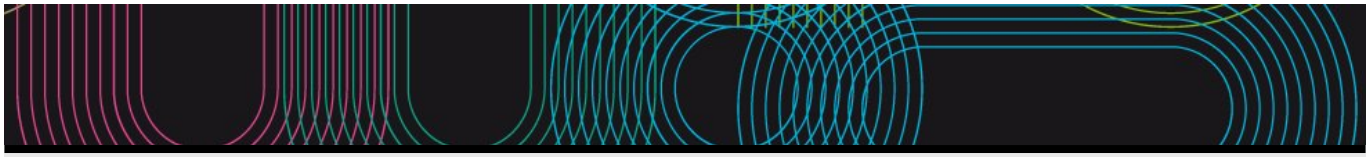

IDENTIFYING DATA				
Network Security				
Subject	Network Security			
Code	V05G301V01305			
Study programme	Grado en Ingeniería de Tecnologías de Telecomunicación			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	6	Optional	3rd	1st
Teaching language	Spanish			
Department				
Coordinator	Fernández Masaguer, Francisco Rodríguez Rubio, Raúl Fernando			
Lecturers	Fernández Masaguer, Francisco Rodríguez Rubio, Raúl Fernando			
E-mail	francisco.fernandez@det.uvigo.es rrubio@det.uvigo.es			
Web	http://faitic.uvigo.es			
General description	In this course are studied , in an unified way, the main problems and threats to security in networks and telematic services, and distinct techniques to protect them are presented. First the subject is considered from a general point of view, so that the concepts, services and security techniques studied, can be applied to any type of network, telematic service or information system to secure. This block is formed by chapters 1 to 4. This carries to treat with detail the three central subjects of security: the algorithmic part (encipherment, digital signature and integrity), the authentication problem and the procedures of key management. The aim is to give the student the knowledge and practice to entitle him/her to ease his understanding of the particular techniques that each application can require and to apply them to other scenarios that he(she) have to face. Afterwards the subject is considered in a more particular way, reviewing the problems, techniques and standards of security in some of the communication environments of greater prevalence in actuality. Thus a chapter is devoted to the security to the IP level, central protocol in the Internet architecture, and another chapter to the security in the Web, given the current importance of this way of telematic intercommunitation. Here the student will familiarize with the theoretical and practical aspects of the SSL protocol, central for the security of Web transactions. Given also the every time greater utilisation of wireless communications and his particular security problems, one chapter is devoted to the subject. The course is closed with an introduccion to other two subjects of increasing transcendence: botnets, malicious networks and software, and the forensic analysis of information systems.			

Training and Learning Results	
Code	
B3	CG3: The knowledge of basic subjects and technologies that enables the student to learn new methods and technologies, as well as to give him great versatility to confront and adapt to new situations
B4	CG4: The ability to solve problems with initiative, to make creative decisions and to communicate and transmit knowledge and skills, understanding the ethical and professional responsibility of the Technical Telecommunication Engineer activity.
B6	CG6: The aptitude to manage mandatory specifications, procedures and laws.
C28	CE28/TEL2 The ability to apply the techniques that are basis of computer networks, services and applications, such as management, signaling and switching, routing and securing systems (cryptographic protocols, tunneling, firewalls, charging mechanisms, authentication and content protection) traffic engineering (graph theory, queuing theory and teletraffic) rating, reliability and quality of service in both fixed, mobile, personal, local or long distance environments with different bandwidths, including telephony and data.
D2	CT2 Understanding Engineering within a framework of sustainable development.

D3 CT3 Awareness of the need for long-life training and continuous quality improvement, showing a flexible, open and ethical attitude toward different opinions and situations, particularly on non-discrimination based on sex, race or religion, as well as respect for fundamental rights, accessibility, etc.

Expected results from this subject

Expected results from this subject	Training and Learning Results		
Understand the foundations of the cryptographic science	B3		
To acquire the necessary knowledges to ensure the security of a computer or telematic system.	B3		
To acquire skills on the process of analysis of the attacks that can suffer a network and the main mechanisms of defence against them.	B4	C28	D3
Know the main architectures of applicable security to the computer and telematic systems.	B4	C28	D3
Know the main ideas of the norms and standard more important in matter of security in computer systems and communication networks.	B6	C28	D2

