# CS6701-CRYPTOGRAPHY AND NETWORK SECURITY

## Question Bank

## Unit-I

### INTRODUCTION & NUMBER THEORY

### Part A

1. DifferentiatebetweenActiveattacksandPassiveAttacks
2. DefineSteganography.
3. QuoteEuler'stheorem.
4. Definecryptanalysis.
5. CompareSubstitutionandTranspositiontechniques.
6. AnalyzewhyRandom numbersareusedinNetworkSecurity
7. Listthefourcategoriesofsecuritythreats
8. Solve $11^7$ mod13.
9. Defineprimitiveroot.
10. Give examplesforsubstitutioncipher.
11. Definecryptography
12. ExplainwhyModulararithmetichasbeenusedincryptography.
13. CompareBlockandStreamcipher.
14. Classifythebasicfunctionsusedinencryptionalgorithms.
15. Describesecuritymechanism.
16. Assess thefollowingcipherTextusingbruteforceattack: CMTMROOEOORW (Hint:Algorithm-Railfence)
17. Generalizewhynetworkneedsecurity.
18. Giveexamplesfortranspositioncipher.
19. Showhowtoconvertthegiventext"SYEDAMMAL"intociphertextusingRail fenceTechnique.
20. Planhowmanykeysarerequiredbytwopeopletocommunicateviaacipher.

### Part B

1. StateandDescribe Fermat's theorem(8)
2. StateandDescribe Euler's theorem(8)
3. TabulatethesubstitutionTechniquesindetail(8)
4. DescribetheTranspositionTechniquesindetail(8)
5. Listthedifferenttypesofattacksandexplainindetail.(8)
6. DescribeChineseremaindertheoremwithexample.(8)
7. Evaluate $3^{21}$ mod11usingFermat'stheorem.(4)
8. FindGCDusingEuler'sTheoremwithExample.(6)
9. FindGCDof1070and1066usingEuclidalgorithm.(6)

10. Encryptthemessage“PAY” usinghillcipherwiththefollowingkeymatrix andshow thedecryption toformulateoriginal plaintext(8)

$$K=\begin{vmatrix}17 & 17 & 5\\ 21 & 18 & 21\\ 2 & 2 & 19\end{vmatrix}$$

11. Generalizethesecurityservicesclassificationsandsecuritymechanismsin detail.(8)

Summarizethefollowingindetail

(i) ModularExponentiation(8)
(ii) Finitefields(8)

12. ApplyCaesaricipherandk=5decryptthegivenCiphertext“YMJTYMJWXNIJTKXNQJSHJ”. (8)
13. ApplyVigenerecipher; encryptthewords“explanation”usingthekey“leg”. (8)
    (i) DiscussbrieflytheDiscreteAlgorithms.(8)
    (ii) DiscussabouttheGroups,RingsandField(8)
14. Differentiate between transposition cipher andsubstitution cipher. Apply two stage transpositionsCipher on the “treat diagrams as single units” using the keyword“sequence”.
    (i)WhatisSteganography?Brieflyexamineanythreetechniquesused.(8)
    (ii)Whatismono-alphabeticcipher?ExaminehowitdiffersfromCaesarcipher? (8)
    Solveusingplay-faircipher.Encryptthewords“SemesterResult”withthe keyword“Examination”.Listtherulesused.
15. Withaneatblockdiagram,explainthenetworksecuritymodelandthe importantparametersassociatedwithit.(8)
16. Differentiateactiveandpassivesecurityattacks.Categorizetheseattacksandexplainoneexamplesof each(8)
17. Explainhowtosolve$x^2 \equiv 1 \pmod{35}$usingChineseremaindertheorem.(8)
18. ExplainindetailtheEuclid’sAlgorithm.(8)
19. Discussthefollowing
    a) Message Integrity(2) b) Denialof Service(2) c) Availability(2)
    d) Authentication(2)
20. (ii)Estimate$11^{13} \bmod 53$usingmodularexponentiation.(8)

