

(a) Discuss any three areas that you would expect to be addressed in a typical corporate security policy document for an SME. (6 marks)

(b) Your company has decided to pilot a two-factor authentication scheme. Explain what this means (6 marks)

(c) You are to provide advice on security policy in an organisation. The organisation prizes data integrity above all else. Discuss what read/write policy you might consider appropriate for this environment (8 marks)

PTO

5
(a) Explain what is meant by the terms (1) Confidentiality (2) Integrity and (3) Availability (6 marks)
(b) In an hierarchical environment that prizes confidentiality above all else, discuss what read/write policy you might expect to find in place. (8 marks)
(c) Give your understanding of the term ‘Chinese wall’ (6 marks)

6
(a) Discuss any one problem that Solid State Drive technology poses for current forensic practice (8 marks)
(b) A suspect claims that they cannot remember the password for an encrypted file. Discuss any three options that may be available to you as an investigator (6 marks)
(c) You are tasked with outlining to staff how an ARP cache poisoning attack works. Briefly outline the main points that you would expect to make in connection. (6 marks)

7
“Smartphones and social networking have almost eliminated privacy for many people.” Discuss this statement. (20 marks)

NUI Galway
OÉ Gaillimh

Semester 2 Examinations 2013/ 2014

Exam Code(s)	4BCT1
Exam(s)	BSc in Computer Science and Information Technology
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	1
Repeat Paper	No
External Examiner(s)	Dr. J. Power
Internal Examiner(s)	Prof. G. Lyons Dr. M. Madden *Dr. C. Mulvihill

Instructions: Answer any 4 questions.
All questions will be marked equally.

Duration	2 hours
No. of Pages	2
Discipline(s)	Information Technology
Course Co-ordinator(s)	

Requirements:

MCQ	Release to Library: Yes ☒ No □
Handout	None
Statistical/ Log Tables	None
Cambridge Tables	None
Graph Paper	None
Log Graph Paper	None
Other Materials	None
Graphic material in colour	Yes □ No ☒

PTO

1

(a) What is meant by the terms ‘stream cipher’ and ‘block cipher’? (4 marks)

(b) 'Block ciphers are found with many modes of operation such as Cipher Feedback Mode, Cipher Block Chain, and Counter Mode.’ Give an account of Counter Mode, giving any one advantage and any one disadvantage that you see with this mode of operation (6 marks)

(c) You have been asked to review a student project proposal for a stream cipher. The proposal reads: ‘A plaintext message is enciphered with our own stream cipher. There is a keystream that performs an XOR with each plaintext bit. The plaintext is recovered by performing a further XOR on the ciphertext with the same keystream. The keystream is in fact a repeating short key (currently a byte); our group does not see any need whatsoever at this time for a so-called keystream generator.’ Advise the group on the state of their proposal. (10 marks)

2

(a) ‘Public-key systems often depend on so-called trapdoor one-way functions’. Explain what is meant by the term ‘trapdoor one-way function’ (4 marks)

(b) In the context of public-key cryptography, explain what is meant by the terms ‘public key’, ‘private key’ and ‘certification authority’(6 marks)

(c) Alice is working on an assignment for her tutor Emma. Alice decides to consult Bob, who is in her class. Alice signs her assignment work with her private signature key. She then encrypts all of this with Bob's public encryption key. She sends the resulting message to Bob for comments. Bob decrypts the message and reads the assignment work. He finds an error but instead of informing Alice, he encrypts the signed assignment with Emma’s public key and sends it on. Emma believes that the assignment work is from Alice and Alice receives a low grade. Advise Alice on how to deal with this scenario (10 marks)

3

(a) Distinguish between a hash function and a MAC (message authentication code) (5 marks)

(b) 'To achieve data origin authentication for a digital signature scheme with a symmetric MAC key, a trusted third party (ttp) or arbitrator should be employed'. By considering two parties communicating via a ttp, illustrate the operation of such a scheme. (7 marks)

(c) ‘An RSA digital signature with appendix involves the use of a hash function’. Give a brief account of how signing and verification works with such a scheme. (8 marks)

PTO

4
(a) ‘A dynamic password scheme often involves a challenge and a response, and the use of a so-called token that implements a password function and an associated key.’ Briefly outline the operation of such a scheme (6 marks)

(b) Freshness in a communication is sometimes provided by a clock, perhaps also by sequence numbers, or sometimes through nonce mechanisms. Mention any one special requirement for each of these three schemes. (6 marks)

(c) Briefly outline what is meant by ‘zero-knowledge entity authentication’, using any analogy of your choice to illustrate your answer. (8 marks)

5
(a) Give your understanding of the terms confidentiality, integrity, and availability in the context of computer security. (6 marks)

(b) What type of access environment might be expected to enforce 'no write up' and 'no read down' modes between subjects and objects? Explain what is meant by 'no read down' and 'no write up' in the course of your answer. (6 marks)

(c) Your organisation is considering installing and customising an infrastructure for criminal investigations. Confidentiality of data has been identified as the single most important issue to be addressed. Would access modes such as that in **5 (b)** be the most suitable? If not, what would you suggest? (8 marks)

6
(a) Explain what is meant by the 'Daubert Criteria' and discuss why they are considered relevant in the context of computer forensics. (6 marks)

(b) You are an IT officer for a medium-sized Irish company and have found a steganographic program on a copy of a hard disk that originates from a laptop associated with an office housing several junior employees. Your organisation is heavily involved in confidential IP negotiations at this time, and the security policy in place does not permit such software to be in the possession of such employees. In the light of your understanding of security policies, what response or responses would you consider appropriate? (6 marks)

(c) Give an account of the importance of email headers in network forensics.
(8 marks)

7
“Cryptographic protocols are often to be found on the Internet.” Discuss this statement with reference to the handshake (8 marks) and record (8 marks) protocols of SSL, explaining the term ‘protocol’ (4 marks) in the course of your answer.
(20 marks in total)

Semester 2 Examinations 2014/ 2015

Exam Code(s)	4BCT1, 1SWB1
Exam(s)	Year 4 BSc in Computer Science and Information Technology, Science without Borders
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	1
Repeat Paper	No
External Examiner(s)	Dr. J. Power
Internal Examiner(s)	Prof. G. Lyons Dr. M. Madden *Dr. C. Mulvihill

Instructions: Answer any 4 questions.
All questions will be marked equally.

Duration	2 hours
No. of Pages	3
Discipline(s)	Information Technology
Course Co-ordinator(s)	Dr. D. Chambers

Requirements:

Release in Exam Venue	Yes	☒	No	□
MCQ	Yes	□	No	☒
Handout	None			
Statistical/ Log Tables	None			
Cambridge Tables	None			
Graph Paper	None			
Log Graph Paper	None			
Other Materials	None			
Graphic material in colour	Yes	□	No	☒

PTO

1
(a) What is meant by the term ‘block cipher’? (4 marks)

(b) Develop a simple model of the operation of a stream cipher, explaining the term ‘keystream generator’ in the course of your answer. (6 marks)

(c) Discuss any two ciphertext manipulations that could occur if deploying a block cipher in ECB (Electronic Code Book) mode. (10 marks)

2
(a) Briefly explain what is meant by a MAC (message authentication code).(5 marks)

(b) 'Digital signatures are about delivering a service aimed at data integrity and are not about encryption’. Explain what is meant by this claim. (7 marks)

(c) ‘MAC algorithms could be based on a block cipher or a hash function’. Give a brief overview of either CBC-MAC or HMAC in the light of this statement.
(8 marks)

3
(a) Briefly compare clock-based and sequence-based freshness mechanisms.(6 marks)

(b) ‘Dynamic password schemes can address freshness and identity requirements through the use of PINs, tokens and challenge-response mechanisms.’ Outline how authentication between a server and a user might work with such a scheme. (6 marks)

(c) Briefly outline what is meant by ‘zero-knowledge entity authentication’, using any analogy of your choice to illustrate your answer. (8 marks)