Contents

Topic	
1 Mathematics foundations of security.	- Basic notions of Complexity Theory. - Basic notions of Number Theory.
2. Cypher, digital signature and hash algorithms	- Types of criptosistems and algorithms. - Integrity and hash algorithms. - Symetric key cryptosistems. Mac functions. Encrytion. Shannon principles. Stream and block cyphers. DES and AES algorithms Cypher modes of operation. - Public key cryptosystems. RSA, DSA and elliptic curves. - Influence of quantum computing on cryptography.
3. Certification and Public Key Infrastructures.	- Security problems of asimetric cryptography. Certification and certificate formats. - Trust models. Flat trust model and PGP. Third partiy trust model and certification authorities. - Certificate Infrastructures. Certification path. - Certificate revocation.
4. Authentication and key agreement protocols.	- Authentication methods. - Threats to an authentication protocol. Countermeasures. - Requirements of a key agreement protocol. Diffie-Hellman protocol. - Authentication in simmetric cryptosistems. Cases of study: GSM and Kerberos. - Authentication in asimetric cryptosistems. Cases of study: X509 and SSL. - Passwords based protocols: SRP. - Single Sign On (SSO)
5. Security at the network layer	- Threats in the network layer. - IP Security Architecture. - IPsec Protocol. IPsec tunnels. IPsec and NAT. - Key manegement protocols: IKE, ISAKMP and OAKLEY.
6. Security in the Web and electronic commerce.	- Problems of security in the Web. - Protocols: SSL and TLS. - Certification in the Web.
7. Wireless security and AAA protocols.	- Threats to security in wireless environments. - Wireless Application Protocol (WAP). WTLS. Protocols WEP, WPA, WPA2 (802.11i). - AAA Protocols: RADIUS.
8. Systems Security.	- Firewalls and systems against intrusions. - Malicious software and networks. - Forensic analysis of systems.

Planning

	Class hours	Hours outside the classroom	Total hours
Lecturing	21	38	59
Autonomous problem solving	0	10	10
Mentored work	6	28	34
Laboratory practical	11	22	33
Laboratory practice	1	0	1
Essay	1	0	1
Essay questions exam	1	5	6
Essay questions exam	1	5	6

*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.

Methodologies	
	Description
Lecturing	Exhibition by means of powerpoint presentations and blackboard of the theoric contents of the course. They will develop the theoretical subjects of the matter that do not remain covered by the others methodologies employed. In those subjects considered indispensable, will pose and will resolve some exercises that serve of help for the realisation of other similar by the student of autonomous form. With this methodology, student will adquire part of CG3 y CE28 competences.
Autonomous problem solving	The student will solve in an autonomous form the exercises, cuestions or problems of the bulletin not solved in the face-to-face hours. The doubts arisen will be agreed and will be exposed to the tutor in normal tutor time. This methodology is aimed to CG4 and CE28 competences.
Mentored work	Work in group. Several theoretical and practical works to develop will be explained to the students, between which each group will have to choose one. In the C class type, will expose to each group the aims of the work, hardware and software tools to use, form to tackle it and will realise a follow-up to each group. This methodology, is aimed to adquire part of CG4,CG6, CE28, CT2 and CT3 competences.
Laboratory practical	Work in group. The group will developed some practices in the laboratory, focused to mature and carry to practice the theoretical concepts , as to improve his ability for the engineering of secure networks and services. This methodology, is aimed to CG6, CE28, CT2 and CT3 competences.

Personalized assistance	
Methodologies	**Description**
Laboratory practical	Individualized monitoring of each group work. Comments of diverse options, recommendations and strategies for the good development of the project. Reviews with each group the level of understanding and advance of the project, particular doubts that can arise, design and Java coding errors. Help for the understanding of the JCA/JCE and JSSE packages. Individualized help for instalation of the keystore management tool and of the basic Java code of the practice.
Mentored work	Individualized monitoring of each student in the group. General comments to the group of recommendations and strategies for the good development of the project. Reviews with each group of the level of understandings and advance of the project, particular doubts that can arise, design or approach errors and options of improvement.
Autonomous problem solving	Reviews and comments of the diverse exercises proposed. The student will have in Faitic with the solucion to some of the proposed exercises.

Assessment					
	Description	Qualification	Training and Learning Results		
Laboratory practice	Proof of group in which the teacher will value laboratory practises, reviewing his operation with the members of the group. This proof will be made in the last or previous to last week of the four-month period as it will be published in Moovi platform in the firsts weeks of the four-month period. All the members of the group have to be present at the moment of the presentation. The teacher will do an authorship interview of which the level of participation of each student will be deduced and of which, together with the correct operation, the individual mark of each student will be determined.	25	B6	C28	D3
Essay	Assessment of the tutored project or work realised by the group (type C). The group will do a demonstration to the teacher of the project or work done and results obtained. This proof will be made in the last or previous to last week of the four-month period as it will be published in Moovi platform in the firsts weeks of the four-month period. All the members of the group have to be presents in the moment of the presentation. The teacher will do an authorship interview of which the level of participation of each student in the proyect will be deduced and of which, together with the correct operation, the individual mark of each student will be determined.	25	B4 B6	C28	D2 D3

Essay questions exam	Final exam of the course. This exam will consist of a group of exercises/questions on the contents given in the course.	25	B3 B4	C28
Essay questions exam	Partial exam of the course, neccesary for students that follow continuos evaluation. This exam will consist of a group of exercises/questions on the contents given until aproximately the middle of the theoretic course.	25	B3 B4	C28

Other comments on the Evaluation

- **CHOICE OF CONTINUOUS EVALUATION.**

  By default it will be considered that the student opts by continuous assessment (CA). If a student wishes to opt by no continuous, he/she will must communicate it to the teacher before the week 5 of the academic course. The communication must be made by email.

