**SYNTHESIZED SCHOOL PROGRAM**

|  |  |
| --- | --- |
| **ACADEMIC UNIT:** | Escuela Superior de Cómputo |

|  |  |  |  |
| --- | --- | --- | --- |
| **ACADEMIC PROGRAM:** | Ingeniería en Sistemas Computacionales. | | |
| **LEARNING UNIT:** | Cryptography | **LEVEL:** | III |

|  |
| --- |
| **AIM OF THE LEARNING UNIT:**  The student designs primitives and cryptographic applications using existant algorithms, techniques and existant tools.  **CONTENTS:**   1. Cryptography Fundamentals. 2. Symmetric Cryptography. 3. Public key Cryptography. 4. Digital Signatures.   **TEACHING PRINCIPLES:**  The teacher will apply a Projects-Based learning process, through inductive and heuristic methods using analysis techniques, technical data, charts, cooperative presentation, exercise-solving and the production of the learning evidences. Moreover, an autonomous learning will be encouraged by the development of a final project.  **EVALUATION ANDPASSING REQUERIMENTS:**  The program will evaluate the students in a continuous formative and summative way, which will lead into the completion of learning portfolio. Some other assessing methods will be used, such as revisions, lab practicals, class participation, exercises, learning evidences and a final project.  Other means to pass this Unit of Learning:   * Evaluation of acknowledges previously acquired, with base in the issues defined by the academy. * Official recognition by either another IPN Academic Unit of the IPN or by a national or international external academic institution besides IPN.   **REFERENCES:**   * Konheim, A. G. (2007). “*Computer Security and cryptography”.* United States of America: Ed. John Wiley & Sons. ISBN-13: 978-0471947837. * Paar, C. Pelzl ,J. Preneel B. (2009) “*Understanding Cryptography: A textbook for students and practitioners.”* United States of America: Ed. Springer Verlag. ISBN-13: 978-3642041006. * Stallings, W. (2010) “*Cryptography and network security.”* (5ª Ed.). United States of America: Ed. Prentice Hall. ISBN-13: 978-00136097044. * Stinson, D. R. (2005). “*Cryptography: theory and practice.”* (3ª Ed.). United States of America: Ed. Chapman&Hall/CRC. ISBN-13: 978-1584885085. * Trappe, W., Washington L. (2006) “*Introduction to Cryptography with Coding Theory.”* (2ª Ed.). United States of America: Ed. Prentice Hall. ISBN-13: 978-0130618146. |

|  |  |  |
| --- | --- | --- |
| **ACADEMIC UNIT:** Escuela Superior de Cómputo.  **ACADEMIC PROGRAM:** Ingeniería en Sistemas Computacionales  **LATERAL OUTPUT:** Analista Programador de Sistemas de Información.  **FORMATION AREA:** Professional.  **MODALITY:** Presence. |  | **LEARNING UNIT:** Cryptography  **TYPE OF LEARNING UNIT:** Theorical - Practical, Optative. **USE:** August, 2011  **LEVEL:** III.  **CREDITS:** 7.5 Tepic, 4.39 SATCA |