4
(a) ‘Public-key systems often depend on a trapdoor one-way function.’ Explain what is meant by this statement. (4 marks)

(b) In the context of public-key cryptography, explain what is meant by the terms ‘X.509 public key certificate’ and ‘Certification Authority’. (6 marks)

(c) Alice is working on an assignment for her tutor Emma. Alice signs her assignment with her private signature key. She decides to consult Bob, who is in her class. Alice encrypts her signed assignment with Bob’s public encryption key and sends the signed and encrypted assignment to Bob for a second opinion. Bob decrypts with his private decryption key, verifies Alice’s signature with her public verification key, notices a flaw in the assignment, but sends the assignment on to Emma encrypted with Emma’s public encryption key. As Alice signed the assignment she gets a low mark. Is there any way that this scenario can be counteracted? (10 marks)

PTO

5

(a) Explain what is meant by the terms ‘confidentiality’ and ‘integrity’ in the context of computer security. (6 marks)

(b) Briefly outline the ‘Chinese Wall’ model of access control, explaining what is meant by the term ‘conflict of interest classes’ in the course of your answer.
(8 marks)

(c) What type of access control environment might be expected to enforce the so-called 'no read up' and 'no write down' (aka the ss-property and the *-property) access control properties between subjects and objects? Explain what is meant by 'no read up' and 'no write down' in the course of your answer. (6 marks)

6

(a) Briefly describe the following aspects of dealing with a suspect device: (1) sanitizing forensic disks (2) data carving and (3) examining log files. (9 marks)

(b) Explain the relevance of the ‘Daubert Criteria’ for computer forensics. (5 marks)

(c) ‘The presence of steganographic material on a device may lead to the defence of plausible deniability being invoked.’ Explain what is meant by this statement in the context of a forensic investigation. (6 marks)

7

In the context of the discussion found in the recent paper ‘Surreptitiously weakening cryptographic systems’ by Schneier, Fredrikson, Kohno and Ristenpart, or through your own investigations, briefly give your understanding of the following four cases: Lotus Notes, Dual Elliptic Curve DRBG, Debian OpenSSL PRNG, certificate checking double goto. (5 marks for each of the four - 20 marks in total)

NUI Galway
OÉ Gaillimh

Semester 2 Examinations 2015/ 2016

Exam Code(s)	4BCT1, 1SWB1, 1OA1, 4BS2
Exam(s)	Year 4 BSc in Computer Science and Information Technology, Science without Borders, Occasional Students, Fourth Science
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	1
Repeat Paper	No
External Examiner(s)	Dr. J. Power
Internal Examiner(s)	Prof. G. Lyons Dr. J. Duggan *Dr. C. Mulvihill

Instructions: Answer any 3 questions.
All questions will be marked equally.

Duration	2 hours
No. of Pages	3
Discipline(s)	Information Technology
Course Co-ordinator(s)	Dr. D. Chambers

Requirements:

Release in Exam Venue	Yes	☒	No	□
MCQ	Yes	□	No	☒
Handout	None			
Statistical/ Log Tables	None			
Cambridge Tables	None			
Graph Paper	None			
Log Graph Paper	None			
Other Materials	None			
Graphic material in colour	Yes	□	No	☒

PTO

1

(a) Hash functions should be easy to compute and they should convert input of arbitrary size into a fixed-size output. In addition, they should provide three security properties: Pre-image resistance, second pre-image resistance and collision resistance. Explain what is meant by each of these security properties. (8 marks)

(b) A Message Authentication Code (MAC) differs from a hash function in that it has a symmetric key associated with it. In terms of security services, what in your view does a MAC provide that is not available with a hash function? (8 marks)

(c) Consider a digital signature scheme that involves a trusted arbitrator (A), a signer (S), and a verifier (V). A symmetric MAC key (K-SA) is shared by the signer and the arbitrator. Another such MAC key (K-AV) is shared between the arbitrator and the verifier. Sketch how a message should be transmitted from the signer to the verifier in such a scheme, and determine whether such a scheme can provide a non-repudiation service in the event that the signer S denies sending the message. (9 marks)

2

(a) 'A stream cipher can be viewed as performing bit-by-bit encryption on the plaintext using a keystream. Bit-by-bit decryption is then performed at the receiver.' By considering the expression Ci == Pi XOR Ki , where C is ciphertext, P is plaintext, K represents the keystream, XOR is exclusive-or, and i represents the current bit, explain how decryption works in such a scheme. (8 marks)

(b) In terms of strengthening a typical block cipher by introducing message dependency, outline how encryption and decryption work for the mode of operation known as Cipher Block Chain (CBC). (8 marks)

(c) 'A padding oracle attack is a very powerful way to attack a block cipher.' By considering an initialisation vector IV, and the first two blocks of ciphertext C1 and C2, explain how a padding oracle attack might work against an encryption service running in CBC mode. Assume that the blocksize is eight bytes. (9 marks)

3

(a) 'In order to provide an authentication service, one, two and three factor authentication can be employed for identifying an entity.' Explain what is meant by each of the terms 'one factor', 'two factor' and 'three factor' authentication. (8 marks)

(b) 'In addition to identifying an entity, in order to avoid replay attacks there should be some assurance of freshness in a communication. Freshness is often provided by a nonce.' Explain what is meant by the term 'nonce' and sketch how a nonce is employed to provide an assurance of freshness to a relying party. (8 marks)

(c) A bank uses a dynamic password scheme for authentication. Tokens (with keypads and screens) have been issued to customers. A customer accesses their bank account online. A challenge is issued to their mobile phone. Outline any one way such a scheme might operate, explaining the role of the challenge, the token and the response in the course of your answer. (9 marks)

PTO

4

(a) ‘Public key encryption services such as RSA, ElGamal and Elliptic Curve rely on the apparent hardness of things like factorisation, extracting modulo roots, or solving a discrete log problem.’ In terms of an RSA encryption service using public keys and private keys, explain in operational terms how a message is encrypted and decrypted, briefly explaining the terms ‘Certification Authority’ and ‘Public Key Certificate’ in the course of your answer. (8 marks)

(b) ‘In connection with authentication, the fact that a man-in-the middle attack can succeed against Diffie-Hellman shows that a typical goal such as mutual entity authentication may not been achieved.’ Outline how a protocol based on Diffie-Hellman such as STS (station-to-station) achieves mutual entity authentication by employing an established signature/verification key pair. (8 marks)

(c) ‘Alice signs a draft message intended for Eve with her private signature key. She then encrypts the message with Bob’s public encryption key and sends it to her assistant Bob for comment. Bob decrypts the message with his private decryption key and verifies that it came from Alice with Alice’s public verification key. Bob then sends the message on to Eve directly using her public encryption key, pointing out numerous errors. The trust between Alice and Bob is abused here. Eve thinks that the message came from Alice (which it did), but that no-one else saw it (but Bob did).’ Outline any one way that Alice could ensure that the draft status of her message to Eve is clear to all parties. (9 marks)

5

(a) In terms of computer forensics, explain what is meant by the term ‘order of volatility’ in the context of collecting computer evidence. (7 marks)

(b) ‘Storage in the so-called ‘Cloud’ can lead to many problems for computer forensics.’ By considering NISTIR 8006 Cloud Computing Forensic Science Challenges, or otherwise, outline any three challenges that you view as significant at this time. (9 marks)

(c) ‘Steganography provides many challenges for forensic work, not the least of which is detecting it in the first place.’ Give you understanding of the term ‘steganography’, discuss any one way you might attempt to detect its presence, and explain why the defence of plausible deniability is sometimes employed in connection with steganography. (9 marks)

6

‘There is a balance to be struck between security and privacy. This is all the more so as we move into a world of devices and the Internet of Things.’ By considering Landau’s presentation to Congress on 1 March 2016, or otherwise, discuss this statement from the following three perspectives: Security threats (8 marks), encryption (8 marks), and securing devices such as smartphones (9 marks.)