- **ORDINARY CALL.**

  Continuous assessment (CA). This will be formed by:

  1. Laboratory work B, representing 25% of the total mark. The exact date of delivery of this work will be published in Moovi platform in the firsts weeks of the four-month period, after coordination with other matters.
  2. Project C, representing 25% of the total mark. The exact date of delivery of this work will be published in Moovi platform in the firsts weeks of the four-month period, after coordination with other matters.
  3. Partial exam of the contents given until about the quarter's middle, representing 25% of the mark. This exam will do average with the final exam if the student minimun mark is 3.5 points of 10. If the student mark is lower than this minimun he/she must do another exam of this part in the final exam. The date of this exam will be approved at the Comision Academica de Grado (CAG) and published at the beginning of the four-month period.
  4. Final exam, in the agreed date in Board of School. Two cases are posible:

     - Students with mark greather than minimum in the partial exam. This exam will consist of the subjects given from about the quarter's middle to the end. It will represent 25% of the total mark. To be able to surpass the course the student must obtain in this exam a minimum mark of 3,5 points of 10.
     - Students with mark lower than minimum in the partial exam. This exam will consist of all the subjects given in the course.It will represent 50% of the total mark. To be able to surpass the course the student must obtain in this exam a minimum mark of 3,5 points of 10, with a minimun of 3,5 points on each of the two parts of the exam.

  Global assessment (GA). The students that do not choose CA will do a final exam by 80% of the mark, together with B laboratory practise, that will provide the other 20%.

  The final exam will be the same for all the students, independently of if they opt by continuous or global assessment.

- **EXTRAORDINARY CALL**

  Students that do not choose CA in the first call will do a final exam by 80% of the final mark, together with the laboratory practices that will complete the other 20%. It is saved the mark of the laboratory of the ordinary call.
  The students that have opted in the first call by CA, can follow in the extraordinary call by CA or change to GA. The students that change to GA, MUST communicate it explicitly to the teacher by electronic mail not later than 7 days before the date of the extraordinary exam.

- In the first case, that is, for students who continue by CA in the extraordinary call, the total mark will consist, as in the ordinary call, by 50% for the theoric exam, 25% for the laboratory practices B and 25% for the project C. The mark of the partial and final exam (when the minimun mark is surpasses), is saved from the ordinary call. All students that have not surpassed the minimum mark in the theoric exam of the ordinary call MUST do the final exam in the extraordinary call, but only of the part (or parts) for which have not reached this minimum mark (3,5).
- In the second case, GA students in the extraordinary call will do a final exam by 80% of the note, and laboratory practices by 20%. The laboratory mark of the ordinary call will be maintained in this case, properly scaled/porcentuated.

The students that change from GA to CA, will maintain the laboratory mark.

- **ADDITIONAL NOTES.**
  - *Minimal cualification for theory evaluation (long answer tests and development)*. Independently of if continuous or global assesment, and independently of the call, it will be necessary to get a minimun of 3.5 over 10 for CA and 4 over 10 for GA, in the theoretical exam (long answer tests and development), for the approval of the course.
  - It will be considered to the student as "no presented" if he/she has not followed continous evaluation and has not presented to the final exam. Equally, if he/she follows CA (continuous evaluation) and has not attended anyone of the A, B and C parts, he/she will be considered as "no presented".
  - The qualifications obtained in the laboratory B and project C will be valid only during the academic course in that they were realised.
  - In the case that the total mark is equal or higher than 5, but the minimun in some part has not been reached, the final mark will be 4.9 points (failure).

- **END OF PROGRAM EXAM.**
  - Will be formed by:
    - Theoretical exam (50%). Personal exam about all theoric themes of the course, representing 50% of the total mark. The student will need a minimal mark of 3,5 of 10 for the approval of the course.
    - Laboratory work B, representing 25% of the mark.
    - Project C, representing 25% of the mark.

Sources of information

Basic Bibliography

F. Fernandez Masaguer, **Apuntes de Seguridad en Redes y Sistemas de Informacion**, 1ª ed., Revisión 2023

William Stallings, **Cryptography and Network Security. Principles and practice.**, 8ª ed., Pearson, 2020

Complementary Bibliography

R.Perlman, C. Kaufman, M.Speciner, **Network Security: Private communications on a public world**, 2ª ed., Prentice Hall, 2002

Joseph Migga Kizza, **Guide to Computer Network Security**, 2ª ed.,

Douglas R. Stinson, **Cryptography. Theory and Practice.**, 3ª ed.,

M. Laurent Maknavicius, **Wireless and Mobile Network Security**, 1ª, Wiley, 2009

Enisa, **Botnets: Detection; Measurement, Disinfection & Defence**, Enisa, 2011

Recommendations

Subjects that are recommended to be taken simultaneously

Architectures and Services/V05G301V01310
Internet Services/V05G301V01301

Subjects that it is recommended to have taken before

Programming II/V05G301V01110