EE 518: Network Security

Lecture Schedule	Tuesday,Thursday 6:00 – 7:30 pm	**Semester**	Fall 2019
Credit Hours	Three	**Pre-requisite**	Computer Networks (UG)
Instructor	Muhammad Ali	**Contact**	m.ali@uet.edu.pk
Office	Room # 206 EE Department UET, Lahore	**Office Hours**	Tuesday,Thursday 4:00 – 6:00 pm
Course Description	The course aims to provide overview of the main concepts and mathematics behind most of the cryptographic algorithms. It gives the theoretical knowledge concerning the architectures of symmetric and asymmetric cryptosystems. The course describes key management and message authentication. It also outlines some of the well known security standards as IPsec, Kerberos, Secure Socket Layer (SSL)/Public Key Infrastructure (PKI).		

Measurable Learning Outcomes	**CLOs**	**Description**	**PLOs**	**Level**
	CLO1	Symmetric-key cryptography and protocols using symmetric-key encipherment	PLO1	High
	CLO2	Asymmetric-key cryptography and protocols using asymmetric-key encipherment	PLO1	High
	CLO3	Become familiar with integrity, authentication and key distribution	PLO1	High
	CLO4	Become familiar with network and system security	PLO1	High
	CLO5	Implement cryptography and analyse protocols in Python/Perl	PLO5	High

Textbooks	**REQUIRED**: Lecture notes, Avinash Kak, Purdue University **OPTIONAL**: Cryptography and Network Security by Behrouz A. Forouzan and Debdeep Mukhopadhyay, 2nd Edition, McGraw Hill. Network Security: PRIVATE Communication in PUBLIC World by Charlie Kaufman, Radia Perlman and Mike Speciner, 2nd Edition, Pearson Education.		
Grading Policy	Assignments/Quizzes Midterm Final	30% 30% 40%	CLO1 to CLO5 CLO1 to CLO2 CLO3 to CLO4

Lecture Plan

Weeks	Topics	Lecture notes & CLOs
0.5*	Classical Encryption Techniques	Lec2 CLO1-2 & CLO5
1.5*	Finite Fields	Lec4-7 CLO1-2 & CLO5
1*	AES: The Advanced Encryption Standard	Lec8 CLO1 & CLO5
0.5*	Block and Stream Ciphers	Lec9 CLO1-2 & CLO5
0.5*	Key Distribution	Lec10 CLO3 & CLO5
1*	Prime Numbers and Discrete Logarithms	Lec11 CLO2
1*	Public-Key Cryptography and the RSA Algorithm	Lec12 CLO2 & CLO5
0.5*	Certificates, Certificate Authorities, and Digital Signatures	Lec13 CLO2 & CLO5
1.5*	Elliptic Curve Cryptography	Lec14 CLO2 & CLO5
MIDTERM		
1*	Hashing for Message Authentication	Lec15 CLO3 & CLO5
0.5*	TCP/IP Vulnerabilities: IP Spoofing and Denial-of-Service Attacks	Lec16 CLO4 & CLO5
0.5*	DNS and the DNS Cache Poisoning Attack	Lec17 CLO4 & CLO5
1*	Firewalls	Lec18,19 CLO4
1*	PGP, IPSec, SSL/TLS, and Tor Protocols	Lec20 CLO4
0.5*	The Buffer Overflow Attack	Lec21 CLO4 & CLO5
0.5*	Malware: Viruses and Worms	Lec22 CLO4 & CLO5
0.5*	Port and Vulnerability Scanning, Packet Sniffing, Intrusion Detection, and Penetration Testing	Lec23 CLO4
0.5*	Dictionary Attacks and Rainbow-Table Attacks on Password Protected Systems	Lec24 CLO3
1*	Security Vulnerabilities of Mobile Devices	Lec32 CLO4 & CLO5
FINAL		

* - Tentative