Autumn Examinations 2015/ 2016

Exam Code(s)	4BCT1, 1SWB1
Exam(s)	Year 4 BSc in Computer Science and Information Technology, Science without Borders
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	1
Repeat Paper	Yes
External Examiner(s)	Dr. J. Power
Internal Examiner(s)	Prof. G. Lyons Dr. J. Duggan *Dr. C. Mulvihill

Instructions: Answer any 3 questions.
All questions will be marked equally.

Duration	2 hours
No. of Pages	3
Discipline(s)	Information Technology
Course Co-ordinator(s)	Dr. D. Chambers

Requirements:

Release in Exam Venue	Yes	☒	No	□
MCQ	Yes	□	No	☒
Handout	None			
Statistical/ Log Tables	None			
Cambridge Tables	None			
Graph Paper	None			
Log Graph Paper	None			
Other Materials	None			
Graphic material in colour	Yes	□	No	☒

PTO

1

(a) What is meant by the term ‘block cipher’? (4 marks)

(b) 'Block ciphers are found with many modes of operation such as Cipher Feedback Mode, Cipher Block Chain, and Counter Mode.’ Give an account of the Cipher Block Chain mode of operation (6 marks)

(c) Discuss the security elements that are present in any online student service with which you are familiar (10 marks)

2

(a) ‘Public-key systems often depend on the apparent hardness of certain problems.’ Explain what is meant by this statement (4 marks)

(b) In the context of public-key cryptography, explain what is meant by the terms ‘registration authority’, ‘revocation list’ and ‘certification authority’. (6 marks)

(c) Alice is working on an assignment for her tutor Emma. Alice signs her assignment with her private signing key. Alice then encrypts this with Bob’s public encryption key and sends the assignment to Bob (who is in her class) for comment. Bob finds errors but instead of returning the assignment, he encrypts the signed assignment with Emma’s public encryption key and sends it on to Emma. So Alice signed it, but Bob sent it. Outline two approaches to dealing with this situation. (10 marks)

3

(a) ‘Two-factor authentication can be more secure than single factor.’ Briefly outline what is meant by two-factor authentication. (6 marks)

(b) ‘Nonce mechanisms provide freshness’. Explain how nonce mechanisms work. (6 marks)

(c) Give your understanding of the principles behind ‘zero-knowledge entity authentication’, using any analogy of your choice to illustrate your answer. (8 marks)

<u>PTO</u>

4

(a) Explain what is meant by the terms (1) Data origin authentication (2) Non-repudiation (6 marks)

(b) Give an account of the any one challenge-response scheme (for example, a login session with a bank or an authorisation via a payment card) with which you are familiar. (8 marks)

(c) What type of access environment might be expected to enforce 'no write up' and 'no read down' modes of operation between subjects and objects? Explain what is meant by 'no write up' and 'no read down' in the course of your answer. (6 marks)

5

(a) List any three challenges for cloud forensics (8 marks)

(b) Explain the relevance of the so-called ‘Daubert Criteria’ in computer forensics (6 marks)

(c) A laptop that has been returned by an employee now has a steganographic program on it. This was not there when the machine was released. In your opinion does this situation warrant further investigation? (6 marks)

6

“Information that people imagine to be private is increasingly available through social networking environments and search engines. Sometimes this information can even be changed”. Discuss this statement from the perspectives of confidentiality (7 marks), integrity (7 marks) and availability (6 marks).

Semester Two Examinations 2016/2017

Exam Code(s)	4BCT1, 1MECE1
Exam(s)	Year 4 BSC in Computing Science and Information Technology, Masters in Electronic and Computer Engineering
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	1
Repeat Paper	No
External Examiner(s)	Dr. J. Power
Internal Examiner(s)	Dr. M. Schukat *Dr. C. Mulvihill

Instructions: Answer any 3 questions.
All questions will be marked equally.

Duration	2 hours
No. of Pages	3
Discipline(s)	Information Technology
Course Co-ordinator(s)	Dr. D. Chambers

Requirements:

Release in Exam Venue	Yes	☒	No	□
MCQ	Yes	□	No	☒
Handout	None			
Statistical/ Log Tables	None			
Cambridge Tables	None			
Graph Paper	None			
Log Graph Paper	None			
Other Materials	None			
Graphic material in colour	Yes	□	No	☒

PTO

1 (a) Entity authentication schemes often require some evidence of freshness in a communication, and this evidence is typically provided by nonces, clock-based mechanisms or sequence numbers. Explain briefly what is meant by the three terms ‘nonces’, ‘clock-based mechanisms’ and ‘sequence numbers’ in the context of supplying evidence of freshness (9 marks)

(b) Apart from freshness, entity authentication schemes should establish evidence of identity. A zero-knowledge scheme should allow a prover to convince a verifier of the identity of the prover without enabling the verifier to later impersonate the prover. Using any analogy of your own choosing, sketch at a high level how such a scheme might operate (8 marks)

(c) Consider a simple protocol for checking on the ‘liveness’ of Alice that involves the exchange of two messages. Bob, the checker, sends a message CHECK to Alice that contains a nonce and a query. Alice’s reply contains the message CHECK and a Message Authentication Code computed on the message CHECK. Find any one flaw in this scheme for Bob’s checking on the ‘liveness’ of Alice, and suggest how the flaw might be addressed (8 marks)

2 (a) In the context of scientific evidence, the so-called ‘Daubert’ criteria list four things that should be considered in order to have confidence that evidence supplied by some investigative technique is reliable. In your view how do these criteria impact on mobile forensic investigations? (8 marks)

(b) You are an IT officer for an organisation that is subject to considerable regulatory oversight and that has subscribed to very strict policies on information leakage. In the course of a routine examination of a laptop that was issued to a member of a team working on a recent case, you have found artefacts that indicate that a steganographic program was once present on the machine. Discuss whether in your view this discovery warrants further investigation, sketch what procedure you might follow if it does, and in the alternative sketch how you would close your examination if it does not (9 marks)

(c) Outline any two challenges that you think face digital forensics through the emergence of the ‘Internet of Things’ (8 marks)

3

Consider the document ‘Framework for Improving Critical Infrastructure Cybersecurity’, released by the National Institute of Standards and Technology (NIST) as draft version 1.1 in January 2017. The framework presented in this document is, as stated in the document, a ‘risk-based approach to managing cybersecurity risk’. Give your understanding of this framework under the three headings ‘Framework Core’ (9 marks), ‘Framework Implementation Tiers’ (8 marks) and ‘Framework Profile’ (8 marks).

4 (a) ‘A hash function is associated with notions of data integrity’. Give three security properties that a hash function should satisfy, and briefly indicate any one application area where in your view such security properties are needed (9 marks)

(b) Message Authentication Codes differ from a hash function in that they employ a shared key and a hash function (as such) has no key. From a security perspective, what, if anything, does a message authentication code offer that a hash function does not in your view? (8 marks)

(c) In one public-key digital signature scheme that provides for data origin authentication and non-repudiation, the hash of a long message M is signed and then the message and the hash are sent to the receiver. Suppose that a new scheme is proposed where a message M is decomposed into two small sub-units M1 and M2 and that M1 and M2 are individually signed and sent to the receiver. It is suggested that this is a better scheme in that it does not need a hash function. Is this proposed new scheme vulnerable in a way that the hashed scheme isn’t in your view? (8 marks)

5 (a) By considering the plaintext ‘010101’ and an associated key ‘111111’, explain the principle underlying encryption and decryption for a simple stream cipher that depends on a randomly generated keystream and XOR (8 marks)

(b) ‘Block ciphers work on blocks rather than bits’. With the aid of a diagram, show one encryption round for either a generic Feistel cipher or the AES block cipher (8 marks)

