Miami Dade College

**Course Description**

**CET4663C | Electronic Security | 3.00 credits**

This is an upper division course for students who are majoring in electronics engineering technologies. The student will learn information and communication security principles for computer systems and networks including authentication, protection, security models, cryptography, applications, and public policy, along with case studies. Prerequisite: CET2123C, COP2270.

**Course Competencies:**

**Competency 1:** The student will demonstrate an understanding of key electronic security terminology and techniques by:

1. Identifying the necessary components to ensure a system is secure (i.e. confidentiality, integrity, and availability)
2. Defining the principle of most effortless penetration and its implications on secure design
3. Identifying and providing examples of the four primary threats that all attacks can be categorized into (i.e. interception, interruption, modification, and fabrication)
4. Identifying and describing the three requirements for any attack to occur (i.e. method, opportunity, and motive)
5. Comparing and contrasting the three primary goals of computer security (i.e. confidentiality, integrity, and availability) and explaining why there is often a trade-in in implementing these goals
6. Identifying the primary vulnerabilities within hardware, software, and data
7. Enumerating the most common types of computer criminals (i.e. amateurs, crackers/hackers, career criminals, governments, and terrorists)
8. Enumerating and describing the defense methods (i.e. prevent, deter, deflect, detect, and recover). 9. Defining and implementing a steganography algorithm

**Competency 2:** The student will demonstrate an understanding of elementary cryptography by:

1. Defining key terminology used in cryptography (e.g. plaintext, ciphertext, keys, cipher, encipher, cryptosystem, cryptanalysis, etc.)
2. Comparing and contrasting substitution versus permutation ciphers
3. Describing, implementing, and using a basic substitution cipher (e.g. Caesar cipher)
4. Describing, implementing, and using a basic permutation cipher (e.g. Caesar cipher)
5. Explaining why one-time pads are considered to have perfect, unbreakable encryption as well as why they are challenging to implement
6. Enumerating and explaining Shannon's five characteristics of "good ciphers"
7. Enumerating and defining properties required of "trustworthy encryption systems"
8. Defining, comparing, and contrasting the difference between confusion and diffusion
9. Defining, comparing, and contrasting the difference between stream ciphers and block ciphers
10. Using crypto analytic techniques to break simple substitution and permutation ciphers

**Competency 3:** The student will demonstrate an understanding of symmetrical encryption by:

1. Describing the environment that led to the development of the Data Encryption Standard (DES)
2. Identifying, describing, and explaining the purpose of each stage of the DES algorithm
3. Explaining why the input and output permutation in DES do not improve the security
4. Enumerating the weaknesses of the DES algorithm
5. Comparing and contrasting the protection provided by 3DES as compared to 2DES
6. Using the DES algorithm to encrypt a data file
7. Describing the environment that led to the development of the Advanced Encryption Standard (AES)
8. Identifying, describing, and explaining the purpose of each stage of the AES algorithm
9. Comparing and contrasting the DES and AES algorithms
10. Defining what a Feistel structure is and why it is essential to the design of encryption techniques
11. Using the DES and AES algorithms to encrypt and decrypt data

**Competency 4:** The student will demonstrate an understanding of asymmetrical encryption by:

1. Identifying the inherent difficulties with symmetric encryption

2. Explaining how asymmetric encryption helps to mitigate the difficulties with symmetric encryption
3. Performing modular arithmetic, including modular addition, modular multiplication, and modular exponentiation
4. Defining key expressions and terminology, including multiplicative inverse, relatively prime, and the totient function
5. Describing the steps required to perform the RSA (Rivest, Shamir, Adleman) encryption algorithm
6. Performing the RSA algorithm on a given number by hand
7. Using the RSA algorithm to encrypt and decrypt data
8. Describing a key exchange algorithm or protocol (e.g. Diffie Hellman)
9. Defining, explaining, and using a standard hashing function such as MD5

**Competency 5:** The student will demonstrate an understanding of the various encryption modes of operation by:

1. Describing the need for modes of operation when messages become more significant than the block size of an algorithm
2. Explaining how the Electronic Code Book (ECB) mode of operation works and its advantages and disadvantages
3. Explaining how the Cipher Block Chaining (CBC) mode of operation works and its advantages and disadvantages
4. Explaining how the k-Bit Cipher Feedback (CFB) mode of operation works and its advantages and disadvantages
5. Explaining how the k-Bit Output Feedback (OFB) mode of operation works and its advantages and disadvantages
6. Explaining how the Counter (CTR) mode of operation works and its advantages and disadvantages
7. Describing how the various modes of operation can be used to implement hash algorithms

**Competency 6:** The student will demonstrate an understanding of program-level security by:

1. Identifying early methods of preventative program security, including penetrate and patch and tiger teams and their inherent flaws
2. Defining, describing, and identifying the various forms of no malicious program errors within a code sequence (e.g. buffer overflow, string injection, time of check/time of use, incomplete mediation, etc)
3. Enumerating, comparing, and contrasting the different forms of malicious code (e.g. Virus, Trojan Horse, Logic Bomb, Time Bomb, Trapdoor, Worm, Rappit, etc)
4. Describing how encapsulation, modulation, and mutual suspicion all assist in the development of secure code
5. Identifying the strengths of peer review code, as well as the difficulties with proving program correctness.
6. Describing the attack vectors that can take place after a program is compromised (e.g. shellcode injection, variable dumping, etc)

**Competency 7:** The student will demonstrate an understanding of legal and ethical issues related to electronic security by:

1. Identifying ethical, professional responsibilities, risks, and liabilities in electronic, computer, and network environments
2. Describing mandatory access control and how covert channels can be used to subvert such control.
3. Defining and describing the Orange Book and its successors
4. Discussing privacy implications of electronic security
5. Discussing the impact of emerging technologies such as RFID, electronic voting, and VOIP
6. Presenting or debating a case study of an ethical dilemma related to electronic security and/or privacy

**Competency 8:** The student will demonstrate the ability to interpret and present research in the area of electronic security by:

1. Describing the latest developments in computer and network security
2. Locating, reading, and presenting a recent journal or conference paper presented at an IEEE or ACM-accepted conference

**Learning Outcomes:**

- Use quantitative analytical skills to evaluate and process numerical data
- Solve problems using critical and creative thinking and scientific reasoning

- Formulate strategies to locate, evaluate, and apply information
- Demonstrate knowledge of ethical thinking and its application to issues in society
- Use computer and emerging technologies effectively