|  |
| --- |
| **EDUCATIVE AIM**  This learning unit enhances the profile of graduates in Computer Systems Engineering providing cryptographic techniques and tools that allows to protect information in a computer system. It also helps develop strategic and creative thinking, collaborative work and assertive communication.  Learning units required are Algorithm and Structured Programming, Data Structure, Object-Oriented Programming, Discrete Mathematics and Probability. The subsequent units are Work Safety and Terminal Work I and II.  **AIM OF THE LEARNING UNIT:**  The student designs primitives and cryptographic applications using existant algorithms, techniques and existant tools. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CREDITS HOURS**  **THEORETICAL CREDITS / WEEK:** 3.0  **PRACTICAL CREDITS / WEEK:** 1.5  **HOURS** **THEORETICAL /TERM:** 54  **HOURS** **PRACTICAL / SEMESTER:**  27  **HOURS AUTONOMOUS LEARNING:** 54  **CREDITS HOURS** **/ SEMESTER:** 81 |  | **LEARNING UNIT DESIGNED BY:** Academia de Sistemas Distribuidos.  **REVISED BY:**  **Dr. Flavio Arturo Sánchez Garfias. Subdirección Académica**  **APPROVED BY:**  **Ing. Apolinar Francisco Cruz Lázaro.**  **Presidente del CTCE** |  | **AUTHORIZED BY:** Comisión de Programas Académicos del Consejo General Consultivo del IPN  **Ing. Rodrigo de Jesús Serrano Domínguez**  **Secretario Técnico de la Comisión de Programas Académicos** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **LEARNING UNIT:** | Cryptography | **PAGE:** | 3 | **OUT OF** | 10 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **N° THEMATIC UNIT:** I **TITLE:** Cryptography Fundamentals | | | | | | |
| **UNIT OF COMPETENCE**  The student relates the characteristics of a cryptographic system based on its primitives and services. | | | | | | |
| **No.** | **CONTENTS** | **Teacher led-instruction HOURS** | | **Autonomous Learning**  **HOURS** | | **REFERENCES KEY** |
| **T** | **P** | **T** | **P** |
| 1.1  1.2  1.3  1.4  1.4.1  1.4.2  1.4.3  1.4.4 | Definition and importance of cryptography  Cryptographic services.  Cryptographic system characteristics  Attacks  Ciphertext only  Known plaintext  Chosen plaintext  Chosen ciphertext | 1.0  1.0  0.5  2.0 | 0.5 | 0.5  0.5  1.0  1.0 | 1.0 | 2B, 3B, 4B, 5B, 1C |
|  | Subtotals: | 4.5 | 0.5 | 3.0 | 1.0 |  |
| **TEACHING PRINCIPLES**  This Thematic Unit will be Projects-Based learning strategy, trough heuristic method, with the techniques of elaboration of charts, documentary research, brainstorming, technical data and exercise-solving, lab practical and production of learning evidence and the accomplishment of a project proposal. | | | | | | |
| **LEARNING EVALUATION**  Assessment  Portfolio of Evidences:  Charts 5%  Technical data 5%  Exercise-solving 25%  Proposal of project 20%  Rubric of Self-Evaluation 2%  Rubric of Co-Evaluation 3%  Learning Evidence 40% | | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **LEARNING UNIT:** | Cryptography | **PAGE:** | 4 | **OUT OF** | 10 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **N° THEMATIC UNIT:** II **NAME:** Symmetric Cryptography | | | | | | |
| **UNIT OF COMPETENCE**  The student develops symmetric cryptographic protocols based on private key ciphers. | | | | | | |
| **No.** | **CONTENTS** | **Teacher led-instruction HOURS** | | **Autonomous Learning**  **HOURS** | | **REFERENCES KEY** |
| **T** | **P** | **T** | **P** |
| 2.1  2.2  2.3  2.4  2.4.1  2.4.2  2.4.3  2.5 | Symmetric cryptography characteristics  Perfect secrecy  Classical cryptosystems  Modern cryptography algorithms  Stream ciphers  Block ciphers  Security  Modes of operation | 0.5  1.0  1.0  3.0  0.5 | 1.0  1.0  0.5 | 0.5  2.0  2.0  6.0  1.0 | 2.0  2.0  1.0 | 2B,3B,4B,5B,1C |
