



**BHUBANANANDA ORISSA SCHOOL OF ENGINEERING, CUTTACK**

**DEPARTMENT OF Computer Science & IT**

**ACADEMIC SESSION-(2020-21-SUMMER)**

**SEMESTER/BRANCH:- 6<sup>th</sup> sem CSE&IT  
Cryptography & Network security**

**LESSON PLAN**

**SUBJECT:-**

**FACULTY NAME:- Mrs. Danturthi Susmita Semester  
19.04.2021 to 13.08.2021**

**From:- Date.**

No of week:-17

No of classes available per week : 4

Total period available: 68

Class duration:55 minutes

Teaching Method:Through Online Meeting App, Presentation,Sharing Lecture note PDF through whatsapp group.

Learning Method: Daily Assignment ,Unit/class test, Online Moc test through google form

**Topics wise distribution of Periods given in syllabus**

Sl. No.	Topics	Periods
1	POSSIBLE ATTACKS ON COMPUTERS	05
2	CRYPTOGRAPHY CONCEPTS	10
3	SYMMETRIC & ASYMMETRIC KEY ALGORITHMS	15
4	DIGITAL CERTIFICATE & PUBLIC KEY INFRASTRUCTURE	10
5	INTERNET SECURITY PROTOCOLS	10
6	USER AUTHENTICATION	04
7	NETWORK SECURITY & VPN	06

TOTAL 60

**1. Possible attacks on Computers 05**

- 1.1 The need for security
- 1.2 Security approach
- 1.3 Principles of security
- 1.4 Types of attacks

**2. Cryptography Concepts 10**

- 2.1 Plain text & Cipher Text
- 2.2 Substitution techniques
- 2.3 Transposition techniques
- 2.4 Encryption & Decryption
- 2.5 Symmetric & Asymmetric key cryptography

**3. Symmetric & Asymmetric key algorithms 15**

- 3.1 Symmetric key algorithm types
- 3.2 Overview of Symmetric key cryptography
- 3.3 Data encryption standards
- 3.4 Over view of Asymmetric key cryptography
- 3.5 The RSA algorithm
- 3.6 Symmetric & Asymmetric key cryptography
- 3.7 Digital signature

**4. Digital certificate & Public key infrastructure 10**

- 4.1 Digital certificates
- 4.2 Private key management
- 4.3 PKIX Model
- 4.4 Public key cryptography standards

**5. Internet security protocols 10**

- 5.1 Basic concept
- 5.2 Secure socket layer
- 5.3 Transport layer security
- 5.4 Secure Hyper text transfer protocol(SHHTTP)
- 5.5 Time stamping protocol (TSP)
- 5.6 Secure electronic transaction (SET)

**6. User authentication 04**

- 6.1 Authentication basics
- 6.2 Password
- 6.3 Authentication Tokens
- 6.4 Certificate based authentication
- 6.5 Biometric authentication

## 7. Network Security & VPN 06

7.1 Brief introduction of TCP/IP

7.2 Firewall

7.3 IP Security

7.4 Virtual Private Network (VPN)

### BOOKS Recommended:-

01 A. Kahate Cryptography & Network security TMH

02 W. Stallings Cryptography & Network Security  
Principals and

Practices Prentice Hall

03 Pachghare Cryptography & Information security  
PHI

Coverage of Syllabus upto Internal Exams (I.A.)

Chapter 1,2,3,4

### My Lesson plan:

Wk no.	Dates	No. of Periods available	Topics to be Covered	Topic actually taken	Short Fall if any	initial
1	19.4.21	1	<b>Ch 1 Possible attacks on Computers (05)</b>	need for security	nil	⓪
19.4.21 To 24.4.21	20.4.21	1	1.1 The need for security	Security approach	nil	⓪
	21.4.21	1	1.2 Security approach	principles of security	nil	⓪
	22.4.21	1	1.3 Principles of security	types of attack	nil	⓪
			1.4 Types of attacks	types of attacks	nil	⓪
			Assignment based on above			

