|  |  |  |
| --- | --- | --- |
| **ICT 4102:** | **INFORMATION & WEB SECURITY** | **[3 0 0 3]** |

**Objectives:**

* To provide mathematical tools to understand the working of cryptographic algorithms.
* To provide introduction to the fundamental principles of information security.
* Describe the browser security model including same-origin policy and threat models in web security.
* Discuss the concept of web sessions, secure communication channels such as TLS and importance of secure certificates, authentication including single sign-on such as OAuth and SAML

**Abstract:**

Introduction to Information and Network Security, Mathematical Tools of Symmetric Cryptography, Symmetric-Key Ciphers: Classical and Modern, Mathematical Tools for Asymmetric Cryptography, Asymmetric-Key Cryptography, Message Integrity and Message Authentication, Digital Signature, Key Management, User Authentication, Transport Level Security, Wireless Network Security, Email Security, IP Security

**Syllabus:**

**Introduction to Information and Network Security**  **[2 Hours]**

Computer Security Concepts, The OSI Security Architecture, Security Attacks, Security Services

Security Mechanisms, A Model for Network Security

**Mathematical Tools of Symmetric Cryptography [2 Hours]**

Modular arithmetic, Linear Congruence, Algebraic structures, GF fields

**Symmetric-Key Ciphers [6 Hours]**

Kerckhoff’s principle, Substitution ciphers, Transposition ciphers, Stream and block ciphers, DES, AES, Use of modern block ciphers

**Mathematical Tools for Asymmetric Cryptography [2 Hours]**

Primes, Primality testing, Factorization, CRT, Quadratic congruence, Exponentiation and logarithm

**Asymmetric-Key Cryptography [6 Hours]**

Asymmetric cryptosystems, RSA, Rabin and ElGamal, ECC

**Message Integrity and Message Authentication [4 Hours]**

Message integrity, Random Oracle model, Message authentication, Hash function, SHA-512, Whirlpool

**Digital Signature [4 Hours]**

Digital signature schemes: RSA, ElGamal, Schnorr, ECC, Digital Signature Standard, Attacks on digital signature

**User Authentication [2 Hours]**

Passwords, Challenge-response, Zero-knowledge, Biometrics

**Key Management [2 Hours]**

KDC, Kerberos, Public key distribution: CA, PKI

**Transport Level Security [2 Hours]**

Web Security Considerations, SSL, TLS, HTTPS and SSH

**Wireless Network Security [2 Hours]**

Wireless LAN overview, IEEE 802.11 I Wireless LAN Security

**Email Security [1 Hour]**

PGP, S/MIME

**IP Security [1 Hour]**

Overview, IP Security Policies

**Outcomes:**

By the end of this course, the student should be able to

* Understand advanced concepts on Information as well as web security
* Understand the mathematical structure used in cryptosystems
* Describe common types of attacks in web applications as well as defence against them.
* Apply the knowledge of client-side security capabilities in an application.
* Design the security algorithm for real world applications

**References:**

1. Security in Computing ( 5th Edition) by Charles P. Pfleeger, Shari Lawrence Pfleeger and Jonathan Margulies
2. Cryptography and Network Security: Principles and Practice (5th Edition) by William Stallings
3. Cryptography and Network Security (4th Edition) by Behrouz A.Forouzan, McGraw-Hill