### Module Code
- **CS7NS5**

### Module Name
- **Security and Privacy**

### ECTS weighting
- **5**

### Term
- **HT**

### Contact Hours
- **2 lecture hours per week**

### Module Personnel
- **Dr. Stephen Farrell**

### Learning Outcomes
On successful completion of this module a student will be able to:

- **NS5LO1** discuss information security and demonstrate an understanding of the context in which information security operates in terms of safety, environmental, social and economic aspects;
- **NS5LO2** analyse, assess and choose among techniques for mitigating important privacy threats through appropriate security controls, namely the application of cryptographic primitives;
- **NS5LO3** assess both the risks and threats associated with data security, and assess how the relevant legislative and regulatory frameworks apply;
- **NS5LO4** reason about issues of privacy with respect to data release.

### Module Learning Aims
The objectives of this module are: to develop an in-depth understanding of data privacy, threats and risks of security breaches, an awareness of computer security (cryptography) techniques, and an ability to make appropriate decisions about securing data.

### Module Content
Specific topics addressed in this module include:

- **Cryptography**
  - Symmetric Key Crypto - DES and AES
  - Asymmetric Key Crypto - RSA, DLP, ECC
- **Privacy**
  - Privacy Laws Around the World
  - US and EU Data Protection Laws
  - Machine readable terms and conditions
  - User control over privacy settings
- **Internet Security**
  - Digital Signatures
  - X.509 Certificates and Public Key Infrastructure
  - Secure Sockets Layer (SSL)
- **Authentication**
  - Two-Factor Authentication
  - Biometrics
- **Digital Rights Management (DRM)**
  - Licensing and Enforcement
  - Watermarking
- **Cloud Security**
  - Multi-tenancy Issues
  - Virtualisation System Security Issues, Vulnerabilities and Attacks
  - Legal and Compliance Issues
  - Auditing
- **Social Networks and Privacy**
- **Machine Security**
  - Malware, SQL Injection and Cross-Side Scripting Attacks
  - Buffer Overflows
  - Botnets
- **Electronic Payment Systems**
  - Macro and Micropayments
| Assessment Details | Coursework 20%  
|                   | Examination 80%  
|                   | o E-Cash, Credit and Debit Cards  
|                   | o Bitcoin and Blockchains  