(c) Consider a security solution that provides a confidentiality service via a block cipher deployed in Cipher Block Chain (CBC) mode and also an integrity service delivered via so-called ‘CBC-MAC’. Discuss whether this scheme is vulnerable to a Message Authentication Code (MAC) forgery attack if the same key is used for both the confidentiality service and the integrity service. You may assume that a message consists of N blocks and that an attacker has changed all enciphered blocks apart from the last one (9 marks)

6 (a) In the context of a public key encryption scheme such as RSA, explain what is meant by the terms ‘private key’, ‘public key’ and ‘digital certificate’ (9 marks)

(b) Apart from specialised attacks, an encryption scheme such as RSA depends in general on the assumed ‘hardness’ of certain problems which are believed to give rise to ‘one-way’ functions. Briefly outline any two such problems that RSA relies on, explaining the term ‘one-way function’ in the course of your answer (8 marks)

(c) Public key schemes such as RSA are often deployed as so-called ‘hybrid encryption’ schemes, with the public key element being used to transfer a symmetric key which is subsequently used for general message encryption. By considering a long message that is to pass from Alice to Bob, briefly sketch how such a hybrid encryption scheme might operate (8 marks)

Autumn Examinations 2016/2017

Exam Code(s)	4BCT1, 1MECE1
Exam(s)	Year 4 BSC in Computing Science and Information Technology, Masters in Electronic and Computer Engineering
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	1
Repeat Paper	Yes
External Examiner(s)	Dr. J. Power
Internal Examiner(s)	Dr. M. Schukat *Dr. C. Mulvihill

Instructions: Answer any 3 questions.
All questions will be marked equally.

Duration	2 hours
No. of Pages	3
Discipline(s)	Information Technology
Course Co-ordinator(s)	Dr. D. Chambers

Requirements:

Release in Exam Venue	Yes ☒ No □
MCQ	Yes □ No ☒
Handout	None
Statistical/ Log Tables	None
Cambridge Tables	None
Graph Paper	None
Log Graph Paper	None
Other Materials	None
Graphic material in colour	Yes □ No ☒

PTO

1 (a) Explain how a nonce can be used to provide evidence of freshness in a communication between two parties (9 marks)

(b) Outline how any dynamic password scheme (e.g. challenge response) that you are familiar with can be used to provide evidence of identity in a communication between two parties (8 marks)

(c) In the absence of mutual trust, a zero knowledge scheme for entity authentication might be deployed. Outline how such a scheme works, using any analogy of your own choice. (8 marks)

2 (a) List any four criteria that a forensic investigative technique should satisfy in order to have confidence that evidence supplied by the investigative technique is reliable. (8 marks)

(b) Discuss the process of disk imaging, explaining the term 'write blocker' in the course of your answer(9 marks)

(c) Outline any two challenges that you think face digital forensics through the emergence of mobile devices (8 marks)

3

Consider the document ‘Framework for Improving Critical Infrastructure Cybersecurity’, released by the National Institute of Standards and Technology (NIST) as draft version 1.1 in January 2017. The framework presented in this document is, as stated in the document, a ‘risk-based approach to managing cybersecurity risk’. Give your understanding of this framework under the three headings ‘Framework Core’ (9 marks), ‘Framework Implementation Tiers’ (8 marks) and ‘Framework Profile’ (8 marks).

4 (a) Give any two security properties that a hash function should satisfy, and briefly indicate any application area where in your view any one such security property is needed (9 marks)

(b) What does a message authentication code (MAC) offer that a hash function does not in your view? (8 marks)

(c) Sketch how a MAC scheme could be used to provide for digital signatures, assuming the existence of a trusted third party (arbitrator) (8 marks)

5 (a) By considering the plaintext ‘011100’ and an associated key ‘000000’, explain the principle underlying encryption and decryption for a simple stream cipher that depends on a randomly generated keystream and XOR (8 marks)

(b) ‘Block ciphers work on blocks rather than bits’. With the aid of a diagram, show one encryption round for the AES block cipher (8 marks)

(c) Consider a security solution that provides a confidentiality service via a block cipher deployed in Cipher Block Chain (CBC) mode and also an integrity service delivered via so-called ‘CBC-MAC’. Discuss whether this scheme is vulnerable to a Message Authentication Code (MAC) forgery attack if the same key is used for both the confidentiality service and the integrity service. You may assume that a message consists of N blocks and that an attacker has changed all enciphered blocks apart from the last one (9 marks)

6 (a) In the context of a public key encryption scheme such as RSA, explain what is meant by the terms ‘Certification Authority’, ‘Registration Authority’ and ‘Digital Certificate’ (9 marks)

(b) Sketch in outline how an RSA digital signature scheme with appendix works (8 marks)

(c) Explain in your own words what is meant by the idea that public key encryption and public key digital signature have complementary requirenments. Make use of the terms 'sign', 'verify' 'encrypt' and 'decrypt' in the course of your answer (8 marks)

NUI Galway
OÉ Gaillimh

Semester Two Examinations 2017/2018

Exam Code(s)	4BCT1, 1MECE1, 1OA1, 1EM1
Exam(s)	Year 4 BSC in Computing Science and Information Technology, Masters in Electronic and Computer Engineering, Overseas, Erasmus
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	1
Repeat Paper	No
External Examiner(s)	Dr. Jacob Howe
Internal Examiner(s)	Prof M. Madden *Dr. C. Mulvihill

Instructions: Answer any 3 questions.
All questions will be marked equally.

Duration	2 hours
No. of Pages	3
Discipline(s)	Information Technology
Course Co-ordinator(s)	Dr. D. Chambers

Requirements:

Release in Exam Venue	Yes	☒	No	□
MCQ	Yes	□	No	☒
Handout	None			
Statistical/ Log Tables	None			
Cambridge Tables	None			
Graph Paper	None			
Log Graph Paper	None			
Other Materials	None			
Graphic material in colour	Yes	□	No	☒

PTO

1

(a) Entity authentication requires evidence of identity. This may be achieved via one, two, or three factors. Explain what is meant by each of the terms 'one factor', 'two factor' and 'three factor' authentication. (9 marks)

(b) Entity authentication also requires evidence of freshness. This can be provided by timestamps or, as one alternative, by so-called nonces. Give any one advantage and any one disadvantage of each such approach. (8 marks)

(c) Outline the steps involved in any one entity authentication scheme that is based on two-factor challenge-response between a user and a server. The scheme should make use of 'tokens' on which password functions have been implemented. (8 marks)

2

(a) The 'Daubert' criteria, in one instantiation, enumerate properties that should be possessed by a digital investigative technique in order to have confidence that evidence supplied by that technique is reliable. Outline any two of these criteria. (8 marks)

(b) Outline any two challenges that the so-called 'Internet of Things' may pose for digital forensics. (8 marks)

(c) 'Steganography presents a challenge for forensic investigators, not only from a technical perspective but also because of the possible defence of plausible deniability'. Outline why image-based steganography may be hard to find on a suspect device and explain what is meant by the term 'plausible deniability' in the course of your answer. (9 marks)

3

Consider the document 'Framework for Improving Critical Infrastructure Cybersecurity', released by the National Institute of Standards and Technology (NIST) in 2017. The framework presented in this document is, as stated in the document, a 'risk-based approach to managing cybersecurity risk'. Discuss this framework under the following three headings 'Framework Core' (9 marks), 'Framework Implementation Tiers' (8 marks), and 'Framework Profile' (8 marks).