|  | Subtotals: | 6.0 | 2.5 | 11.5 | 5.0 |  |
| **TEACHING PRINCIPLES**  Will be projects-Based learning strategy, trough heuristic method, with the techniques of charts, exercise-solving, cooperative presentation, advance of the project, lab practical and the production of the learning evidences. | | | | | | |
| **LEARNING EVALUATION**  Portfolio of Evidences:  Charts 5%  Comparison table 5%  Exercise-solving 5%  Lab practical reports 20%  Advance of the project 20%  Rubric of self-evaluation 2%  Rubric of co-evaluation 3%  Evidence of learning 40% | | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **LEARNING UNIT:** | Cryptography | **PAGE:** | 5 | **OUT OF** | 10 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **THEMATIC UNIT:** III **TITLE:** Public key Cryptography | | | | | | |
| **UNIT OF COMPETENCE**  The student implements public key cryptography protocols, using modular arithmetic. | | | | | | |
| **No.** | **CONTENTS** | **Teacher led-instruction HOURS** | | **Autonomous Learning**  **HOURS** | | **REFERENCES KEY** |
| **T** | **P** | **T** | **P** |
| 3.1  3.2  3.3  3.3.1  3.3.2  3.3.3  3.3.4  3.4  3.4.2  3.4.3 | Public key cryptography characteristics.  Integers modulo n.  Number theory  Extended Euclidean algorithm  Fermat’s theorem  Chinese remainder theorem  Intractable problems in number theory  Public key algorithms  Key exchange  Encryption algorithms | 0.5  1.0  2.5  1.0 | 2.0  1.0 | 0.5  2.5  6.0  3.5 | 4.0  3.5 | 3B,4B,5B,1C |
|  | Subtotals: | 5.0 | 3.0 | 12.5 | 7.5 |  |
| **TEACHING PRINCIPLES**  Will be projects-Based learning strategy, through inductive and heuristic methods, with the techniques of elaboration of exercise-solving, cooperative presentation, practical and learning evidence, the production of the learning evidences and advance of the project. | | | | | | |
| **LEARNING EVALUATION**  Project portfolio:  Charts 5%  Exercise-solving 5%  Technical data 5%  Lab practical reports 20%  Advance of the Project 20%  Self-Evaluation rubrics 2%  Cooperative Evaluation rubrics 3%  Written learning Evidence 40% | | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **LEARNING UNIT:** | Cryptography | **PAGE:** | 6 | **OUT OF** | 10 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **THEMATIC UNIT:** IV **TITLE:** Digital signatures | | | | | | |
| **UNIT OF COMPETENCE**  The student solves authentication problems in a computer system using digital signatures. | | | | | | |
| **No.** | **CONTENTS** | **Teacher led-instruction HOURS** | | **Autonomous Learning**  **HOURS** | | **REFERENCES KEY** |
| **T** | **P** | **T** | **P** |
| 4.1  4.1.1  4.1.2  4.2  4.3  4.3.1  4.3.2  4.3.3 | Hash functions  Birthday attack  Collisions  Message authentication codes: MAC  Digital signatures.  RSA signature scheme  ElGamal signature scheme  Digital Signature Algorithm (DSA) | 1.0  1.0  1.5 | 1.0  0.5  0.5 | 3.0  2.0  3.0 | 2.0  1.0  2.5 | 3B,4B,5B,  1C |
|  | Subtotals: | 3.5 | 2.0 | 8.0 | 5.5 |  |
| **TEACHING PRINCIPLES**  Will be projects-Based learning strategy, trough inductive and heuristic methods, with the techniques of cooperative presentation, practical, the production of the learning evidences and the presentation of the final project. | | | | | | |
| **LEARNING EVALUATION**  Project Portfolio:  Charts 5%  Report of project 40%  Lab practical reports 20%  Self-Evaluation rubrics 2%  Cooperative Evaluation rubrics 3%  Written learning Evidence 30% | | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **LEARNING UNIT:** | Cryptography | **PAGE:** | 7 | **OUT OF** | 10 |