## Unit-II

## BLOCK CIPHERS & PUBLIC KEY CRYPTOGRAPHY

### Part A

1. DefineRC5.
2. Listthefivemodesofoperationofblockcipher?
3. Analyzewhethersymmetricandasymmetriccryptographicalgorithmneedkey exchange.
4. Formulate fewapplicationsofRC5algorithm.
5. GivewhatprimitiveoperationsareusedinRC5?
6. CriticizewhythemiddleportionoftripleDESadecryptionratherthan encryption? Defineavalancheeffect?
7. PointoutisitpossibletousetheDESalgorithmtogeneratemessage authenticationcode.
8. Discoverthedifferencebetweensubbytesandsubwords.
9. Describeistripleencryption?Howmanykeysareusedintripleencryption?
10. Givetheapplicationsofthepublickeycryptosystems.
11. ExplainanyoneattackingtechniqueinRSA.
12. DiscovertheDifferencebetweenpublickeyandconventionalencryption.
13. SummarizethepurposeofDiffie-Hellmankeyexchange.

14. Definetheprincipleelementsofapublickeycryptosystem.
15. Listfourgeneralcharacteristicsofschemaforthedistributionofthepublickey.
16. Showwhatrequirementsmustapublickeycryptosystemtofulfilsecurity.
17. EvaluateencryptionanddecryptionusingRSAalgorithmforthefollowing. p=7,q=11;e=17;m=8
18. GeneralizewhetherstrongprimesarenecessaryinRSA.
19. Identifytherolesofpublicandprivatekey.

## Part B

1. Describeindetail,thekeygenerationinAESalgorithmanditsexpansion format.(8)
2. DescribeTripleDESanditsapplications.(8)
3. Explainthefollowingmodesofoperationinblockcipher.
   i. ElectroniccodebookandCipherblockchaining.(8)
   ii. Cipherfeedbackmodeandoutput
4. FormulatethesingleroundofDESalgorithm and designthekeydiscardingprocessofDES.
5. DescribetheRC5methodusedforencryptionanddecryption and describeTripleDESanditsapplications.
6. DrawthegeneralstructureofDESanddescribehowencryptionanddecryption arecarriedout and identifythestrengthofDESalgorithm.
7. AnalyzehowmeetinmiddleattackisperformedondoubleDataEncryptionStandard and Explainthesubstitutionbytestransformationandaddroundkey
8. HowAESisusedforencryption/Decryption? Discusswithexample. (ii)DiscussindetailaboutBlowfish.
9. EvaluateusingDiffie-Hellmankeyexchangetechnique.UsersAandBusea commonprimeq=11andaprimitiverootalpha=7.(i)If userAhasprivatekeyXA=3.Whatis A'spublickeyYA? (ii)IfuserB hasprivatekeyXB=6.Whatis B'spublickeyYB? (iii)Whatisthesharedsecretkey?Also
10. DescribeRSAAlgorithm and Estimatethe encryptionanddecryptionvaluesfortheRSAalgorithmparameters.
11. Howisdiscretelogarithmevaluatedfora number?Summarizetheroleofdiscrete logintheDiffie-Hellman keyexchange inexchanging thesecretkeyamongtwo users? What are elliptic curves? Describe how the elliptic curves are useful for
12. BrieflydescribetheideabehindEllipticCurveCryptosystem and describethekeymanagementofpublickey
13. Apply the mathematical foundations of RSA algorithm. Perform encryption decryption forthefollowingdata.P=17, q=7, e=5, n=119, message="6". Use ExtendedEuclid'salgorithmtofindtheprivatekey.
14. UserAandBuseDiffie-Hellmankeyexchangeacommonprimeq=71anda primitiveroota=7.**Calculate**thefollowing. IfuserAhasprivatekey$X_A$=5,whatisA'spublickey$Y_A$. IfuserAhasprivatekeyXB=12,whatisB'spublickeyYBandwhatisshared secretkey?
15. ConsidertheellipticcurveE11(1,6);thatisthecurveisdefinedby$y^2=x^3+x+6$ with amodulesofP=11. Calculate allthe points in E11(1,6). Start by calculationtherighthandsideoftheequationofallthevaluesofn?
16. ExplainbrieflyaboutDiffie-Hellmankeyexchangealgorithmwithitsprosand cons.
17. Explainpublickeycryptographyandwhenisitpreferred.