4

(a) 'A cryptographic hash function should display preimage, second preimage and collision resistance'. Explain what is meant by each of the terms 'preimage resistance', 'second preimage resistance', and 'collision resistance'. (9 marks)

(b) Message Authentication Codes differ from a cryptographic hash function in that they employ a key. How does a key help (if it does) with data origin authentication? (8 marks)

(c) Consider an auction with sealed bids. Bids are protected by a cryptographic hash and it is this hash value that is submitted by a bidder. After the bidding process is completed the bidders reveal their bids, and these can then be checked against the submitted hashes. Suppose that the hash function employed in the auction fails to display collision resistance. Explain why the bidding process is vulnerable. (8 marks)

5

(a) By considering the sample plaintext '010101' and an associated keystream sample '011101', explain how encryption and decryption works for a stream cipher that depends on XOR. What problem would result with a keystream consisting of all zeroes for such a stream cipher? (8 marks)

(b) 'Block ciphers work on blocks rather than bits'. With the aid of a diagram, show one encryption round for <u>either</u> a generic Feistel cipher <u>or</u> the AES block cipher. (8 marks)

(c) 'A block cipher may be strengthened by introducing positional dependency'. Outline how <u>encryption</u> works for the block cipher mode of operation known as cipher block chain (CBC). Note: You do not have to consider decryption. (9 marks)

6

(a) In the context of public key infrastructure, explain what is meant by the terms 'certification authority', 'registration authority' and 'digital certificate'. (9 marks)

(b) An encryption scheme such as RSA depends in part on the assumed 'hardness' of certain problems which are believed to give rise to 'one-way' functions. Briefly outline any one such problem that RSA relies on, explaining the term 'one-way function' in the course of your answer. (8 marks)

(c) One approach to dealing with man-in-the middle attacks on Diffie-Hellman key exchange involves employing pre-existing signature/verification key pairs. Outline why such an approach might defeat man-in-the middle attacks. (8 marks)

NUI Galway
OÉ Gaillimh

Autumn Examinations 2017/2018

Exam Code(s)	4BCT1, 1MECE1
Exam(s)	Year 4 BSC in Computing Science and Information Technology, Masters in Electronic and Computer Engineering
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	1
Repeat Paper	Yes
External Examiner(s)	Dr. Jacob Howe
Internal Examiner(s)	Prof. M. Madden *Dr. C. Mulvihill

Instructions: Answer any 3 questions.
All questions will be marked equally.

Duration	2 hours
No. of Pages	3
Discipline(s)	Information Technology
Course Co-ordinator(s)	Dr. D. Chambers

Requirements:

Release in Exam Venue	Yes ☒	No □
MCQ	Yes □	No ☒
Handout	None	
Statistical/ Log Tables	None	
Cambridge Tables	None	
Graph Paper	None	
Log Graph Paper	None	
Other Materials	None	
Graphic material in colour	Yes □	No ☒

PTO

1 (a) Explain what is meant by the term 'nonce', and show how a nonce can be used to provide evidence of freshness in a communication (9 marks)

(b) Outline how any one dynamic password scheme (e.g. token-based challenge response) that you are familiar with can be used to provide evidence of identity in a communication (8 marks)

(c) Your organisation is considering moving to a two-factor authentication scheme. Currently authentication is achieved via usernames and passwords that must be at least five characters long. From a security perspective, would this proposed move be a good idea in your view? (8 marks)

2 (a) List any three criteria that a forensic investigative technique should satisfy in order to have confidence that evidence supplied by the investigative technique is reliable. (8 marks)

(b) Does steganographic software provide any special difficulties for digital forensic investigations in your view?(9 marks)

(c) Outline any two challenges that you think face digital forensics through the emergence of mobile devices (8 marks)

3

Consider the document ‘Framework for Improving Critical Infrastructure Cybersecurity’, released by the National Institute of Standards and Technology (NIST) as draft version 1.1 in January 2017. The framework presented in this document is, as stated in the document, a ‘risk-based approach to managing cybersecurity risk’. Give your understanding of this framework under the three headings ‘Framework Core’ (9 marks), ‘Framework Implementation Tiers’ (8 marks) and ‘Framework Profile’ (8 marks).

4 (a) Give any one security property that a cryptographic hash function should satisfy, and briefly indicate one application area where in your view this security property is needed (9 marks)

(b) What does a message authentication code (MAC) offer that a hash function does not? (8 marks)

(c) Sketch how a MAC scheme can provide a non-repudiation service, assuming the existence of a trusted third party (arbitrator) (8 marks)

5 (a) By considering the plaintext '011100' and an associated key '000000', explain the principle underlying encryption and decryption for a simple stream cipher that depends on a randomly generated keystream and XOR (8 marks)

(b) 'Block ciphers work on blocks rather than bits'. With the aid of a diagram, show one encryption round for the AES block cipher (8 marks)

(c) Outline what is meant by a Message Authentication Code (MAC) forgery attack. Assume that the same key has been used for a confidentiality service and an integrity service, and that both services are provided by a Cipher Block Chain (CBC) scheme. (9 marks)

6 (a) In the context of a public key encryption scheme such as RSA, explain what is meant by the terms 'Registration Authority' and 'Digital Certificate' (8 marks)

(b) Outline how an RSA digital signature scheme works (9 marks)

(c) Explain in your own words what is meant by the idea that public key encryption and public key digital signature have complementary requirements. (8 marks)

NUI Galway
OÉ Gaillimh

Semester Two Examinations 2018/2019

Exam Code(s)	4BCT1, 1MECE1, 1OA1, 1EM1
Exam(s)	Year 4 BSC in Computing Science and Information Technology, Masters in Electronic and Computer Engineering
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	1
Repeat Paper	No
External Examiner(s)	Dr. Jacob Howe
Internal Examiner(s)	Prof M. Madden *Dr. C. Mulvihill

Instructions: Answer any 3 questions.
All questions will be marked equally.

Duration	2 hours
No. of Pages	2
Discipline(s)	Information Technology
Course Co-ordinator(s)	Dr. D. Chambers

Requirements:

Release in Exam Venue	Yes	☒	No	□
MCQ	Yes	□	No	☒
Handout	None			
Statistical/ Log Tables	None			
Cambridge Tables	None			
Graph Paper	None			
Log Graph Paper	None			
Other Materials	None			
Graphic material in colour	Yes	□	No	☒

PTO

1 (a) Define three security properties that are associated with cryptographic hash functions. (9 marks)

(b) Discuss any one application that might require second preimage resistance (8 marks)

(c) What is given by a message authentication code (MAC) that is not given by a cryptographic hash function? (8 marks)

2 (a) In an authentication scheme, what options are generally found for identifying a party and which option is commonly found with bank terminals? (5 marks)

(b) Explain how a nonce provides evidence of freshness in a communication (5 marks)

(c) Outline the operation of a zero-knowledge authentication scheme using any analogy of your own choice (15 marks)

3 (a) Provide a short overview of a simple stream cipher and explain how the plaintext is recovered from the ciphertext (listing any assumption you make for XOR) (10 marks)

(b) Distinguish between the block cipher modes of operation known as cipher feedback mode and cipher block chain in terms of how they handle encryption. Which behaves more like a stream cipher? (5 marks)

(c) Show how a padding oracle attack works on the last byte in cipher block chain decryption (10 marks)

4 (a) In terms of Public Key Infrastructure (PKI), explain what is meant by the terms 'public key' 'private key', and 'digital certificate' (9 marks)

(b) Differentiate between encryption services and signing services (8 marks)

(c) Briefly explain the purpose of DNSSEC, Registry Lock, Certificate Transparency Logs, Extensible Provisioning Protocol (8 marks)

5 (a) In the context of computer forensics, explain what is meant by the Daubert criteria (9 marks)

(b) What is meant by the term 'steganography' and list any three environments where it could be found? (8 marks)

(c) How does steganalysis help with steganography? List any two approaches an administrator might deploy to help with steganography? (8 marks)

6

By considering the recent paper in ACM Queue by Waldo, or otherwise, discuss Blockchain under the headings:
(a) ledger (5 marks)
(b) reward (5 marks)
(c) trusted versus trustless systems (15 marks)

NUI Galway
OÉ Gaillimh

Autumn Examinations 2018/2019

Exam Code(s)	4BCT1, 1MECE1
Exam(s)	Year 4 BSC in Computing Science and Information Technology, Masters in Electronic and Computer Engineering
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	1
Repeat Paper	Yes
External Examiner(s)	Dr. Jacob Howe
Internal Examiner(s)	Prof. M. Madden *Dr. C. Mulvihill

Instructions: Answer any 3 questions.
All questions will be marked equally.