**RECORD OF PRACTICALS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **NAME OF THE PRACTICAL** | **THEMATIC UNITS** | **DURATION** | **ACCOMPLISHMENT LOCATION** |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14 | Vigenère cipher.  Cryptanalysis of Vigenère cipher.  Hill cipher and its cryptanalysis  Block cipher algorithm  Block ciphers and modes of operation CBC and CTR.  Extended Euclidena algorithm.  Prime factorization.  Discrete logarithm in Zp.  Diffie-Hellman scheme.  Primality test.  Public key encrytion.  Standard hash functions.  MAC.  Digital Signature Algorithm DSA. | I  II  II  II  II  III  III  III  III  III  III  IV  IV  IV | 1.5  1.5  1.5  3.0  1.5  1.5  1.5  1.5  1.5  1.5  3.0  3.0  1.5  3.0 | Computer Labs. |
| **TOTAL OF HOURS** | 27.0 |

|  |
| --- |
| **EVALUATION AND PASSING REQUIREMENTS:**  The lab practicals are considered mandatory to pass this learnig unit.  The lab practicals worth 20% in the thematic units II, III and IV. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **LEARNING UNIT:** | Cryptography | **PAGE:** | 8 | **OUT OF** | 10 |

|  |  |  |
| --- | --- | --- |
| **PERIOD** | **UNIT** | **EVALUATION TERMS** |
| 1  2  3 | I y II  III  IV | Continuous evaluation 60% and written learning evidence 40%  Continuous evaluation 60% and written learning evidence 40%  Continuous evaluation 70% and written learning evidence 30%  The learning unit I worth 15% of final score  The learning unit I worth 18% of final score  The learning unit I worth 33% of final score  The learning unit I worth 34% of final score  Other means to pass this Learning Unit:   * Evaluation of acknowledges previously acquired, with base in the issues defined by the academy. * Official recognition by either another IPN Academic Unit of the IPN or by a national or international external academic institution besides IPN.   If accredited by Special Assessment or a certificate of proficiency, it will be based on guidelines established by the academy on a previous meeting for this purpose. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **LEARNING UNIT:** | Cryptography. | **PAGE:** | 9 | **OUT OF** | 10 |

|  |  |  |  |
| --- | --- | --- | --- |
| **KEY** | **B** | **C** | **REFERENCES** |
| 1  2  3  4  5 | X  X  X  X | X | Konheim, A. G. (2007). *Computer Security and cryptography.* United States of America: Ed. John Wiley & Sons. ISBN-13: 978-0471947837.  Paar, C. Pelzl, J. Preneel B. (2009). *Understanding Cryptography: A textbook for students and practitioners.* United States of America: Ed. Springer Verlag. ISBN-13: 978-3642041006.  Stallings, W. (2010). *Cryptography and network security* (5ª Ed.). United States of America: Ed. Prentice Hall.  ISBN-13: 97800136097044.  Stinson, D. R. (2005). *Cryptography: theory and practice* (3ª Ed.). United States of America: Ed. Chapman&Hall/CRC.  ISBN-13: 978-1584885085.  Trappe, W. Washington, L. (2006). *Introduction to Cryptography with Coding Theory* (2ª Ed.). United States of America: Ed. Prentice Hall. ISBN-13: 978-0130618146. |

**TEACHER EDUCATIONAL PROFILE PER LEARNING UNIT**

1. **GENERAL INFORMATION**

|  |  |
| --- | --- |
| **ACADEMIC UNIT:** | Escuela Superior de Cómputo. |

|  |  |  |  |
| --- | --- | --- | --- |
| **ACADEMIC PROGRAM:** | Ingeniería en Sistemas Computacionales. | **LEVEL** | III |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **FORMATION AREA:** | **Institutional** | **Basic Scientific** | **Professional** | **Terminal and Integration** |

|  |  |  |  |
| --- | --- | --- | --- |
| **ACADEMY:** | Sistemas Distribuidos. | **LEARNING UNIT:** | Cryptography. |

|  |  |
| --- | --- |
| **SPECIALTY AND ACADEMIC REQUIRED LEVEL:** | Masters Degree or Doctor in Computer Science. |

1. **AIM OF THE LEARNING UNIT:**

The student designs primitives and cryptographic applications using existant algorithms, techniques and existant tools.

1. **PROFESSOR EDUCATIONAL PROFILE:**

|  |  |  |  |
| --- | --- | --- | --- |
| **KNOWLEDGE** | **PROFESSIONAL EXPERIENCE** | **ABILITIES** | **APTITUDES** |
| * Cryptographic algorithms * Algebra. * Computer Security protocols. * Algorithmic complexity. * Programming languages * Knowledge of the Institutional Educational Model. * English. | * A year cryptograpy * Actual in educational as facilitator of the knowledge of two years. * A year experience in the Institutional Educational Model. | * Facility with * Problems resolution. * Cooperative. * Leadership. * Applications of Institutional Educational Model. * Decision making. | * Responsible. * Patient * Tolerant. * Respectful. * Collaborative. * Participative. * Interested to learning. * Assertive. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **DESIGNED BY** | **REVISED BY** | **AUTHORIZED BY** | | | |
|  |  |  | | | |
| M. en C. Nidia Asunción Cortez Duarte  M. en C. Sandra Díaz Santiago  COLLABORATING PROFESSORS | Dr. Flavio Arturo Sánchez Garfias  Subdirector Académico | Ing. Apolinar Francisco Cruz Lázaro  Director | | | |
| **Date**: | 2011 |