NUI Galway
OÉ Gaillimh

Summer Examinations 2017-18

Exam Code(s)	3BME1, 4BME1, 1EM1, 1OA1, 1OA9, 4BCT1, 4BMS2, 3BS9, 4BS2
Exam	Third Year & Fourth Year & HDip
Module	CRYPTOGRAPHY
Module Codes	CS402 & MA492 & MA545
External Examiner(s)	Prof T. Brady
Internal Examiner(s)	Prof G. Ellis*
Instructions	Attempt **all** questions. There are ten questions, each carrying 10 marks.
Duration	2 hours
No. of Pages	3 pages (including this cover page)
Discipline	Mathematics

Requirements:

Release in Exam Venue	Yes ☑	No ☐
Release to Library	Yes ☑	No ☐
Non-programmable calculator	Yes ☑	No ☐
Mathematical Tables	Yes ☐	No ☑

1. The ciphertext ... Determine ...

2. The ciphertext ... Determine ...

3. Describe:

(a)
(b)
(c)

4.

5.

6. Answer **either** part (a) **or** part (b).

(a)
(b)

7. Answer **either** part (a) **or** part (b).

(a)

(b) Carefully describe the A5/1 stream cipher which is used to encrypt the on-air traffic in the GSM mobile phone networks in Europe and the US.

8. Answer **either** part (a) **or** part (b).

(a)

(b)

9. Answer **either** part (a) **or** part (b).

(a)

(b)

10. Answer **either** part (a) **or** part (b).

(a)

(b)