Duration	2 hours
No. of Pages	3
Discipline(s)	Information Technology
Course Co-ordinator(s)	Dr. D. Chambers

Handout	None
Statistical/ Log Tables	None
Cambridge Tables	None
Graph Paper	None
Log Graph Paper	None
Other Materials	None

Requirements:
Release in Exam Venue Yes ☒ No □
MCQ Yes □ ☒ No

Graphic material in colour Yes □ No ☒

PTO

1 (a) Explain what is meant by the term 'nonce', and show how a nonce can be used to provide evidence of freshness in a communication (9 marks)

(b) Outline how any one dynamic password scheme (e.g. token-based challenge response) that you are familiar with can be used to provide evidence of identity in a communication (8 marks)

(c) Your organisation is considering moving to a two-factor authentication scheme. Currently authentication is achieved via usernames and passwords that must be at least five characters long. From a security perspective, would this proposed move be a good idea in your view? (8 marks)

2 (a) List any three criteria that a forensic investigative technique should satisfy in order to have confidence that evidence supplied by the investigative technique is reliable. (8 marks)

(b) Does steganographic software provide any special difficulties for digital forensic investigations in your view?(9 marks)

(c) Outline any two challenges that you think face digital forensics through the emergence of mobile devices (8 marks)

3

Consider the document ‘Framework for Improving Critical Infrastructure Cybersecurity’, released by the National Institute of Standards and Technology (NIST) as draft version 1.1 in January 2017. The framework presented in this document is, as stated in the document, a ‘risk-based approach to managing cybersecurity risk’. Give your understanding of this framework under the three headings ‘Framework Core’ (9 marks), ‘Framework Implementation Tiers’ (8 marks) and ‘Framework Profile’ (8 marks).

4 (a) Give any one security property that a cryptographic hash function should satisfy, and briefly indicate one application area where in your view this security property is needed (9 marks)

(b) What does a message authentication code (MAC) offer that a hash function does not? (8 marks)

(c) Sketch how a MAC scheme can provide a non-repudiation service, assuming the existence of a trusted third party (arbitrator) (8 marks)

5 (a) By considering the plaintext ‘011100’ and an associated key ‘000000’, explain the principle underlying encryption and decryption for a simple stream cipher that depends on a randomly generated keystream and XOR (8 marks)

(b) ‘Block ciphers work on blocks rather than bits’. With the aid of a diagram, show one encryption round for the AES block cipher (8 marks)

(c) Outline what is meant by a Message Authentication Code (MAC) forgery attack. Assume that the same key has been used for a confidentiality service and an integrity service, and that both services are provided by a Cipher Block Chain (CBC) scheme. (9 marks)

6 (a) In the context of a public key encryption scheme such as RSA, explain what is meant by the terms ‘Registration Authority’ and ‘Digital Certificate’ (8 marks)

(b) Outline how an RSA digital signature scheme works (9 marks)

(c) Explain in your own words what is meant by the idea that public key encryption and public key digital signature have complementary requirements. (8 marks)

Semester II Examinations, 2021/2022

Exam Code(s) 4BCT1, 1MECE1, 1OA1, 1EM1

Exam(s) Year 4 BSC in Computing Science and Information Technology, Masters in Electronic and Computer Engineering

Module Code(s) CT437

Module(s) Computer Security and Forensic Computing

Paper No. 1

Repeat Paper

Special Paper

External Examiner(s) Dr. Ramona Trestian

Internal Examiner(s) Professor Michael Madden
*Dr. Michael Schukat

Instructions:

Time allowed: **2** hours
Answer any 3 questions. All questions carry equal marks.

Duration 2 hrs

No. of Answer books 2

Requirements:

Handout

MCQ

Statistical Tables

Graph Paper

Log Graph Paper

Graphic Material in colour YES

No. of Pages 5

Discipline(s) Information Technology

Q.1.

(i) Consider NUI Galway computer services decide to setup an IPsec-based VPN (encryption only) to St. Angela's College in Co. Sligo. Additional authentication and / or encryption between endpoints may be added on demand, subject to the University's security policy. Explain in some detail, how IPsec accommodates all these requirements. In your answer, make reference to the following:

- Transport mode versus tunnel mode connections
- ESP and AH, and their respective protocol headers
- Anti-replay window
- Combined SA, with particular focus on end-to-end authentication and encryption.

[8 marks]

(ii) Distinguish between the following port scan types:

- Network ping sweeps
- TCP connect scan
- TCP SYN scan
- TCP FIN scan
- UDP scan

Using an example explain how port knocking can deter some port scans.

[5 marks]

(iii) Explain the functionality of S-boxes and P-boxes. Use diagrams to support your answer.

[2 marks]

(iv) Using an example explain how a simple substitution cipher can be broken via a letter frequency distribution analysis.

[2 marks]

PTO

Q.2.

(i) HomeAuto® is a start-up company for home automation / IoT products. Their flagship home area network product is based on a Wi-Fi access point that communicates with and manages a variety of wireless sensors and actuators, e.g. thermostats and motion detectors. In order to avoid 3rd party products to be used, and to provide secure end-to-end communication, the company decides to install digital certificates on every device. Explain, how such a solution would work. In your answer, make reference to:

- X.509 certificates and a suitable certificate structure for the company's devices
- The purpose of the CA and a suitable CA hierarchy
- How certificate revocation could be implemented
- How certificate extensions could be used
- How the device validation and key generation for secure device-to-access point communication would work.

[8 marks]

(ii) Distinguish between the following **GDPR principles**

- Lawfulness, fairness and transparency
- Data minimisation
- Storage limitation
- Integrity and confidentiality (security)

Use examples to support your answer.

[2 marks]

(iii) Design a stream cipher that is based on two combined 12-bit LFSRs of your choice. Using an example show how the algorithm works and how a serial bitstream can be encoded and decoded.

[5 marks]

(iv) Using a diagram show how a private key block cipher (like DES) can be used to calculate a message authentication code (MAC) over a given input.

[2 marks]

PTO

Q.3.

(i) Outline the various steps involved to provide end-point authentication in a computer network using

- Private key encryption
- Public key encryption
- Zero-knowledge protocols

thereby outlining advantages and disadvantages of each approach.

[8 marks]

(ii) Modern block ciphers support various modes of operation, including:
- Electronic codebook (ECB) mode
- Cipher block chaining (CBC) mode

Distinguish between these two modes and summarise their advantages and disadvantages.

[2 marks]

(iii) Hash chains and rainbow tables are used to recover hashed passwords. Outline similarities and differences between both concepts and give a comprehensive example of how a hashed password can be recovered by a rainbow table.

[5 marks]

(iv) Using an example show how a Rotor Cipher consisting of 3 rotors works.

[2 marks]

PTO

Q.4.

(i) Consider you are asked to provide a security protocol for a wireless sensor network based on WEP (for encryption / authentication) and Diffie-Hellman (for peer-to-peer key negotiation). Using diagrams and examples to support your answer outline how such a system would work, thereby highlighting limitations and weaknesses.

[8 marks]

(ii) Explain in some detail the purpose, structure and inner workings of a Feistel cipher and a Feistel network.

[3 marks]

(iii) Discuss the three security properties that are associated with cryptographic hash functions. Use examples to explain why they are needed.

[4 marks]

(iv) Outline four methods that can be used to render rainbow tables useless for password recovery.