2	26.4.21	1	1.4 Types of attacks	types of attacks & assignment	nil	⊗	
26.4.21 To 1.5.21	27.4.21	1	<b>Ch2 Cryptography Concepts (10)</b>	plaintext & cipher text	nil	⊗	
	28.4.21	1	2.1 Plain text & Cipher Text	substitution tech	nil	⊗	
	29.4.21	1	2.2 Substitution techniques	rules	nil	⊗	
		1	Assignment based on above	"	nil	⊗	NA
3	3.5.21	1	2.2 Substitution techniques	substitution techniques	nil	⊗	
	4.5.21	1	"	"	nil	⊗	
	3.5.21 To 8.5.21	1	2.3 Transposition techniques	transposition technique	nil	⊗	NA
	6.5.21	1	"	"	nil	⊗	
4	10.5.21	1	2.3 Transposition techniques	transpos" techniques	nil	⊗	
	11.5.21	1	2.4 Encryption & Decryption	Encryption & decryption	nil	⊗	
	10.5.21 to 15.5.21	1	2.5 Symmetric key cryptography	Symmetric key cryptography	nil	⊗	NA
	13.5.21	1	& Asymmetric key cryptography	Asymmetric key cryptography	nil	⊗	
		1	Assignment based on above		nil	⊗	
5	17.5.21		<b>Ch3 Symmetric &amp; Asymmetric key algorithms (15)</b>	types of symmetric key algorithms	nil	⊗	
	18.5.21		"	"	nil	⊗	
	17.5.21 to 22.5.21	19.5.21 20.5.21	3.1 Symmetric key algorithm types	"	nil	⊗	NA
			3.2 Overview of Symmetric key cryptography	overview of symmetric key cryptography	nil	⊗	
			Assignment based on above		nil	⊗	
6	21.5.21		3.2 Overview of Symmetric key cryptography	overview of symmetric key cryptography	nil	⊗	
	24.5.21 To 29.5.21	22.5.21 23.5.21	3.3 Data encryption standards	DES	nil	⊗	NA
			3.3 Data encryption standards	DES	nil	⊗	
			3.3 Data encryption standards	DES	nil	⊗	
			3.3 Data encryption standards	DES	nil	⊗	



			Assignment based on above				
7	31.5.21		3.4 Over view of Asymmetric key cryptography	overview of asymmetric key cryptography	✓	✓	NA
31.5.21 To 5.6.21	1.6.21 To 2.6.21		Cont. 3.5 The RSA algorithm	"	✓	✓	
	3.6.21		Assignment based on above	RSA Assignment	✓	✓	
					✓	✓	
8	7.6.21		3.6 Symmetric & Asymmetric key cryptography	Symm. & Asym. key cryptography	✓	✓	NA
7.6.21 To 12.6.21	8.6.21 To 9.6.21		3.7 Digital signature <b>Ch 4 Digital certificate &amp; Public key infrastructure(10)</b>	Digital signature "	✓	✓	
	10.6.21		4.1 Digital certificates Assignment based on above	Digital certificate	✓	✓	
					✓	✓	
9	14.6.21		4.1 Digital certificates	Digital certificate	✓	✓	NA
14.6.21 To 19.6.21	15.6.21 To 16.6.21		Cont.	"	✓	✓	
	17.6.21		Assignment based on above	Assignment	✓	✓	
					✓	✓	
10	21.6.21		4.2 Private key management	PKM	✓	✓	NA
21.6.21 To 26.6.21	22.6.21 To 23.6.21		Cont.	PKM	✓	✓	
	24.6.21		4.3 PKIX Model	PKIX Model	✓	✓	
					✓	✓	
11	28.6.21		4.4 Public key cryptography standards	public key cryptography standards	✓	✓	NA
28.6.21 To 3.7.21	29.6.21		Assignment based on above	Assignment	✓	✓	
	30.6.21		<b>Ch 5. Internet security protocols (10)</b>				
	1.7.21		5.1 Basic concept	ISP basic concepts	✓	✓	
			5.2 Secure socket layer	Secure socket layer	✓	✓	
12	5.7.21		5.2 Secure socket layer	Secure socket layer	✓	✓	NA
5.7.21 To 10.7.21	6.7.21 To 7.7.21		5.3 Transport layer security	TLS	✓	✓	

	8.7.21			TLS	nil	⊙	NA
13	12.7.21		5.4 Secure Hyper text transfer protocol(SHTTP)	SHTTP	nil	⊙	NA
	12.7.21 To 17.7.21	13.7.21 To 14.7.21	5.5 Time stamping protocol (TSP)	TSP	nil	⊙	NA
		15.7.21	5.6 Secure electronic transaction (SET)	SET	nil	⊙	NA
			Assignment based on above	SET & Assignment	nil	⊙	NA
14	19.7.21		<b>Ch6 User authentication(04)</b>	Authentication basics	nil	⊙	NA
		20.7.21	6.1 Authentication basics	password	nil	⊙	NA
	19.7.21 To 24.7.21	21.7.21	6.2 Password	password	nil	⊙	NA
		22.7.21	6.3 Authentication Tokens	Authentication token	nil	⊙	NA
15	26.7.21		6.4 Certificate based authentication	certificate based authentication	nil	⊙	NA
	26.7.21 To 31.7.21	27.7.21 To 28.7.21	6.5 Biometric authentication	Biometric authen	nil	⊙	NA
		29.7.21	Assignment based on above				NA
			<b>Ch7 Network Security &amp; VPN(06)</b>				NA
			7.1 Brief introduction of TCP/IP	TCP/IP	nil	⊙	NA
			7.2 Firewall	Firewall	nil	⊙	NA
16	2.8.21		7.3 IP Security	IP security	nil	⊙	NA
	2.8.21 To 7.8.21	3.8.21 To 4.8.21	7.4 Virtual Private Network (VPN) Assignment based on above	VPN	nil	⊙	NA
		5.8.21	Revision	assignment	nil	⊙	NA
17	9.8.21		Exam related question practice	Revision & question discussion		⊙	NA
	9.8.21 To 13.8.21	10.8.21 To 11.8.21					NA
		12.8.21					NA