## Unit-III

## HASH FUNCTIONS AND DIGITAL SIGNATURES

## Part A

1. Givetherequirementsformessageauthentication?
2. Whatdoyouinterpretfromonewaypropertyinhashfunction?
3. Explaindirectandarbitrateddigitalsignature.
4. Define digitalsignature.
5. Formulatethetypesofattacks addressedbymessageauthentication
6. Listthepropertiesadigitalsignatureshouldhave.
7. Evaluatewhatarethesecurityservicesprovidedbydigitalsignature.
8. DistinguishDSAandElGamalalgorithm.
9. DefineMAC.
10. Listtherequirementsofhashfunction?
11. EstimatetheblocksizeofMD5.
12. DifferentiateMACandhashfunction.
13. Discriminate message authenticationcodeandonewayhashfunction.
14. ShowhowSHAismoresecurethanMD5?
15. Listanythreehashalgorithm.
16. Formulatehowdigitalsignatureisdifferentfromconventional.Giveanytwo.
17. Definetheclassesofmessageauthenticationfunction.
18. CompareMD5andSHAalgorithm.
19. Illustrate theauthenticationrequirements.
20. Classifytheapproachesofdigitalsignature.

## PART-B

1. Wherehashfunctionsareused?Whatcharacteristicsareneededinsecurehash function?writeaboutthesecurityofhashfunctionsandMACs
2. Describedigitalsignaturealgorithmandshowhowsigningandverificationis doneusingDSS.
3. Explaintheprocessofderivingeighty64-bitwords from1024bitsfor processing ofasingleblocksandalsodiscusssingleroundfunctioninSHA-512 algorithm.ShowthevaluesofW16,W17,W18andW19.
4. WhatisDigitalSignature?Explainhowitiscreatedatthesenderendand retrievedatreceiverenddifferentiatedigitalsignaturefromdigital
5. DescribeHMACalgorithmindetail andGive theclassificationofauthenticationfunctionindetail.
6. Compareandgeneralize the featuresofSHAandMD5algorithm. Formulate theobjectivesofHMACanditssecurityfeatures
7. AnalyzetheMD5messagedigestalgorithmwithnecessaryblock
8. DescribeindetailEl-GamalPublickeycryptosystemswithanexample.
9. DescribeDigitalsignaturealgorithm&showhowsigning&verificationisdone usingDSS
10. IllustrateSecureHashAlgorithmindetail andclassifyitsperformancewithMD5.
11. Give abriefnotesonX.509authenticationservices.
12. Discuss thesecurityofhashfunctionsandMACs and describeanyonemethodofefficientimplementationofHMAC.
13. Illustrate indetailmessageauthenticationcodeandits requirements
14. Withaneatflowchart,ShowhowMD5processasingle512bitblock

## UNIT –IV

### SECURITY PRACTICE & SYSTEM SECURITY

## PART-A

1. ListwhataretheClassesofmessageauthenticationfunction?
2. Pointoutthedesigngoalsoffirewalls.
3. ShowwhenthecertificatesarerevokinginX.509.
4. Pointoutthe commonlyusedfirewallsfromthreatsofsecurity.
5. DefineWorm.
6. Differentiatespywareandvirus.
7. IllustrateaclientCwantstocommunicatewithaserverSusingKerberos protocol.Howcanitbeachieved?
8. Inferwhatisan intruder
9. List theadvantagesofintrusiondetectionsystemoverfirewall
10. Define:SET
11. Definevirus.Specifythetypesofviruses?
12. Illustratewhatisapplicationlevelgateway
13. Definefirewall.
14. DescribewhatKerberos is.Whataretheuses?
15. Expressinbriefwhatdoyoumeanbytrustedsystems
16. Comparethe4requirements definedbyKerberos.
17. Listthe3classesofIntruders.
18. Summarize thelimitationsoffirewalls.
19. DesignwhatistheroleofTicketGrantingServerininterrealmoperationsof Kerberos
20. GeneralizewhatisthepurposeofX.509standard