[2 marks]

OLLSCOIL NA GAILLIMHE
UNIVERSITY OF GALWAY

Semester 2 Examinations 2022/2023

Course Instance Code(s)	4BCT, 1MECE, 1OA, 1EM
Exam(s)	B.Sc. (Computer Science & Information Technology), M.E. (Electronic and Computer Engineering)
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	1
External Examiner(s)	Dr. Ramona Trestian
Internal Examiner(s)	Prof. Michael Madden *Dr. Michael Schukat

Instructions: **Answer Question 1 and 2 other questions.**

Duration	**2 hours**
No. of Pages	**4**
Discipline(s)	Computer Science
Course Co-ordinator(s)	Dr. Colm O’Riordan

Requirements:

Release in Exam Venue	Yes [X]	No [ ]
MCQ Answersheet	Yes [ ]	No [X]
Handout	None	
Statistical/ Log Tables	None	
Cambridge Tables	None	
Graph Paper	None	
Log Graph Paper	None	
Other Materials	None	
Graphic material in colour	Yes [ ] No [X]	

Question 1 (Compulsory)

Assume you are a member of the FarmEye project team that develops an all-weather IP-enabled (IoT) CCTV camera system to monitor farm buildings and farm yards. The product is aimed to tackle the growing problem of farm theft and farm trespassing. The target market are both farmers and security services.
The camera provides a 24/7 life stream, with an uncompressed RGB still image being sent every second. Data communication is provided via a proprietary radio link to a nearby Internet-enabled base station, so an end-to-end encryption of the captured images between camera and base station is required. However, the computational resources on the camera are limited, therefore none of the standard L2/L3/L4 security protocols can be adopted. Instead you are asked to provide a secure data communication protocol that streams data from a single camera to the base station.

a) Identify concrete possible active and passive attacks by a threat actor on the radio data communication link. Based on these, outline the requirements for a secure communication protocol.

[4 marks]

b) Based on your findings in a) devise a simple protocol message format that allows the streaming of data from the camera to the base station. Justify your design.

[3 marks]

c) Version 1 of the communication protocol uses a private key block cipher, with the key shared between the camera and the base station. Show how a simple algorithm can be implemented via a Feistel cipher.

[5 marks]

d) Determine if your image encryption should be done in EBC mode or in CBC mode. Distinguish between both modes of operation, and justify your decision.

[3 marks]

e) Version 2 of the protocol uses a stream cipher instead of a block cipher. Using an example explain how such a stream cipher based on an LFSR could be implemented, and show how the encoding and decoding process works.

[5 marks]

f) Determine how your protocol would benefit from an additional hash function complementary to either version 1 or version 2, and subsequently update your design. Outline how this extension increases the robustness of your protocol.

[4 marks]

g) In order to simplify key management it is suggested to integrate the Diffie-Hellman key exchange protocol. Using an example, show how a key exchange between the camera and the base station could be accomplished. Further on, comment on the security / robustness of this extension and, using an example, show how a threat actor could compromise the key exchange.

[6 marks]

PTO

Question 2

a) The FarmEye product in Question 1 became a commercial success and will be complemented by other wireless sensors and actuators, e.g. motion detectors, that communicate with the base station. In order to avoid 3rd party products to be integrated, and to streamline key management, the project manager decides to have digital certificates installed on every device. Explain, how such a solution would work.

In your answer, make reference to:

a. X.509 certificates and a suitable certificate structure for FarmEye's devices
b. The purpose of the CA and a suitable CA hierarchy
c. How certificate revocation could be implemented
d. How certificate extensions could be used
e. How the device validation and key generation for secure device-to-access point communication would work.

[8 marks]

b) FarmEye customers would like to have camera timestamps attached to the transmitted images. In order to avoid rolling out a new communication protocol that contains such timestamps, it is proposed to use steganographic techniques to add such data to the transmitted pictures. Outline in detail, how this can be done. You can assume that the timestamp itself follows the normal ASCII format, i.e. YYYY:MM:DD:HH:MM:SS".

[2 marks]

Question 3

a) What are timing attacks, and how can they be avoided? Support your answer by providing an example for a safe and an unsafe implementation of a function of your choice.

[5 marks]

b) You've been asked by the principal of your former secondary school to help her assessing Kerberos as a possible authentication solution for the school IT infrastructure (that includes both desktops/workstations and server resources). In your response, explain in some detail, how Kerberos works, and how it would allow authenticating users and controlling access to the schools' server resources. In your answer also comment on the security/robustness of Kerberos.

[5 marks]

PTO

Question 4

a) Using examples where appropriate, explain the following (TLS-related) terms:

- Forward secrecy
- OCSP Stapling
- Authenticated Encryption with Additional Data (AEAD)

[3 marks]

b) What is meant by port scanning? In your answer, use diagrams to explain 2 scans of your choice. Further on, show how systems can be hardened against such scans.

[4 marks]

c) Using an example explain how a simple substitution cipher can be broken via a letter frequency distribution analysis.

[3 marks]

OLLSCOIL NA GAILLIMHE
UNIVERSITY OF GALWAY

Semester 2 Examinations 2022/2023

Course Instance Code(s)	4BCT, 1MECE, 1OA, 1EM
Exam(s)	B.Sc. (Computer Science & Information Technology), M.E. (Electronic and Computer Engineering)
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	1
External Examiner(s)	Dr. Ramona Trestian
Internal Examiner(s)	Prof. Michael Madden *Dr. Michael Schukat

Instructions: **Answer Question 1 and 2 other questions.**

Duration	**2 hours**
No. of Pages	**4**
Discipline(s)	Computer Science
Course Co-ordinator(s)	Dr. Colm O'Riordan

Requirements:

Release in Exam Venue	Yes [X]	No [ ]
MCQ Answersheet	Yes [ ]	No [X]
Handout	None	
Statistical/ Log Tables	None	
Cambridge Tables	None	
Graph Paper	None	
Log Graph Paper	None	
Other Materials	None	
Graphic material in colour	Yes [ ] No [X]	

Question 1 (Compulsory)

Assume you are a member of the FarmEye project team that develops an all-weather IP-enabled (IoT) CCTV camera system to monitor farm buildings and farm yards. The product is aimed to tackle the growing problem of farm theft and farm trespassing. The target market are both farmers and security services.
The camera provides a 24/7 life stream, with an uncompressed RGB still image being sent every second. Data communication is provided via a proprietary radio link to a nearby Internet-enabled base station, so an end-to-end encryption of the captured images between camera and base station is required. However, the computational resources on the camera are limited, therefore none of the standard L2/L3/L4 security protocols can be adopted. Instead you are asked to provide a secure data communication protocol that streams data from a single camera to the base station.

a) Identify concrete possible active and passive attacks by a threat actor on the radio data communication link. Based on these, outline the requirements for a secure communication protocol.

[4 marks]

b) Based on your findings in a) devise a simple protocol message format that allows the streaming of data from the camera to the base station. Justify your design.

[3 marks]

c) Version 1 of the communication protocol uses a private key block cipher, with the key shared between the camera and the base station. Show how a simple algorithm can be implemented via a Feistel cipher.

[5 marks]

d) Determine if your image encryption should be done in EBC mode or in CBC mode. Distinguish between both modes of operation, and justify your decision.

[3 marks]

e) Version 2 of the protocol uses a stream cipher instead of a block cipher. Using an example explain how such a stream cipher based on an LFSR could be implemented, and show how the encoding and decoding process works.

[5 marks]

f) Determine how your protocol would benefit from an additional hash function complementary to either version 1 or version 2, and subsequently update your design. Outline how this extension increases the robustness of your protocol.

[4 marks]

g) In order to simplify key management it is suggested to integrate the Diffie-Hellman key exchange protocol. Using an example, show how a key exchange between the camera and the base station could be accomplished. Further on, comment on the security / robustness of this extension and, using an example, show how a threat actor could compromise the key exchange.

