DR. A.P.J. ABDUL KALAM TECHNICAL UNIVERSITY, LUCKNOW, UTTAR PRADESH

EVALUATION SCHEME & SYLLABUS

FOR

B. TECH. 4TH YEAR

Electronics and Computer Engineering

Based On

NEP2020

(Effective from the Session: 2025-26)

DR. A.P.J. ABDUL KALAM TECHNICAL UNIVERSITY, LUCKNOW, UTTAR PRADESH

B. TECH (ELECTRONICS AND COMPUTER ENGINEERING) CURRICULUM STRUCTURE

SEMESTER- VII

Sl. No.	Subject Code	Subject	Learning Mode	Periods			Evaluation Scheme				End Semester		Total	Credit
				L	T	P	CT	TA	Total	PS	TE	PE		
1	BCIT701	Cryptography and Network Security	Offline	3	-	-	20	10	30		70		100	3
2	B**07*	Deptt- Elective-IV	Offline	3	-	-	20	10	30		70		100	3
3	BOEM**	Open Elective-II	MOOC's	3	0	0	20	10	30		70		100	3
4	BCIT751	Cryptography and Network Security LAB	Offline	0	0	2				50		50	100	1
5	BECZ752	Mini Projects or Internship Assessment*		0	0	4	-	-	-	100	-	-	100	2
6	BECZ753	Project-1		0	0	10				150		-	150	5
7	BECZ754	Startup and Entrepreneurial Activity Assessment#		0	0	4				100			100	2
		Total		**9**	**0**	**20**							**750**	**19**

*The Mini Project or internship (5-6 weeks) conducted during summer break after VI semester will be assessed during VII semester. *#The Startup and Entrepreneurial Activity Assessment will be done in the 7th semester, under which a student will have to undergo a startup/entrepreneurship activity of at least 60 hours till the 6th semester*

SEMESTER- VII

Sl. No.	Subject Code	Subject	Learning Mode	Periods			Evaluation Scheme				End Semester		Total	Credit
				L	T	P	CT	TA	Total	PS	TE	PE		
1	BOENM**	Open Elective-III	MOOC'S	3	0	0	20	10	30		70		100	3
2	BOENM**	Open Elective-IV	MOOC'S	3	0	0	20	10	30		70		100	3
4	BECZ851	Project-II		0	0	18				100		350	450	10
		Total		**6**	**0**	**18**							**650**	**16**

The Internal Assessment of MOOCs will be done by the respective institute, and the External Assessment (End Semester Examination) will be done by the University.

Departmental Elective-IV

1. BCS070- Internet of Things
2. BCS071- Cloud Computing
3. BECZ070- Electric Vehicle Technology
4. BCS073- Design and Development of Applications

B. TECH (ELECTRONICS AND COMPUTER ENIGNEERING)
SEVENTH SEMESTER (DETAILED SYLLABUS)

BCIT701 Cryptography & Network Security

Course Outcome (CO)		Bloom's Knowledge Level (KL)
At the end of course, the student will be able:		
CO 1	Classify the symmetric encryption techniques and Illustrate various Public key cryptographic techniques.	K_2, K_3
CO 2	Understand security protocols for protecting data on networks and be able to digitally sign emails and files.	K_1, K_2
CO 3	Understand vulnerability assessments and the weakness of using passwords for authentication	K_4
CO 4	Be able to perform simple vulnerability assessments and password audits	K_3
CO 5	Summarize the intrusion detection and its solutions to overcome the attacks.	K_6

DETAILED SYLLABUS		3-0-0
Unit	**Topic**	**Proposed Lecture**
I	Introduction to security attacks, services and mechanism, Classical encryption techniques- substitution ciphers and transposition ciphers, cryptanalysis, steganography, Stream and block ciphers. Modern Block Ciphers: Block ciphers principles, Shannon's theory of confusion and diffusion, fiestal structure, Data encryption standard(DES), Strength of DES, Idea of differential cryptanalysis, block cipher modes of operations, Triple DES	**08**
II	Introduction to group, field, finite field of the form GF(p), modular arithmetic, prime and relative prime numbers, Extended Euclidean Algorithm, Advanced Encryption Standard (AES) encryption and decryptionFermat's and Euler's theorem, Primarily testing, Chinese Remainder theorem, Discrete Logarithmic Problem,Principals of public key crypto systems, RSA algorithm, security of RSA	**08**
III	Message Authentication Codes: Authentication requirements, authentication functions, message authentication code, hash functions, birthday attacks, security of hash functions, Secure hash algorithm (SHA) Digital Signatures: Digital Signatures, Elgamal Digital Signature Techniques, Digital signature standards (DSS), proof of digital signature algorithm,	**08**
IV	Key Management and distribution: Symmetric key distribution, Diffie-Hellman Key Exchange, Public key distribution, X.509 Certificates, Public key Infrastructure. Authentication Applications: Kerberos, Electronic mail security: pretty good privacy (PGP), S/MIME.	**08**
V	IP Security: Architecture, Authentication header, Encapsulating security payloads, combining security associations, key management. Introduction to Secure Socket Layer, Secure electronic, transaction (SET) System Security: Introductory idea of Intrusion, Intrusion detection, Viruses and related threats, firewalls	**08**

Text books:

1. William Stallings, "Cryptography and Network Security: Principals and Practice", Pearson Education, 2020.
2. Behrouz A. Frouzan, "Cryptography and Network Security", McGraw Hill, 2015.
3. C K Shyamala, N Harini, Dr. T.R.Padmnabhan, "Cryptography and Security", Wiley, 2011
4. Bruce Schiener, "Applied Cryptography", Wiley, 2015.
5. Bernard Menezes, "Network Security and Cryptography", Cengage Learning, 2010.
6. Atul Kahate, "Cryptography and Network Security", McGraw Hill, 2020.