MOHANLAL SUKHADIA UNIVERSITY, UDAIPUR

BACHELOR OF COMPUTER APPLICATION
(BCA Annual Scheme)

(To be offered in affiliated colleges from session 2016-17)

1. **Duration of the Course :** The BCA (AnnualScheme)course will be of three years duration. Each year will be approximately 10 months (minimum 180 working days) duration.
2. **Medium of Instruction :** The medium of instruction and examination shall be English.

Third Year B.C.A.

(a) The minimum marks for passing III year shall be 40% in each paper and 40% marks in the aggregate of papers.

A candidate may be allowed to reappear in two papers of III year if he has/she secured at least 40% marks in at least six papers/practicals/project out of 8 theory/practical/project papers and more than 40% in aggregate. Such candidate shall be required to appear in papers in which he has secured less than 40% marks along with due papers of I & II year (if any) when these courses are offered again, so as to sat isfy the passing criteria laid in III(a).

(c) A candidate fails to satisfy the criteria III(a), III(b) shall be required to rejoin the course in III year, if otherwise eligible in accordance with the University regulations laid in this regard.

No candidate shall be deemed to have satisfied examination requirement for the award of BCA degree unless he fulfills the criteria for passing I year, II year and III year examinations, as laid in I(a), II(a) and III(a).

Candidate will not be allowed to reappear in any papers of I,II & III year to improve the percentage.

At the end of final examination, the candidates eligible for the award of B.C.A. (Annual Scheme)degree shall be classified on the basis to the marks obtained in the I,II & III year examinations, taken together, as follows:

(a) **I division with distinction :** 75% or more marks in the aggregate and provided the candidate has passed all the papers and examinations in the first attempt.

(b) **I division :** 60% or more marks but fails to satisfy the criteria for being classified as first division with distinction laid in (a).

(c) **II division : 48% or more but less than 60%**

(d) **III division: 40% or more but less than 48%**

A candidate must pass the examinations within five years of the initial admission to the first year of the course.

BCA303: Information Security &Cryptography

UNIT-I

Overview of cryptography : Need of security, cryptographic goals, security approaches, basic terminology and concepts, symmetric key encryption - block cipher and stream cipher, substitution cipher and transposition ciphers, key space, public key cryptography, symmetric key v/s public key cryptography. Protocols and mechanisms, key management through symmetric key and public key techniques, attacks on encryption schemes, attacks on protocols, models for evaluating security, perspective for computational security.

UNIT-II

Pseudorandom bits and sequences : Random bit generation – hardware based generator and software based generator, tests for measuring randomness – frequency, serial, poker, runs and autocorrelation test. Blum-Blum-Shub pseudorandom bit generator.

Stream ciphers: Classification, one time pad, properties of synchronous and self-synchronizing stream cipher, linear and nonlinear feedback shift registers, stream ciphers based on LFSRs and its property, SEAL.

UNIT-III

Block ciphers : Modes of operation – ECB, CBC, CFB and OFB mode, exhaustive key search and multiple encryption, classical ciphers – transposition and substitution based ciphers, Vigenere ciphers, cryptanalysis of classical ciphers, Data Encryption Standard algorithm, double and triple DES, IDEA, Advance encryption standard, comparison of block ciphers, differential and linear cryptanalysis.

Public key encryption : Overview of symmetric key cryptography, RSA algorithm, EIGmal encryption, Knapsack encryption algorithm. public key cryptography standard (PKCS), PKI and security.

UNIT-IV

Message and Users authentication : One way hash functions, message digest, MD5 algorithm, secure hash algorithm (SHA1), comparison between different message digest algorithm, message authentication code.

Users authentication : authentication basics, password, authentication tokens, certificate based authentication, biometric authentication, Kerberos, Single sign on approach.

UNIT-V

Digital signature: digital envelope, classification of digital signature schemes – appendix and message recovery, attacks on signature.

Key management techniques: simple key establishment models, tradeoffs among key establishing protocols, techniques for distributing confidential key, techniques for distributing public keys, comparison of techniques for distributing public keys, key management involving multiple domains, key management life cycle.

Text/Reference Books

1. Applied cryptography – Menezes, Oorschot andVanstone
2. Network Security Essentials - WilliamStallings