[6 marks]

PTO

Question 2

a) The FarmEye product in Question 1 became a commercial success and will be complemented by other wireless sensors and actuators, e.g. motion detectors, that communicate with the base station. In order to avoid 3rd party products to be integrated, and to streamline key management, the project manager decides to have digital certificates installed on every device. Explain, how such a solution would work.
In your answer, make reference to:

a. X.509 certificates and a suitable certificate structure for FarmEye's devices
b. The purpose of the CA and a suitable CA hierarchy
c. How certificate revocation could be implemented
d. How certificate extensions could be used
e. How the device validation and key generation for secure device-to-access point communication would work.

[8 marks]

b) FarmEye customers would like to have camera timestamps attached to the transmitted images. In order to avoid rolling out a new communication protocol that contains such timestamps, it is proposed to use steganographic techniques to add such data to the transmitted pictures. Outline in detail, how this can be done. You can assume that the timestamp itself follows the normal ASCII format, i.e. YYYY:MM:DD:HH:MM:SS".

[2 marks]

Question 3

a) What are timing attacks, and how can they be avoided? Support your answer by providing an example for a safe and an unsafe implementation of a function of your choice.

[5 marks]

b) You've been asked by the principal of your former secondary school to help her assessing Kerberos as a possible authentication solution for the school IT infrastructure (that includes both desktops/workstations and server resources). In your response, explain in some detail, how Kerberos works, and how it would allow authenticating users and controlling access to the schools' server resources. In your answer also comment on the security/robustness of Kerberos.

[5 marks]

PTO

Question 4

a) Using examples where appropriate, explain the following (TLS-related) terms:

- Forward secrecy
- OCSP Stapling
- Authenticated Encryption with Additional Data (AEAD)

[3 marks]

b) What is meant by port scanning? In your answer, use diagrams to explain 2 scans of your choice. Further on, show how systems can be hardened against such scans.

[4 marks]

c) Using an example explain how a simple substitution cipher can be broken via a letter frequency distribution analysis.

[3 marks]

OLLSCOIL NA GAILLIMHE
UNIVERSITY OF GALWAY

Semester 2 Examinations 2023/2024

Course Instance Code(s)	4BCT, 1MECE, 1OA, 1EM
Exam(s)	B.Sc. (Computer Science & Information Technology), M.E. (Electronic and Computer Engineering)
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	1
External Examiner(s)	Dr. Ramona Trestian
Internal Examiner(s)	Prof. Michael Madden *Dr. Michael Schukat

Instructions: **Answer any four questions.**
All questions carry equal marks.

Duration	**2 hours**
No. of Pages	**4**
Discipline(s)	Computer Science
Course Co-ordinator(s)	Dr. Effirul Ramlan

Requirements:

Release in Exam Venue	No[ ]	Yes [☑]
MCQ Answer sheet	No [☑]	Yes [ ]
Handout	No [☑]	Yes [ ]
Formulae & Tables*	No [☑]	Yes [ ]
Cambridge Tables 2nd Edition**	No [☑]	Yes [ ]
Graph Paper*** A4 Graph Paper 1mm 0.1cm Squared (Standard)	No [☑]	Yes [ ]
Other Materials	No [☑]	Yes [ ]
Graphic material in colour	No [☑]	Yes [ ]

End of requirements.

Question 1 (15 Marks)

a) Assume you operate a distributed network of sensors to monitor the water quality of lakes and rivers in Co. Galway. The battery-operated sensors are resource-constrained (also in terms of their memory footprint / CPU performance), and use wireless networks (e.g., Wi-Fi, 4G) to transmit sensor readings to a datacentre in Oranmore.
Considering all the above constraints, determine the most efficient solution to provide for data integrity of the **transmitted sensor readings using a hash function, in order to prevent data manipulation** by a MitM. Use a diagram to support your answer.

[10 marks]

b) Distinguish between the terms **true random number generator**, **pseudo-random number generator**, and **pseudo-random function**. Provide diagrams to support your answer.

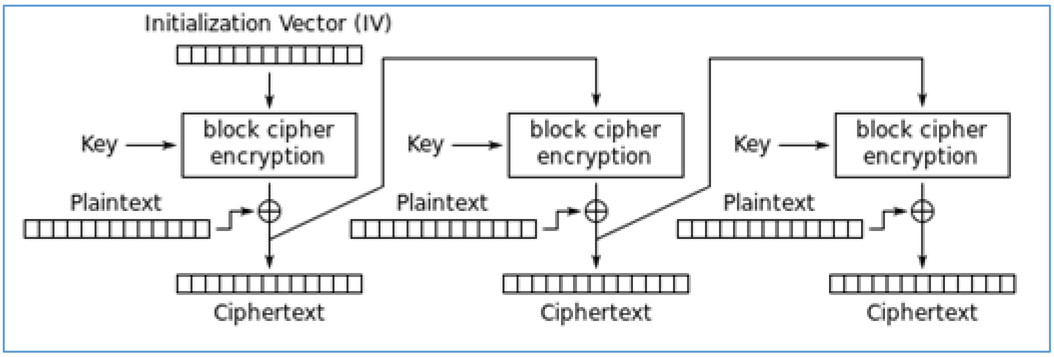
[5 marks]

Question 2 (15 Marks)

a) In the context of block ciphers, what is meant by the term **mode of operation**? Identify the mode of operation shown in the diagrams below and draw a diagram that shows the corresponding data decryption process.
Further on, determine if this mode supports:

- Parallelisable encryption
- Parallelisable decryption
- Random read access of individual blocks for decryption.

[9 marks]



b) Operating system kernels and network protocol stacks may be vulnerable to buffer overflow attacks if they are implemented in the "C" programming language. Using examples show how such attacks can happen and suggest to what extent they can be detected and avoided.

[6 marks]

PTO

Question 3 (15 Marks)

a) Digital certificates are normally used to bind a public key to an identity. However, this technology could also be used to implement a digital vaccination travel certificate. Such a certificate would be issued by a healthcare provider to vaccinated travellers and stored on their mobile phones. A 3rd party (e.g., border control) would subsequently read and validate the certificate to determine if and when its owner completed which vaccination (e.g., hepatitis A, tetanus or typhoid).

Further elaborate on this idea, thereby outlining

- a suitable internal certificate structure (that may contain features of attribute extension fields or attribute certificates),
- an architecture and method to issue, validate, and to revoke such a certificate.

Fully explain your design, using diagrams where appropriate.

[9 marks]

b) Using diagrams where appropriate, distinguish between the following IPSec-related terms / concepts:

a. Tunnel mode versus transport mode
b. Anti-replay window
c. Combining security associations

[6 marks]

Question 4 (15 Marks)

a) Distinguish between the terms **timing attack** and **unsafe function**.
Explain why the function below is unsafe and suggest code improvements.

```
bool isNumberInArray(int number, int *array, int arrayLength) {
   int i;
   for (i = 0; i < arrayLength; i++)
               if (number == array[i])
                     return true;
   return false;
```

[6 marks]

b) Using diagrams show how data encryption / decryption is achieved with Double-DES and Triple-DES. Evaluate, to what extent both algorithms are vulnerable to a **meet-in-the-middle attack**.

[9 marks]

PTO

Question 5 (15 Marks)

a) Explain the following (TLS-related) terms, using diagrams where appropriate:

- OCSP Stapling
- Version rollback attack
- Certificate path validation
- The key share Extension
- Mutual authentication

[5 marks]

b) Using examples, explain the concept and the inner workings of a **Feistel cipher**, a **SP network**, and its components (i.e., **S-boxes** and **P-boxes**).
Further on explain, how a Feistel cipher can be combined with a SP network, and from there further expanded to a Feistel network, in order to build a block cipher.

[10 marks]

Question 6 (15 Marks)

a) Using diagrams to support your answer, distinguish between and explain the inner workings of:

- a LFSR
- a combined LFSR
- a NLFSR

[6 marks]

b) Discuss in some detail, if and how **message authentication** (potentially in combination with a message sequence number) can prevent the following attacks on data communication:

- (Sender) Masquerade
- Denial-of-Service
- Content modification
- Sequence modification
- Timing modification

[9 marks]

END OF EXAM