## PART-B

1. FormulatewhataretherequirementsofKerberos?ExplainaboutKerberos version.
2. ExplaintheFirewalldesignprinciples.
3. Whatareviruses?Explainthevirusrelatedthreatsandthecountermeasures applied.
4. WhatismeantbymessagedigestandexplainaboutHMACdigitalsignatures.
5. Illustratethetechnicaldetailsoffirewall.
6. Illustratethethreecommontypesoffirewallswithdiagrams.
7. DescribeSecureElectronicTransactionforE-Commercetransactionwithneat diagram
8. Summarizeonthesignificanttypesofviruscategories.
9. Whatisatrustedsystem?Expressthebasicconceptofdataaccesscontrolin trustedsystems
10. Describethearchitectureofdistributedintrusiondetectionsystemwiththe necessarydiagrams
11. List aboutvirusandrelatedthreatsindetail
12. Estimatewhatistheroleofintrusiondetectionsystem?Whatarethethree benefitsthatcanbeprovidedbytheintrusiondetectionsystem?
13. Differentiate betweenstatisticalanomalydetectionandrulebasedintrusion detectionsystem?
14. Analyze thearchitectureofdistributedintrusiondetectionsystemwiththe necessarydiagrams.
15. Howdoesscreenedhostarchitectureforfirewallsdifferfromscreenedsubnetfirewallarchitecture? Whichoffermoresecurityfortheinformation assetstheremainonthetrustednetwork?Explainwithneatsketch?
16. Describetherolesofthedifferentserversin Kerberosprotocol.Howdoesthe usergetauthenticatedtothedifferentservers?

17. Give brieflyabouttrustedsystems
18. Classify the variousmeasuresthatmaybeusedforintrusiondetection.
19. Showhowtheencryptioniskeygeneratedfrompasswordin Kerberos?
20. Explainwiththehelpofanexamplehowauser'scertificateisobtainedfrom anothercertificationauthorityinX.509scheme
21. Pointout theauthenticationdialogusedbyKerberosforobtainingservice
22. ListouttheparticipantsofSETsystem,andexplainindetail
23. Describethedifferenttypesoffirewallsanditsconfigurationindetail

## UNIT-V

## E-MAIL, IP & WEB SECURITY

### PART-A

1. Whatisdualsignature?Whatitispurpose?
2. ShowwhataretheservicesprovidedbyPGP?
3. DefineS/MIME.
4. DrawtheheaderformatandlabelISAKMPmessage.
5. ExplainwhataretheprotocolsusedtoprovideIPsecurity?
6. GivetheapplicationsofIPSecurity.
7. WhatismeantbySET?WhatarethefeaturesofSET?
8. AnalyzewhyR64conversionusefulforemailgeneration?
9. Whatarethestepsinvolvedin SETTransactions?
10. Tellthereasonwhyemailcompatibilityfunctionin PGPneeded
11. DescribetunnelmodeinIPsecurity.
12. DefineSPI.
13. Developascenariowhererepla yattackispossible?
14. Differentiatetransportmodeandtunnelmode.
15. SummarizethepurposeofSSLallotprotocol?
16. ExaminedoesESPincludeapaddingfield?
17. Developthereasonsforusing PGP.
18. DecidewhyPGPgenerateasignaturebeforeapplyingcompression.
19. IllustratetheservicesprovidedbyIPSec?

### PART-B

1. HowdoesPGPprovideauthenticationandconfidentiality foremailservices andforfiletransferapplications? Drawtheblockdiagramandexplainthe components
2. Explainthegeneralformatof PGPmessage.
3. Summarize theOperationsofPGP?Briefthevariousservicesprovided byPGP.
4. Discussthethreatsfacedbyane-mailandexplainitssecurityrequirementsto provideasecuree-mailservice.
5. DescribeaboutthePKI.
6. DescribetheISAKMPformatwithdiagrams
7. Summarizeabouttheauthenticationheaderof IP and discussaboutencapsulatingsecuritypayloadofIP

8. ListthedifferentprotocolsofSSL.ExplainindetailHandshakeprotocol
9. TellhowdoestheservergetauthenticatedtoclientinSSL?
10. ExplainIPSecprotocolsindetail.Alsodevelopapplicationsandadvantagesof IPSec.
11. SketchandanalyzetheIPSecDocumentOverviewdiagram
12. WhatisPGP?Examinehowauthenticationandconfidentialityismaintained inPGP
13. Explainthekeyringsanditssignificancein PGP.Showhowthemessage
14. AnalyzetheCryptographicalgorithmsusedinS/MIME and ExplainS/MIMEcertificationprocessing