DING (OLE) : ActiveX controls Vs. Ordinary Windows Controls – Installing ActiveX controls – Calendar Control – ActiveX control container programming – create ActiveX control at runtime – Component Object Model (COM) – containment and aggregation Vs. inheritance – OLE drag and drop – OLE embedded component and containers – sample applications

UNIT-V

ADVANCED CONCEPTS : Database Management with Microsoft ODBC – Structured Query Language – MFC ODBC classes – sample database applications – filter and sort strings – DAO concepts – displaying database records in scrolling view – Threading – VC++ Networking issues – Winsock – WinInet – building a web client – Internet Information Server – ISAPI server extension – chat application – playing and multimedia (sound and video) files

TEXT BOOKS :

1. Charles Petzold, "Windows Programming", Microsoft press, 1996 (Unit I)

2. David J.Kruglinski, George Shepherd and Scot Wingo, "Programming Visual C++", Microsoft press, 1999 (Unit II – V)

REFERENCE:

1. Steve Holtzner, "Visual C++ 6 Programming", Wiley Dreamtech India Pvt. Ltd., 2003.

BCA 303: 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.

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 :

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

UNIT-IV

Message and Users authentication : One way hash func-tions, message digest, MD5 algorithm, secure hash al-gorithm (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 ap-proach.

UNIT-V

Digital signature: digital envelope, classification of digi-tal signature schemes – appendix and message recov-ery, attacks on signature.

Key management techniques: simple key establishment

1. Applied cryptography – Menezes, Oorschot Vanstone

2. Network Security Essentials - William Stallings